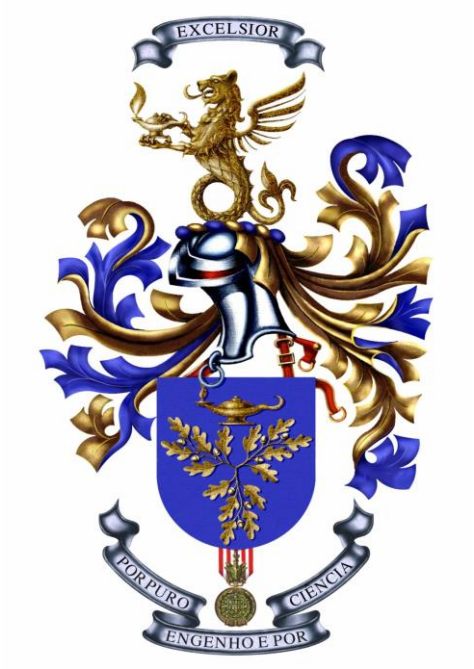
INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
MESTRADO EM CIÊNCIAS MILITARES, SEGURANÇA E DEFESA
2018/2019



DISSERTAÇÃO

O PROCESSO DO MANUAL DE TALLINN E A EVOLUÇÃO DA ESTRATÉGIA DE DISSUASÃO NO CIBERESPAÇO

Rubén Vega Bustelo
COMANDANTE DE INFANTERÍA DEM, ESPAÑA

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O PROCESSO DO MANUAL DE TALLINN E A EVOLUÇÃO DA ESTRATÉGIA DE DISSUASÃO NO CIBERESPAÇO

***CTE INF DEM ESP,* Rubén Vega Bustelo**

bustelo.rv@ium.pt

rvegbus@oc.mde.es

Dissertação do MCMSD

Pedrouços 2019

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O PROCESSO DO MANUAL DE TALLINN E A EVOLUÇÃO DA ESTRATÉGIA DE DISSUASÃO NO CIBERESPAÇO

***CTE INF DEM ESP*, Rubén Vega Bustelo**

Dissertação do MCMSD

Orientador: Professora Doutora Sofia de Vasconcelos Casimiro

Pedrouços 2019

Declaração de compromisso Anti Plágio

Eu, **Rubén Vega Bustelo** declaro por minha honra que o documento intitulado **"O processo do Manual de Tallinn e a evolução da estratégia de dissuasão no ciberespaço."** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do MCMSD 2018/2019 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, 27 de junho de 2019

Rubén Vega Bustelo

Comandante de Infantería (ESP)

Agradecimentos

A todos os que tornaram possível a realização deste trabalho.

Em especial:

À minha mulher Mari Paz, pela sua compreensão e apoio incondicional, pela tranquilidade que sempre me deu, pelas inúmeras horas que sacrificou para que eu pudesse investigar.

Ao Exmo. Sr. General Jerónimo Domínguez Bascoy, *Vocal Togado* do *Tribunal Militar Central* espanhol, ao Exmo. Sr. Coronel D. Ángel Gómez de Ágreda, chefe da Área de Análise Geopolítica da Divisão de Coordenação e Estudos de Segurança e Defesa, do Ministério de Defesa de Espanha e ao Exmo. Sr. CMG Enrique Cubeiro Cabello, chefe de operações do Mando Conjunto de Ciberdefesa de Espanha, pelas ideias e orientações que tanto contribuíram para iniciar este trabalho e estabelecer o caminho que permitiu atingir os seus objetivos.

Ao Capitão Miguel Ángel Daza Arbolí, por me apresentar, desde a sua grande experiência na investigação militar operativa, o pacote de *software* livre R, no momento crítico em que o custo e as limitações do *software* proprietário me impeliam a desistir da minha ideia de empregar ferramentas informáticas de análise qualitativa e semiquantitativa para processar o extenso *corpus* de fontes primárias em que assenta este trabalho. A flexibilidade e as imensas livrarias do R permitiram-me selecionar mais de mil fragmentos discursivos das principais autoridades da NATO, processá-los e apresentar os resultados da análise em gráficos que permitem visualizar a essência condensada do discurso dissuasório da NATO.

A todos os que contribuem para o *software* livre, por colocar ao alcance da humanidade *software* do mais avançado e por permitir que a falta de fundos não seja um obstáculo para quem goste de aproveitar, nas suas investigações, o imenso potencial das atuais tecnologias da informação e da computação.

O meu reconhecimento singular à minha orientadora, Professora Doutora Sofia de Vasconcelos Casimiro, pela sua valiosa orientação e pelo notável contributo para a melhora do meu português.

Obrigado, por fim, aos professores e camaradas do Instituto Universitário Militar, de quem tanto aprendi.

Índice

Lista de abreviaturas, siglas e acrónimos. x

Introdução 1

1 Estado da arte, metodologia e conceitos estruturantes. 6

1.1 Estado da arte 6

1.2 Modelo de análise. Metodologia 6

1.3 Modelo de análise. Conceitos. 9

2 Evolução da dissuasão ao abrigo do Processo de Tallinn. Dimensão prática. 17

2.1 Soberania e renacionalização do ciberespaço 17

2.2 A imputação na prática 21

2.3 Capacidade 26

2.4 Ambiguidade 29

2.5 Cooperação 33

2.6 Comunicação e sinalização 39

3 Compatibilidade do Processo de Tallinn com as opções de dissuasão 45

3.1 Dissuasão punitiva 45

3.2 Dissuasão defensiva 47

3.3 Na procura de uma opção de dissuasão eficaz 51

Conclusões 54

Bibliografia. 62

Metodologia da investigação 62

Monografías 63

Trabalhos de investigação e artigos científicos e na imprensa especializada. 67

Textos oficiais, textos legais e outras fontes primárias escritas 73

Corpus de fontes primárias da NATO codificadas e analisadas com R 76

Entrevistas e declarações 101

Páginas web e artigos 101

Índice de Anexos

Anexo A - Variáveis e fundamentação de indicadores de Bustelo (2017, Apd-B)…Anx A-1

Índice de Apensos

Apêndice A - Afinamento indutivo do modelo conceitual, análise relacional.....Apd A-1
Apêndice B - Dimensão teórica. Os Manuais e as dificuldades de dissuasão no ciberespaço.....Apd B-1
Apêndice C - Mapa conceitual e modelo de análise…….....Apd C-1
Apêndice D - Código para a análise relacional com o pacote *igraph* para R…...…Apd D-1
Apêndice E - Código desenvolvido para mineração e análise de texto com *tm* e R...Apd E-1

Índice de Figuras

Figura 1 – Modelo de análise. Metodologia. 9
Figura 2 – Dendrograma: Análise de comunidades por modularidade da codificação inicial (Algoritmo Greedy). 10
Figura 3 – Dendrograma: Análise de comunidades por modularidade da codificação final (Algoritmo Greedy). 11
Figura 4 – Obtenção dos conceitos estruturantes e variáveis para uma estratégia de dissuasão eficaz..... 12
Figura 5 – Soberania: análise terminológica comparativa dos quatro períodos. 17
Figura 6 – Soberania: análise terminológica comparativa desde o começo do TMP até à cimeira de Bruxelas..... 18
Figura 7 – Soberania: evolução terminológica no quadro da dissuasão da NATO no ciberespaço..... 20
Figura 8 – Imputação: análise terminológica comparativa dos quatro períodos. 21
Figura 9 – Imputação: em torno da publicação do TM2. 22
Figura 10 – Imputação: em torno do começo do TMP. 23
Figura 11 – Imputação: em torno da publicação do TM. 24
Figura 12 – Imputação: evolução terminológica no quadro da dissuasão da NATO no ciberespaço..... 25
Figura 13 – Imputação: análise terminológica comparativa dos quatro períodos. 26
Figura 14 – Capacidade: evolução terminológica no quadro da dissuasão da NATO no ciberespaço..... 29
Figura 15 – Ambiguidade: análise terminológica comparativa desde o começo do TMP. . 30
Figura 16 – Ambiguidade: análise terminológica em torno do TM2. 31
Figura 17 – Ambiguidade: evolução terminológica no quadro da dissuasão da NATO no ciberespaço..... 32

Figura 18 – Cooperação: análise terminológica comparativa dos quatro períodos. 33
Figura 19 – Ambiguidade: análise terminológica em torno do começo do TMP..... 34
Figura 20 – Cooperação: análise terminológica em torno do TM. 35
Figura 21 – Cooperação: análise terminológica em torno do TM2. 37
Figura 22 – Cooperação: evolução terminológica no quadro da dissuasão da NATO no ciberespaço. 39
Figura 23 – Comunicação da Capacidade: evolução terminológica no quadro da dissuasão NATO no ciberespaço 39
Figura 24 – Comunicação da Determinação: evolução terminológica no quadro da dissuasão NATO no ciberespaço. 40
Figura 25 – Sinalização: análise terminológica comparativa desde o começo do TMP. 42
Figura 26 – Sinalização: evolução terminológica no quadro da dissuasão da NATO no ciberespaço. 43
Figura 27 – Dissuasão Punitiva: análise terminológica comparativa em torno do TM. 45
Figura 28 – Dissuasão Punitiva: análise terminológica comparativa desde o começo do TMP. 46
Figura 29 – Dissuasão Punitiva: evolução terminológica no quadro da dissuasão da NATO no ciberespaço. 47
Figura 30 – Dissuasão Defensiva: análise terminológica comparativa em torno do TM2. . 48
Figura 31 – Dissuasão Defensiva: análise terminológica comparativa desde o começo do TMP. 50
Figura 32 – Dissuasão Defensiva: evolução terminológica no quadro da dissuasão da NATO no ciberespaço 50
Figura 33 – Documentos totais do fundo documentário *vs* documentos *cyber* e documentos dissuasão *cyber*. 51
Figura 34 – Documentos ciber *vs* documentos dissuasão *cyber* por dia. 51
Figura 35 – Frequência dos códigos atribuídos na codificação inicial. ..... Apd A-2
Figura 36 – Codificação inicial. Grafo de adjacência por solapamento (Fruchterman-Reingold) ..... Apd A-3
Figura 37 – Codificação inicial. Grafo de solapamentos (Kamada-Kawai) ..... Apd A-4
Figura 38 – Codificação inicial. Matriz de adjacência por solapamento (Mapa de calor) .... Apd A-5
Figura 39 – Frequência dos códigos atribuídos na codificação final. ..... Apd A-6
Figura 40 – Codificação Final. Grafo de solapamentos (Fruchterman-Reingold) .... Apd A-7

Figura 41 – Codificação Final. Grafo de solapamentos (Kamada- Kawai)..... Apd A-8
Figura 42 – Codificação Final. Matriz de adjacência por solapamento (Mapa de calor)..... Apd A-9
Figura 43 – Codificação Inicial. Comunidades de relação por solapamento ..... (Algoritmo Greedy) ..... Apd A-10
Figura 44 – Codificação Final. Comunidades de relação por solapamento (Algoritmo Greedy) ..... Apd A-10
Figura 45 – Avaliação de indicadores de Soberania..... Apd B-3
Figura 46 – Avaliação de indicadores de Imputação..... Apd B-8
Figura 47 – Avaliação de indicadores de Capacidade..... Apd B-12
Figura 48 – Avaliação de indicadores de Ambiguidade..... Apd B-14
Figura 49 – Avaliação de indicadores de Cooperação. ..... Apd B-15
Figura 50 – Avaliação de indicadores de Comunicação e Sinalização. ..... Apd B-17

Índice de Tabelas

Tabela 1 - Número de documentos no *corpus* de fontes primárias por estádios de seleção . 8
Tabela 2 - Número de códigos disponíveis e assignados ao *corpus* de fontes primárias nos processos de codificação..... Apd A-1

Resumo

Na Cimeira de Gales, a NATO declarou a ciberdefesa como parte nuclear da sua segurança coletiva e declarou a aplicabilidade do Direito Internacional no ciberespaço. Em Varsóvia, a NATO reafirmou o mandato coletivo no ciberespaço, declarou-o mais um domínio das operações e confirmou o compromisso com a legalidade internacional. Portanto, para a NATO atingir os seus objetivos devem concorrer dois elementos: capacidade de dissuasão alargada no ciberespaço e respeito à legalidade internacional.

Em paralelo, desde 2009 o *NATO Cooperative Cyber Defence Centre of Excellence* está a promover o *Tallinn Manual Process* orientado à investigação e formação relativas à aplicabilidade do Direito Internacional no ciberespaço. Os produtos mais salientáveis deste processo foram a publicação do *Tallinn Manual*, em 2013, e a do *Tallinn Manual 2.0*, em 2017, os dois sob a responsabilidade exclusiva de seus autores.

Através de uma estratégia de investigação qualitativa, selecionaram-se mais de mil fragmentos discursivos das principais autoridades da NATO, processaram-se com ferramentas semiquantitativas para apresentar os resultados da análise em gráficos que visualizam a essência condensada do discurso dissuasório da NATO, e, por fim, aplicou-se um modelo de raciocínio hipotético-dedutivo para avaliar como é que o *Tallinn Manual Process* influencia a dissuasão da NATO no ciberespaço.

Palavras-chave

Dissuasão, ciberespaço, OTAN, Direito Internacional, *Tallinn Manual*.

Abstract

At the NATO Wales Summit, it was agreed that cyber defence is part of NATO's core task of collective defence and that International Law applies in cyberspace. At Warsaw, 2016, NATO reaffirmed the collective mandate at cyberspace, declared it an operational domain and reaffirmed its commitment to act in accordance with International Law. Therefore, for NATO to achieve its goals, two elements must compete: deterrent capacity in cyberspace and respect to international legality.

In parallel, since 2009 the NATO Cooperative Cyber Defence Centre of Excellence is promoting the Tallinn Manual Process, oriented to research and training regarding the applicability of International Law in cyberspace. The most salient products of this process were the Tallinn Manual, published in 2013, and the Tallinn Manual 2.0, published in 2017, both under the sole responsibility of their authors.

Through a qualitative research strategy, more than a thousand discursive fragments were selected from the main NATO authorities. This corpus was processed with semiquantitative tools to present the results of the analysis in graphs that visualize the condensed essence of NATO's dissuasive discourse. Finally, a hypothetical-deductive reasoning model was applied to assess how the Tallinn Manual Process influences NATO deterrence in cyberspace.

Keywords

Deterrence, Cyberspace, NATO, International Law, Tallinn Manual.

Lista de abreviaturas, siglas e acrónimos.

CCDCOE	*NATO Cooperative Cyber Defence Centre of Excellence* / Centro de Excelência de Ciberdefesa Cooperativa da OTAN
CNU	Carta das Nações Unidas
CSNU	Conselho de Segurança das Nações Unidas
cTMP	Começo do TMP
FOC	*Full Operational Capability* / Capacidade Operativa Plena.
GGE	*Group of Governmental Experts* / Grupo de Peritos Governamentais
ICRC	*International Committee of the Red Cross* / Comité Internacional da Cruz Vermelha.
MoU	*Memorandum of Understanding* / Memorando de Entendimento.
NAC	North Atlantic Council / Conselho do Atlântico Norte.
NATO	*North Atlantic Treaty Organization* / Organização do Tratado do Atlântico Norte.
NRC	*NATO-Russia Council* / Conselho OTAN-Russia.
OSCE	Organização para a Segurança e Cooperação na Europa
OTAN	Organização do Tratado do Atlântico Norte.
R	Ambiente de *software* livre para computação estatística e análise quantitativo e qualitativo.
RQDA	*R Qualitative Data Analisys* / Análise Qualitativa de Dados para R.
SROE	*Standing Rules of Engagement* / Regras Permanentes de Empenhamento.
tm	*Text Mining Package* / Pacote de Analise por Mineração de Texto para R.
TM	*Tallinn Manual* / Manual de Tallinn. (Schmitt et al., 2013)
TM2	*Tallinn Manual 2.0.* / Manual de Tallinn 2.0. (Schmitt et al., 2017)
TMP	*Tallinn Manual Process* / Processo do Manual de Tallinn.
UN	*United Nations* / Organização das Nações Unidas

Introdução

Este Trabalho de Investigação, desenvolvido na Fase de Dissertação do Mestrado em Ciências Militares – Segurança e Defesa, subordina-se ao tema "O Processo do Manual de Tallinn e a evolução da estratégia de dissuasão no ciberespaço."

No quadro de linhas de investigação do IUM, o tema insere-se no domínio das ciências militares, área do estudo das crises e dos conflitos armados, nomeadamente no campo da estratégia, tendo uma área de sobreposição com o domínio das ciências jurídicas, na área do Direito Internacional Público.

O Processo do Manual de Tallinn (TMP), desenvolvido pelo *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE), começou em 2009 e assenta em dois pilares: a investigação sobre as questões legais pertinentes às ciberoperações e o treino projetado para operacionalizar tais questões (CCDCOE, s.d.a, CCDCOE, s.d.b, CCDCOE, s.d.b).

O primeiro marco do processo, muito relevante no âmbito internacional, atingiu-se em 2013 com a publicação do Manual de Tallinn (TM) (Schmitt et al., 2013), que rapidamente se constituiu numa referência teórica primordial, mas juridicamente não vinculativa. O segundo resultado de grande relevo do processo atingiu-se com a publicação do Manual de Tallinn 2.0 (TM2) (Schmitt et al., 2017) em fevereiro de 2017. Nos dois casos, tratam-se de documentos publicados sob a responsabilidade dos seus autores, não sendo vinculativos para nenhuma nação ou organização.

No entanto, o TMP não decorreu desacompanhado. Simultaneamente decorreram uma série de processos paralelos cujos posicionamentos jurídicos nem sempre foram convergentes com aqueles postulados pelos autores dos manuais.

Assim, cabe salientar o processo do Grupo de Peritos Governamentais (GGE) sobre Avanços no Campo da Informação e das Telecomunicações no Contexto da Segurança Internacional, iniciado em 2003 (UN, 2003) e cuja quinta reunião concluiu sem acordo em agosto de 2017 (UN, 2017), alegadamente por sobrepor os interesses político-estratégicos às questões jurídicas (Schmitt e Vihul, 2017). É difícil desligar este fracasso do novo enfoque mais funcional do Direito, que postula uma abordagem mais focada em garantir a estabilidade internacional ou a segurança dos Estados do que nos princípios teóricos gerais do Direito Internacional. Este enfoque é considerado incorreto por alguns autores, ao reduzir a Lei à política (Waxman e Shany, 2017).

O posicionamento jurídico dos manuais de Tallinn também encontra contestação num processo paralelo que está a ser desenvolvido, sob a liderança da Rússia e da China,

que pretendem um tratamento jurídico do ciberespaço diferenciado do dos restantes domínios das operações (UN, 2011; UN, 2015a).

Deixando temporariamente de lado as questões jurídicas, no domínio da estratégia, o tema abordado é de grande relevância e atualidade, não estando isento de interessantes polémicas.

Na dimensão teórica está-se a debater a exequibilidade de desenvolver estratégias de dissuasão no ciberespaço, pelas dificuldades que se apresentam em termos de soberania, imputação, capacidade, ambiguidade, cooperação, comunicação, sinalização e credibilidade.

Na dimensão da praxe internacional, em 2014, na Cimeira de Gales da NATO, concordou-se que a ciberdefesa faz parte nuclear do esquema de segurança coletiva e declarou-se a aplicabilidade do Direito Internacional no ciberespaço, incluindo o Direito Internacional Humanitário e a Carta das Nações Unidas (NATO, 2014b). Porém, esta declaração de aplicabilidade do Direito Internacional no ciberespaço não passa de uma declaração de intenções de uma parte da comunidade internacional, que encontra uma forte contestação por parte de outros atores internacionais de relevo como os já referidos.

Na seguinte Cimeira, em Varsóvia, 2016, a NATO reafirmou o mandato coletivo em relação à ciberdefesa e declarou o ciberespaço como mais um domínio das operações, que deve ser defendido com a mesma efetividade que o terrestre, o marítimo e o aéreo. A NATO considera que assim melhorará a sua capacidade de dissuasão e de defesa. No mesmo comunicado, a NATO reafirmou o seu compromisso em atuar de acordo com legalidade internacional no ciberespaço (NATO, 2016f). Portanto, para a NATO atingir os objetivos que fixou devem concorrer dois elementos: manter a capacidade de dissuasão alargada no ciberespaço e atuar de acordo com a legalidade internacional. A estrita observância do segundo condicionará a liberdade de ação para atingir o primeiro. É nesta necessidade de compatibilização que se coloca o problema de investigação.

Verifica-se assim que as divergências interpretativas quanto à aplicabilidade do Direito Internacional no ciberespaço, especialmente no domínio do *jus ad bellum* e do *jus in bello* excedem o simples debate teórico ou académico e constituem uma questão de máximo interesse político e estratégico, porque o nível de aceitação internacional de cada postulado já está a condicionar a exequibilidade das estratégias de segurança e defesa no ciberespaço. O impacto deste processo de evolução da interpretação normativa é especialmente relevante no domínio da dissuasão, cujas componentes serão potenciadas ou

enfraquecidas à medida que evolui a doutrina do Direito Internacional no ciberespaço (CCDCOE, 2015; Nye, 2017 e Bustelo, 2017).

Com este trabalho pretende-se que a capacidade de dissuasão no ciberespaço beneficie dos estudos que têm vindo a ser desenvolvidos em matéria de interpretação das normas de Direito Internacional Público aplicadas ao ciberespaço. Assim, o objeto de estudo deste trabalho de investigação é a influência do Processo do Manual de Tallinn na estratégia de dissuasão da NATO no ciberespaço.

A magnitude do espaço de conhecimento em que se coloca este objeto de investigação, na área de intersecção entre os domínios da Estratégia e do Direito Internacional Público, faz imprescindível uma delimitação apropriada.

Em termos espaciais e geográficos, o caráter global e transversal do ciberespaço, assim como o impacto que as decisões de Estados da mais variada relevância política e estratégica[1] têm demonstrado no domínio do Direito Internacional Público do ciberespaço, obrigam a uma abordagem do estudo a escala global, mas limitando os atores a considerar. Portanto, neste estudo só se abordará a dimensão interestatal da dissuasão, embora seja amplamente aceite que os efeitos das atividades dos atores não estatais continuarão a ter efeitos muito relevantes no ciberespaço (Jensen, 2012, pp.781, 782).

Em termos de tempo, o trabalho abrange desde antes do início do Processo até à Cimeira de Bruxelas de NATO em junho de 2018.

Em termos de conteúdo, o trabalho foca-se na dimensão prática, atendendo à praxe da dissuasão da NATO no ciberespaço. Contudo, é necessário cimentar previamente a investigação na dimensão teórica.

A abordagem jurídica do trabalho focar-se-á no quadro *jus ad bellum*, porque o quadro do *jus in bello* só deveria aplicar-se desde as primeiras hostilidades (Mulinen, 1987, p.7) e, nesse caso, a dissuasão teria falhado. Contudo a credibilidade das respostas deve ser avaliada também no segundo caso. No ciberespaço, esta avaliação é mais necessária do que noutros domínios, como o respeitante à utilização de armamento nuclear. Se a dissuasão nuclear falhasse, as consequências seriam catastróficas o que permite ao dissuasor avaliar os limites legais com mais flexibilidade sem perder credibilidade (Brodie, 1958, pp.23-24).

O objetivo geral a atingir com o trabalho é o seguinte: *compreender como o Processo do Manual de Tallinn influencia a estratégia de dissuasão da NATO no ciberespaço.*

[1] Por exemplo as declarações do representante de Cuba no do quinto GGE (Rodriguez, 2017).

Para atingir este objetivo, é necessário compreender como o TMP afeta os fatores determinantes para a exequibilidade de uma estratégia de dissuasão no ciberespaço. Tal compreensão deve levar a um grau de conhecimento que permita melhorar a opção de dissuasão que, combinando elementos punitivos e defensivos, constitua uma estratégia de dissuasão eficaz no ciberespaço (Klimburg, 2012, pp. 81-86).

Por forma a alcançar o objetivo geral, definimos os seguintes objetivos específicos:

OE1: Determinar como o Processo do Manual de Tallinn afeta as componentes da dissuasão no ciberespaço.

OE2: Determinar como o Processo do Manual de Tallinn afeta as opções de dissuasão no ciberespaço.

Em consequência, de forma a atingirmos o nosso objetivo geral, e resolver o problema que enfrentamos, identificamos a seguinte pergunta de partida:

Como é que o Processo do Manual de Tallinn influencia a dissuasão da NATO no ciberespaço?

A pergunta de partida leva a duas perguntas derivadas:

PD1 - *Em que medida o Processo do Manual de Tallinn contribui para superar as dificuldades específicas suscitadas com a aplicação de doutrinas de dissuasão no ciberespaço?*

PD2 - *Em que medida o Processo do Manual de Tallinn é compatível com a adoção de uma opção de dissuasão eficaz no ciberespaço?*

Para resolver o problema, adota-se um esquema de raciocínio hipotético dedutivo, assente numa metodologia de análise qualitativa e estratégia de estudo de caso, fundamentada em dados documentais. Com este fim, cria-se um *corpus* documental de fontes primárias que são analisadas com técnicas qualitativas de codificação aberta, com técnicas de análise relacional baseadas em grafos e com técnicas semiquantitativas de mineração de texto.

A elaboração de hipóteses sólidas será indispensável para a construção do modelo teórico na primeira fase do processo hipotético-dedutivo a desenvolver. Para orientar inicialmente este processo, e cientes da importância de não cair em ideias preconcebidas, formulam-se as hipóteses provisórias que se seguem:

HIP1 - *Os efeitos do Processo do Manual de Tallinn são distintos a nível de cada dificuldade de dissuasão no ciberespaço*.

HIP2 - *A compatibilidade do Processo do Manual de Tallinn com as opções de dissuasão no ciberespaço decorre do seu impacto sobre as dificuldades de dissuasão*

consideradas e da adoção de uma opção de dissuasão alinhada sinergicamente com os contributos que o Processo traz para ultrapassar cada dificuldade.

O relatório de investigação está estruturado em três capítulos, iniciando-se com uma introdução e finalizando com as conclusões. Consta também uma parte pós-textual que inclui a bibliografia e os anexos e apêndices.

O primeiro capítulo contextualiza o problema e fornece a base concetual e os fundamentos metodológicos.

A parte analítica inclui-se nos dois capítulos seguintes. O Capítulo 2 aborda o estudo na dimensão prática do impacto que o TMP teve na estratégia de dissuasão no ciberespaço. O Capítulo 3 dedica-se à procura dos contributos do Processo para com una opção de dissuasão eficaz. A fundamentação teórica destes capítulos inclui-se no Anexo A e nos Apêndices A e B.

O corpo do relatório finaliza com as conclusões.

A bibliografia está classificada em função da tipologia de fontes empregada, segundo o seguinte esquema:

- Metodologia da investigação
- Monografias.
- Trabalhos de investigação e artigos científicos e na imprensa especializada.
- Textos oficiais, textos legais e outras fontes primárias escritas.
- *Corpus* de fontes primárias da NATO codificadas e analisadas com R.
- Entrevistas e declarações.
- Páginas web e artigos.

1 Estado da arte, metodologia e conceitos estruturantes.

1.1 Estado da arte

A contextualização do trabalho obrigou a fazer uma profunda revisão da literatura nos dois domínios em que o trabalho se insere. Esta revisão foi complementada e orientada por três entrevistas exploratórias (Ágreda, 2017; Bascoy,2017 e Cubeiro, 2017) com as que se atingiram os domínios politico-estratégico, estratégico-operacional e jurídico.

No domínio político-estratégico, devemos começar por salientar que a forma de os atores internacionais perceberem a utilidade do ciberespaço é muito diversa: espaço para as operações de informação, janela para a espionagem, mais um domínio das operações, entre muitos outros. Por outro lado, em termos evolutivos, é possível estarmos a assistir a um processo de recondução do ciberespaço ao controlo estatal, em linha com o que acontece no mundo físico. Neste processo de renacionalização, os Estados pretendem recuperar o espaço perdido como provedores de segurança. Outros, como a China, perseguem um horizonte mais distante, como o de construir o seu próprio ciberespaço (Ágreda, 2017).

No subdomínio da dissuasão, reviram-se em primeiro lugar os clássicos da dissuasão de modo abrangente e por forma a determinar os conceitos estruturantes das teorias gerais da dissuasão. Cabe salientar aqui autores como Cimbala (1998, 2014 e 2016), Quackenbush (2011), Brodie (1958) e o prêmio Nobel Thomas C. Schelling (1966), entre outros. Este aspeto é muito relevante, pois a distorção que a dissuasão nuclear trouxe sobre um conceito tão antigo como a dissuasão tem colocado dúvidas sobre a exequibilidade da dissuasão no ciberespaço.

Revistas as teorias gerais da dissuasão, abordou-se o estudo da dissuasão no ciberespaço, e, sendo certo que nos últimos anos se tem escrito muito sobre o assunto, Martin Libicki continua a ser, na perspetiva do autor, a referência fundamental neste tema, cujos trabalhos, convenientemente complementados com os de outros autores na matéria, permitem fazer uma adequada conceptualização de variáveis e indicadores para atender aos objetivos perseguidos por este trabalho.

1.2 Modelo de análise. Metodologia

O balanço final da revisão da literatura permitiu postular que o modelo de raciocínio hipotético-dedutivo seria o mais apropriado para este trabalho. Porém, o posicionamento ontológico de partida, próximo do construtivismo, e o posicionamento epistemológico próximo do interpretativismo (Matias et al., 2016, pp.16-20), levaram a adotar, depois de

contextualizar o problema, o modelo postulado e uma estratégia científica de investigação qualitativa.

A estratégia qualitativa apresentou-se mais adequada, por ser a empregue em todos os trabalhos analisados sobre este assunto, e pela necessidade de desenvolver um importante esforço de concetualização para refinar o modelo teórico no qual assentará o processo dedutivo.

O desenho de pesquisa de estudo de caso é o que melhor viabiliza a consecução do objetivo estabelecido para este trabalho. Se analisarmos a definição de estudo de caso dada por Yin (2013) e Hijmans e Wester (2009), citados por Sampieri et.al (2014b, p.1) verificamos que se adequa ao objeto de estudo e aos objetivos da investigação. Assim, a evolução da estratégia de dissuasão da NATO sob a influência do TMP é suscetível de constituir um caso para estudar. Este desenho de pesquisa também é válido para a finalidade explicativa que perseguimos, uma vez que permitirá avaliar a solução do problema de investigação respondendo às seguintes questões: o quê? como? e porquê? (Saunders, Lewis e Thornhill, 2012, p.179).

O estudo adota um horizonte temporal longitudinal determinado pela evolução no tempo do objeto de estudo.

As técnicas empregues foram variadas, e algumas de elevada complexidade. Assim, para além da análise documental elementar de fontes secundárias, na análise do *corpus* de fontes primárias empregaram-se técnicas qualitativas mediante codificação aberta com a ferramenta RQDA (*R Qualitative Data Analisys*), técnicas de análise relacional baseadas em grafos com o pacote de *software igraph* para o ambiente R, e técnicas semiquantitativas de mineração de texto com o pacote de *software tm* também do ambiente R.

As fontes selecionaram-se fundamentalmente de entre documentos oficiais da NATO e dos seus Estados membros, de documentos de caráter não oficial, mas considerados referências na matéria, bem como de documentos de caráter técnico e científico deste âmbito, obtidos em repositórios de acreditada reputação e preferivelmente de autores de prestígio na matéria em questão.

Para a fase indutiva do percurso de investigação e para a análise na dimensão da prática internacional criou-se um *corpus* de fontes primárias integrado por documentos do repositório oficial da NATO na internet selecionados de acordo com os critérios seguintes:

- Encontravam-se incluídos nas seguintes categorias: *Press Releases*, *Speeches & transcripts* e *Oficial Texts*;

- Resultaram de uma pesquisa cuja primeira filtragem selecionou os documentos que incluíram no texto o termo *cyber*, e aqueles em que, pelo assunto abordado, seria previsível que esse termo aparecesse;
- Resultaram de uma análise dos parágrafos selecionados e dos parágrafos adjacentes, incluindo no *corpus* os documentos que mereciam ser codificados.

Tabela 1 - Número de documentos no *corpus* de fontes primárias por estádios de seleção

	Número de documentos por periodo					TOTAL
Tipo	**.19MAY07**	**19may07-31dic09**	**31dic09-07mar13**	**07mar13-08feb17**	**08feb17-10may18**	
NATO_Press_Releases	1110	445	490	682	40	2767
NATO_Press_Releases_cyber	1	9	13	18	8	49
NATO_Press_Releases_cod	1	7	11	9	5	33
NATO_Press_Releases_Nao_dice_cyber_cod	1	0	0	0	0	1
NATO_Speeches	2610	412	491	719	263	4495
NATO_Speeches_cyber	28	74	90	218	124	534
NATO_Speeches_cod	2	22	21	41	37	123
NATO_Oficial_Texts	745	48	44	45	14	896
NATO_Oficial_Texts_Cyber	5	7	14	12	8	46
NATO_Oficial_Texts_Cod	3	0	4	1	0	8
Total INICIAL						**8158**
Total preseleccionado						**629**
Total codificado						**165**

Fonte: (Autor, 2019)

Como se apresenta na Tabela 1, a aplicação deste critério a 8.158 documentos concluiu com a criação de um *corpus* de 165 documentos, referenciados no apartado "*Corpus* de fontes primárias da NATO codificadas e analisadas com R" da bibliografia.

Em relação ao percurso da investigação, numa primeira fase, hipotética e indutiva, refinou-se o modelo teórico.

Assim, partindo do quadro conceitual desenvolvido pelo mesmo autor (Bustelo, 2017, Apd-A e Apd-B) seguiu-se um processo de codificação aberta de conceção emergente (Sampieri et.al., 2014a, p.476), guiado pela teoria, mas permitindo a introdução de novos códigos quando necessário e sem cair na preconceção de categorias, para a que nos poderia conduzir uma codificação axial. Este processo permitiu afinar o modelo teórico segundo o exposto no subcapítulo seguinte.

Seguidamente, na fase de dedução e teste, procuraram-se relações e explicações (Saunders, Lewis e Thornhill 2012, p.580), na dimensão teórica e na dimensão da praxe internacional. Portanto, não se pretendeu neste trabalho testar as hipóteses por infirmação no sentido de Popper (1935, pp.9-16,57-73).

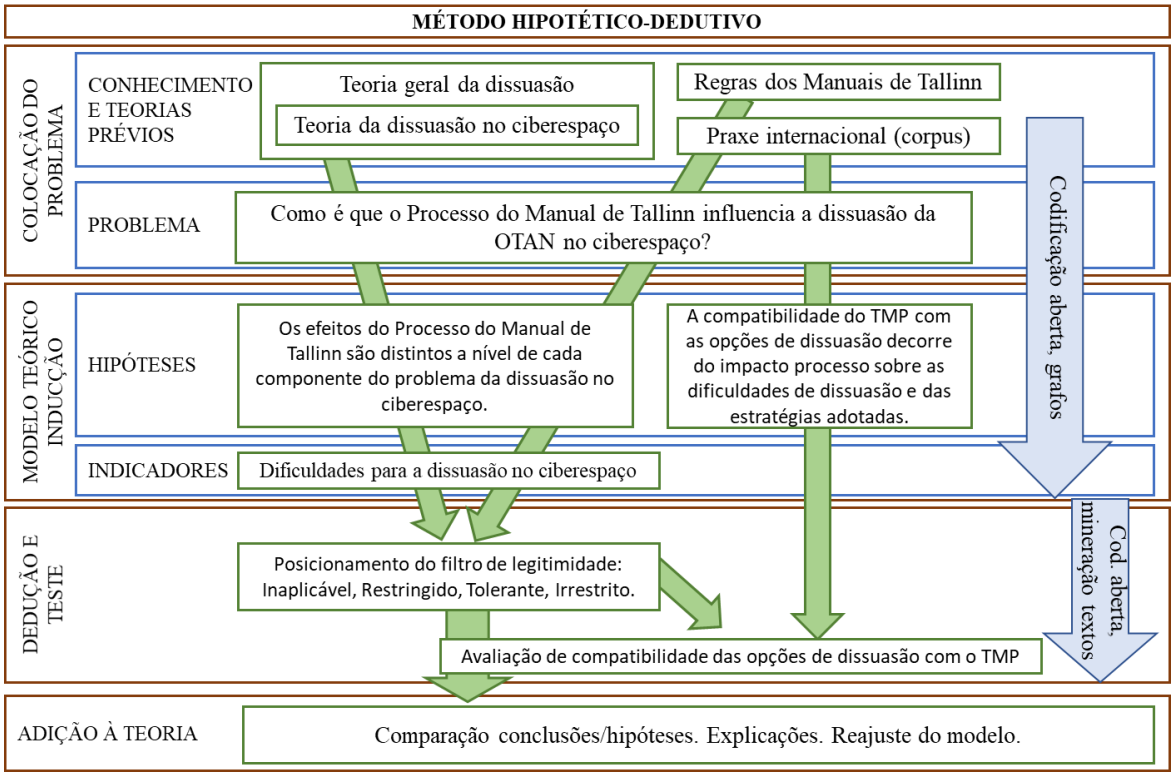


Figura 1 – Modelo de análise. Metodologia.

Fonte: (Autor, 2019)

1.3 Modelo de análise. Conceitos.

O estabelecimento da base conceitual da investigação não foi simples. O ponto de partida foi o esquema conceitual estabelecido pelo mesmo autor (Bustelo, 2017), sobre a base de uma profunda revisão da literatura, então para uma análise no plano puramente teórico. Naquele quadro conceitual era facilmente observável um elevado número de duplicidades na codificação e um elevado número de laços de realimentação entre conceitos, o que não levantava obstáculos de relevo para aquela tipologia de análise, mas podia tornar complexa demais a análise no plano de praxe das relações internacionais que se aborda neste trabalho.

Em consequência, o modelo inicial foi simplificado mediante um processo indutivo enquadrado na fase hipotética da investigação, cuja discussão se inclui no Apêndice A.

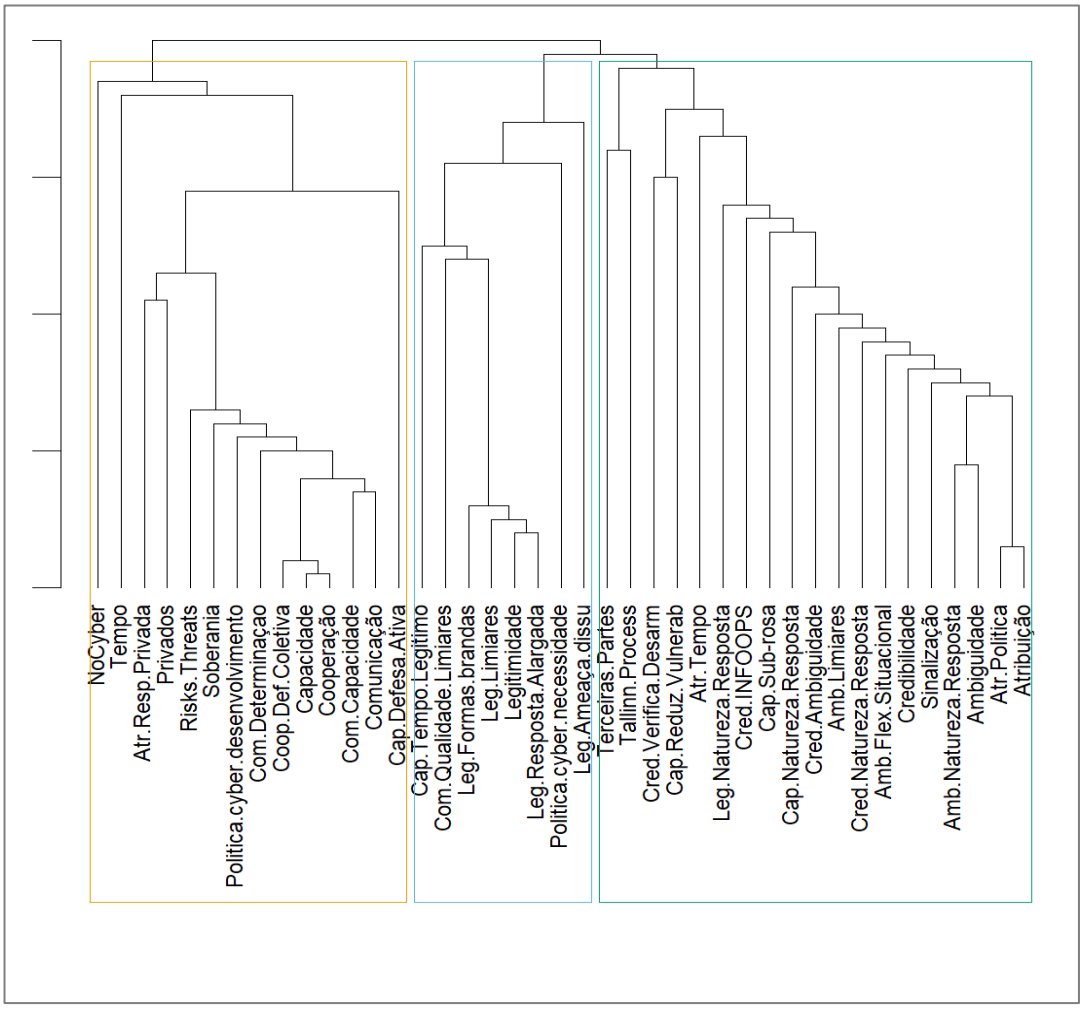


Figura 2 – Dendrograma: Análise de comunidades por modularidade da codificação inicial (Algoritmo Greedy).

Fonte: (Autor, 2019)

Uma vez efetuada a primeira codificação não exaustiva das fontes primárias analisadas (Tabela 1), procedeu-se à análise relacional de códigos mediante grafos[2] com o pacote *igraph* do R. A característica mais relevante do resultado foi a baixa correlação da estrutura categorial de variáveis e indicadores com a estrutura modular das relações entre códigos determinada pelas relações de solapamento dos textos codificados (Figura 2).

Depois de vários ciclos de refinamento da codificação, obteve-se um modelo mais simples passando de 52 para 36 indicadores no quadro teórico. A redução de códigos potenciais seria de 68 para 49. Contudo apenas se refletiam no plano prático 41 e 44 códigos respetivamente. Para além desta simplificação, o novo esquema de codificação permitiu aplicar uma codificação exaustiva, sem afetar a análise prática. A estrutura

[2] O Apêndice D inclui o *software* que se desenvolveu com este fim.

modular do novo esquema de codificação era mais clara e refletia melhor as grandes linhas teóricas da dissuasão (Figura 3).

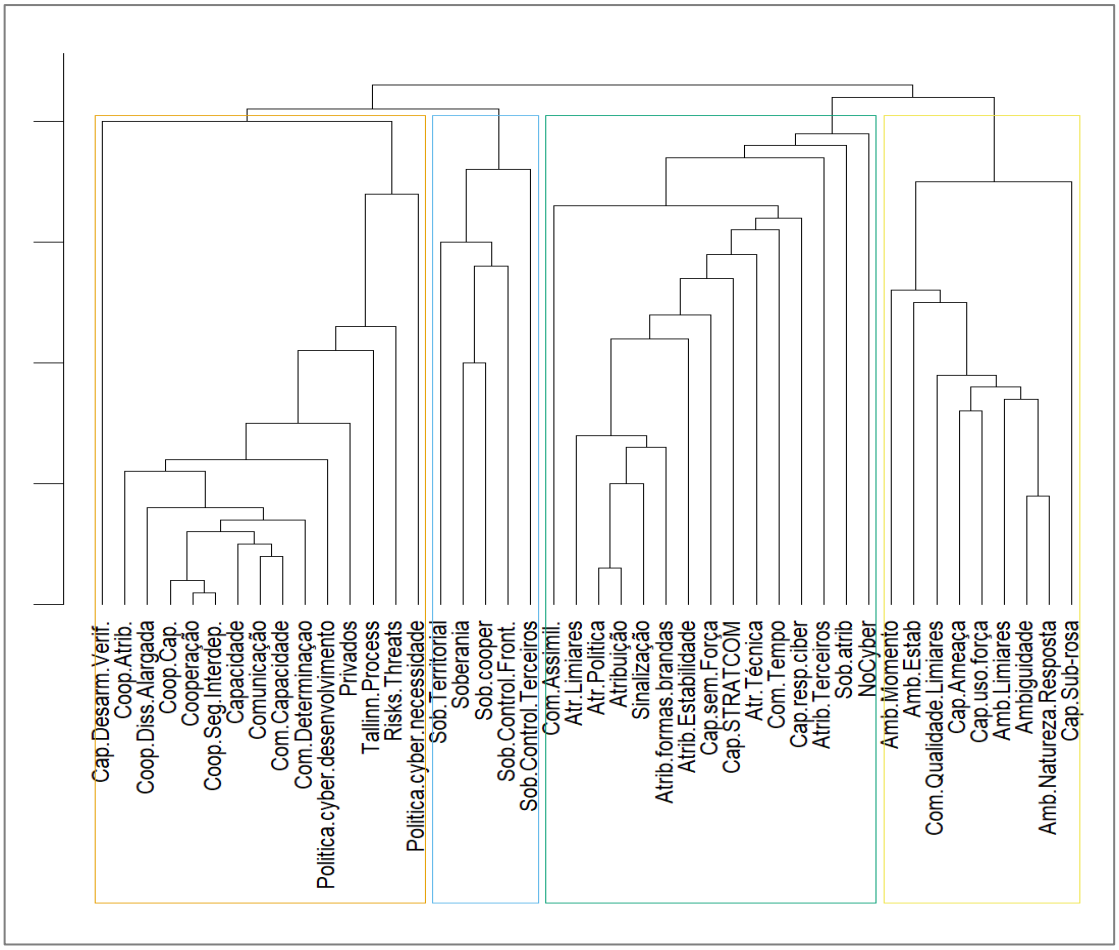


Figura 3 – Dendrograma: Análise de comunidades por modularidade da codificação final (Algoritmo Greedy).

Fonte: (Autor, 2019).

Como resultado deste processo indutivo de afinamento da base teórica, evidencia-se que, quem quiser manter a capacidade de dissuasão alargada no ciberespaço atuando de acordo com a legalidade internacional deve encontrar antes resposta às perguntas clássicas apresentadas na Figura 4.

O afinamento destas respostas permite orquestrar, para os fins deste trabalho, os conceitos teóricos básicos sintetizados pelos estudiosos da dissuasão, tanto geral como específica do ciberespaço. Esta conceptualização constitui a base conceitual do estudo[3], estruturada em três níveis:

1. Conceitos estruturantes de primeiro nível: variáveis dependentes.

[3] O mapa conceitual está incluído no Apêndice C.

2. Variáveis independentes e intervenientes: modulam os conceitos estruturantes de primeiro nível.
3. Indicadores: facilitam a avaliação da evolução das variáveis.

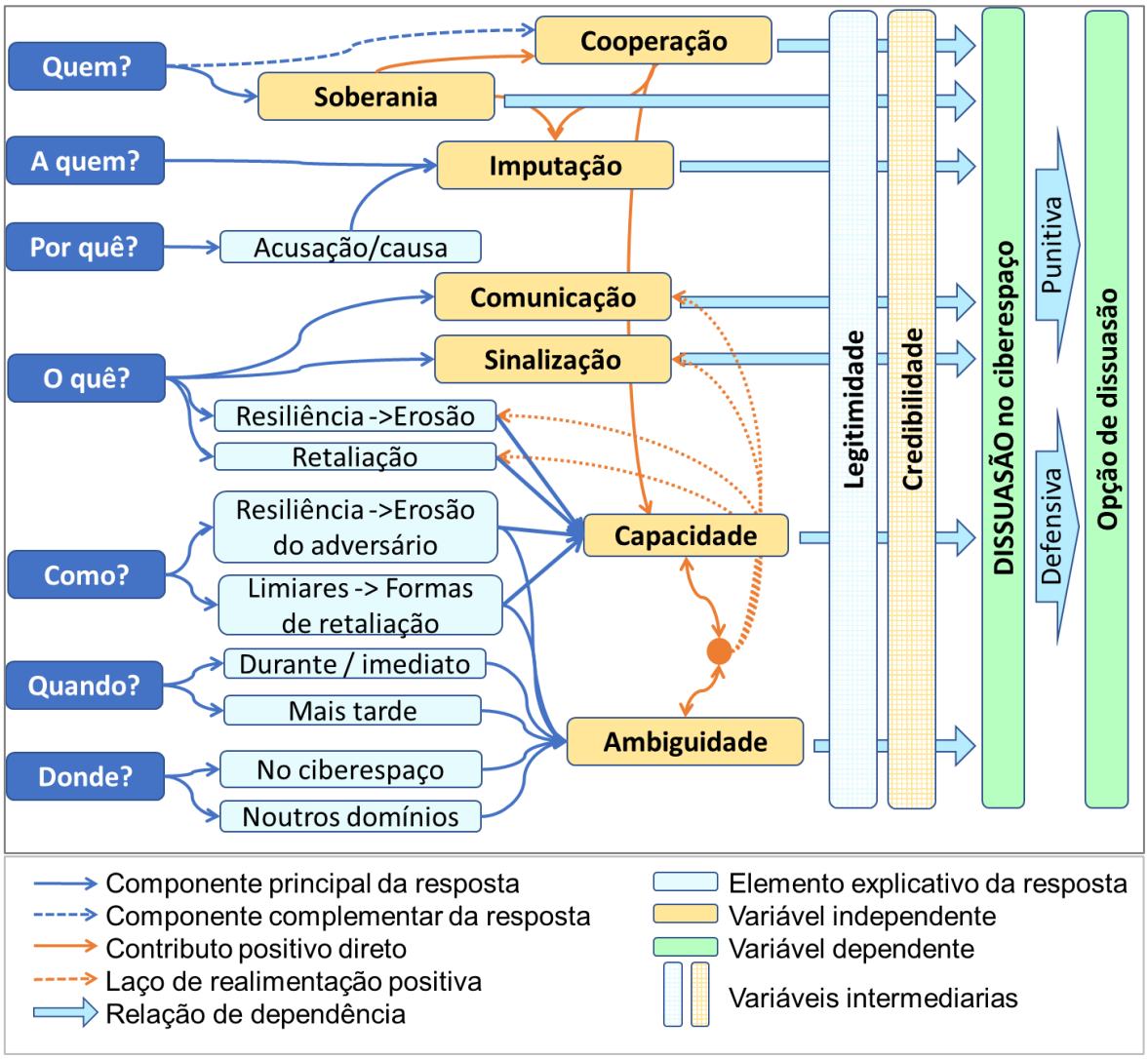


Figura 4 – Obtenção dos conceitos estruturantes e variáveis para uma estratégia de dissuasão eficaz.

Fonte: (Autor, 2019)

Os conceitos estruturantes de primeiro nível, apresentados a seguir, são constituídos pelo objetivo estratégico (a dissuasão no ciberespaço), e pelas opções estratégicas fundamentais para o atingir, resultantes da combinação de resiliência e retaliação potencial.

Dissuasão: estratégia de prevenção da ação adversária pelo medo das consequências que, envolvendo necessariamente capacidades ou intenções militares, cria no adversário um estado de espírito, potencial ou real, decorrente de uma ameaça credível de ação contrária e de consequências inaceitáveis ou decorrente da perceção de que é impossível atingir qualquer ganho capaz de motivar a sua ação (Bustelo, 2017).

Desta definição segue-se a necessidade de definir as duas modalidades básicas de dissuasão.

Dissuasão por represália ou punitiva: estratégia de prevenção da ação adversária pela criação nele de uma expectativa de punição de custos superiores aos ganhos que possa prever. Esta estratégia não é capaz de impedir que o adversário obtenha o ganho decorrente do ataque, porque assenta na ameaça de punição, mas dissuade-o de atacar (Snyder, 1960, p. 163).

Dissuasão por negação ou defensiva: estratégia de prevenção da ação adversária pela criação de uma perceção, pelo adversário, de que há uma capacidade credível para lhe negar qualquer ganho capaz de motivar a sua ação (Davis, 2014, p. 2). Aqui o papel da perceção é fulcral, ao contrário do verificado na definição originária de Snyder (1960, p. 163).

Opção de dissuasão: consiste na combinação de elementos dissuasórios adotada para um caso concreto. Uma estratégia de dissuasão eficaz deve combinar elementos dissuasórios punitivos e defensivos.

Para valorar corretamente a dissuasão desde o ponto de vista da NATO devemos diferenciar a dissuasão alargada da dissuasão central, embora estas estejam estreitamente relacionadas (Snyder 1961 cit. por Quackenbush, 2011, p. 4):

Dissuasão alargada: estratégia de prevenção da ação adversária cujo objetivo se alarga para defender os aliados. (Gray, 2003, p. 13)

Dissuasão central: estratégia de prevenção da ação adversária cujo objetivo consiste em dissuadir um ataque direto contra o defensor, que normalmente se configura como um ataque sobre o seu espaço de soberania. (Gray, 2003, p. 13 e Quackenbush, 2011, p. 4)

Por fim, se considerarmos o domínio das operações em que se há de desenvolver a estratégia, devemos definir:

Dissuasão no ciberespaço: estratégia de prevenção da ação adversária no ciberespaço (Bustelo, 2017).

Dos conceitos estruturantes expostos adotaremos as seguintes variáveis dependentes:

- **Dissuasão no ciberespaço**;
- **Opção de dissuasão**;

que deverão ser sempre avaliadas em sintonia com o quadro conceitual apresentado neste subcapítulo.

No segundo nível encontram-se as variáveis independentes e intervenientes.

Observando novamente a Figura 4, podemos verificar que as respostas para as sete perguntas implícitas num problema de dissuasão com a premissa de legalidade são o ponto de partida para definir os elementos da estratégia. Elementos que apenas no caso de ultrapassar com êxito a filtragem de legitimidade e credibilidade poderão ser aplicados para atingir com sucesso o objetivo dissuasório desejado.

As relações entre estes elementos, candidatos a variáveis independentes, permitem encontrar dependências causais entre alguns deles, o que obriga a introduzir variáveis intervenientes (Sampieri et.al, 2014, pp. 112, 113, 474) e sugere a aplicação da teoria de sistemas para abordar a análise.

Porém, uma abordagem sistémica complicaria imoderadamente o estudo pelo que é necessário simplificar o modelo teórico (Calduch, 2014, pp.70-74), dentro do compatível com os objetivos da investigação. A estrutura de relações observável na Figura 4 apenas apresenta relações diretas, pelo que todos os ciclos de realimentação são positivos. Portanto, é possível afirmar sem risco de errar que o contributo positivo para qualquer elemento de dissuasão considerado será positivo para a variável dependente. Estamos então perante uma estrutura de círculos virtuosos múltiplos (Aracil e Gordillo, 2005, pp.33-38), cuja natureza teórica é instável, mas que na realidade sempre encontra uns limites estabilizadores, neste caso as filtragens de legitimidade e credibilidade. Em conclusão, é válido imputar a condição de variáveis independentes aos candidatos propostos, sendo o seu valor final reajustado, para maior exatidão, com a adição de contributos procedentes de outras variáveis, segundo o esquema da Figura 4.

Adotamos as seguintes variáveis independentes:

- **Soberania**: Atributo superior dos Estados, que se traduz no não reconhecimento de qualquer autoridade externa como superior à sua no interior do seu território. Inclui a capacidade de estabelecer relações com outros Estados.
- **Imputação**: Atribuição de responsabilidade por um ato. No contexto deste trabalho, assenta no processo capaz de determinar a identidade e a localização do atacante original (atribuição perfeita), de um intermediário (atribuição imperfeita) ou de um responsável político (imputação política).
- **Cooperação**: Ação de colaborar com diversos atores, não necessariamente Estados, que assente no princípio da soberania obedece ao princípio do consenso e tem subjacentes objetivos políticos.

- **Comunicação**: Ação de transmitir, e o adversário assimilar, os limiares, a capacidade e a determinação de executar a ameaça dissuasória, abrindo a possibilidade de um confronto violento, mas sem fechar a porta à negociação
- **Sinalização**: Conjunto de atitudes e atos que indicam ao adversário a nossa intenção, de forma a estabelecer um jogo colaborativo em que, mediante pequenos sinais alternativos, os adversários consigam coordenar um desvio progressivo da direção que os pode levar a ultrapassar o limiar desencadeante das hostilidades.
- **Capacidade**: Disponibilidade de meios capazes de produzir um efeito desencorajador no adversário e factibilidade legal e, ou, política de os empregar.
- **Ambiguidade**: Incerteza induzida no adversário para lhe dificultar a valoração do risco em relação ao benefício que pudesse obter. Contribui para a estabilidade garantindo uma faixa de segurança em torno dos limiares de represália.

Adotamos as seguintes variáveis intervenientes e transversais:

- **Legitimidade**: Atributo do poder e do seu exercício que assenta na crença de legalidade e de respeito pelos valores legais.
- **Credibilidade**: Verosimilitude da intenção declarada e da determinação e firmeza para proteger um determinado interesse.

A justificação teórica para a adoção destas variáveis, e a fundamentação para a determinação de indicadores, encontra-se em Bustelo, (2017, Apd-B), que se inclui no Anexo A.

O mecanismo causal para determinar como o TMP influencia a estratégia de dissuasão da NATO no ciberespaço é o seguinte: o TMP altera o filtro de legitimidade e, portanto, modifica os limites aceitáveis e credíveis para os elementos constituintes da estratégia de dissuasão (variáveis independentes). A estratégia de dissuasão apenas se pode construir sem ultrapassar esses limites, que a condicionam. Em consequência, é suficiente medir a cota superior dos elementos de dissuasão legitimados. Mas tal medição não é simples, porque as variáveis consideradas são multifacetadas e cada faceta, doravante designada como indicador, deve ser avaliada individualmente. Estes indicadores constituem o terceiro nível do esquema conceitual e permitem operacionalizar as variáveis, partindo das noções teóricas sobre os problemas que apresenta a dissuasão no ciberespaço, para atribuir às variáveis o valor mais objetivo que for possível. No plano teórico, a medição categorial é a mais adequada para este objetivo. Assim, estabelecem-se as seguintes categorias:

- Inaplicável: o filtro de legitimidade não permite empregar o elemento de dissuasão.
- Restringido: o filtro de legitimidade coloca muitas dificuldades para empregar o elemento de dissuasão, pelo que só será possível empregá-lo de forma muito limitada.
- Tolerante: embora o filtro de legitimidade coloque limitações relevantes, o elemento de dissuasão pode ser empregue com efeitos dissuasórios relevantes.
- Irrestrito: o filtro de legitimidade não apresenta limitações relevantes para a aplicação do elemento de dissuasão.

2 Evolução da dissuasão ao abrigo do Processo de Tallinn. Dimensão prática.

Ao longo deste capítulo estuda-se a evolução da estratégia de dissuasão da NATO no ciberespaço em constante comparação com os três marcos principais do TMP. Não se trata de estabelecer uma relação causal, mas sim de verificar se existe uma certa correlação, entre a filtragem de legitimidade estabelecida no plano teórico e a implementação prática da estratégia de dissuasão da OTAN no ciberespaço.

Portanto, o ponto de partida para abordar o estudo apresentado neste capítulo é a avaliação teórica dos elementos dissuasórios que podem ser incluídos numa estratégia dissuasória de legitimidade compatível com as teses dos manuais de Tallinn. A discussão destes assuntos e a atribuição de valores categoriais às variáveis independentes na dimensão teórica é apresentada no Apêndice B.

2.1 Soberania e renacionalização do ciberespaço

Em termos de soberania, a análise terminológica comparativa dos quatro períodos em estudo (Figura 5) reflete um salto qualitativo significativo no começo do Processo de Tallinn.

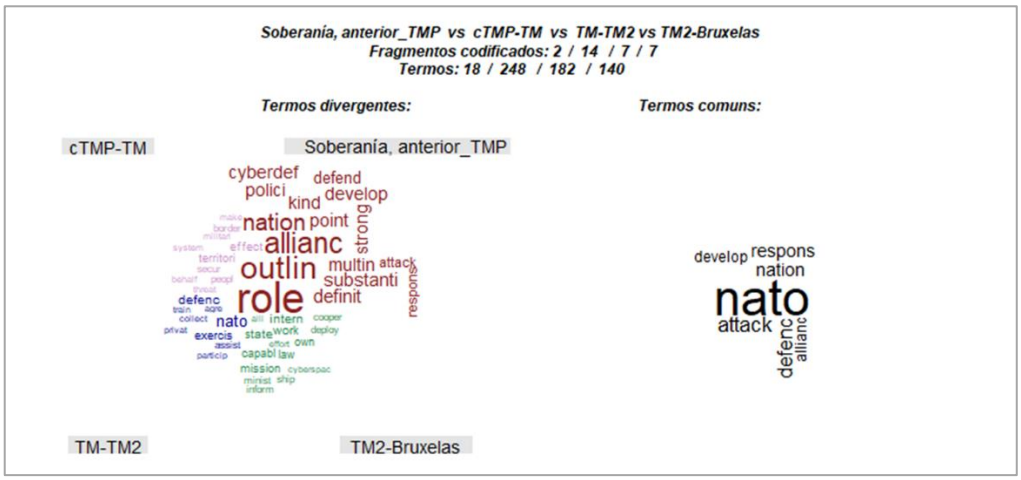


Figura 5 – Soberania: análise terminológica comparativa dos quatro períodos[4].

Fonte: (Autor, 2019)

[4] As nuvens de análise comparativa refletem graficamente o resultado da análise semi-quantitativa dos termos empregues nos fragmentos de texto selecionados qualitativamente no corpus analisado.

No cabeçalho indicam-se os períodos considerados, e o número de fragmentos de texto selecionados em cada período, também o número de termos significativos no total de fragmentos de cada período.

Depois há duas nuvens de palavras, calculadas segundo o algoritmo do Apêndice E. Estas nuvens são em realidade mapas de frequências (no sentido matemático do termo).

A nuvem da esquerda reflete a divergência terminológica entre períodos: O tamanho de um termo é maior quanto maior é o desvio da frequência de aparição desse termo no subgrupo em que se apresenta respeito à sua frequência de aparição no conjunto de subgrupos. A posição angular é determinada pelo subgrupo onde a frequência do termo é máxima. A cor facilita a leitura, identificando o subgrupo.

A nuvem direita reflete os termos mais comuns em todos os períodos. O tamanho do termo é maior quanto mais frequente é o termo.

Assim, antes do começo do TMP o papel da soberania na ciberdefesa era difuso e procurava-se o seu ajuste[5]. Esse papel era considerado "multinacional por definição" (Appathurai, 2007b) ou antes uma "responsabilidade nacional" para a qual a NATO teria de perfilar um modo de contribuir (Scheffer, 2008c). A primeira proposta significativa para aclarar este papel foi a de pré-delegação de autoridade na NATO segundo umas SROE concordadas (NATO, 2010a), afirmando assim implicitamente a soberania dos Estados no ciberespaço quase desde o começo do TMP.

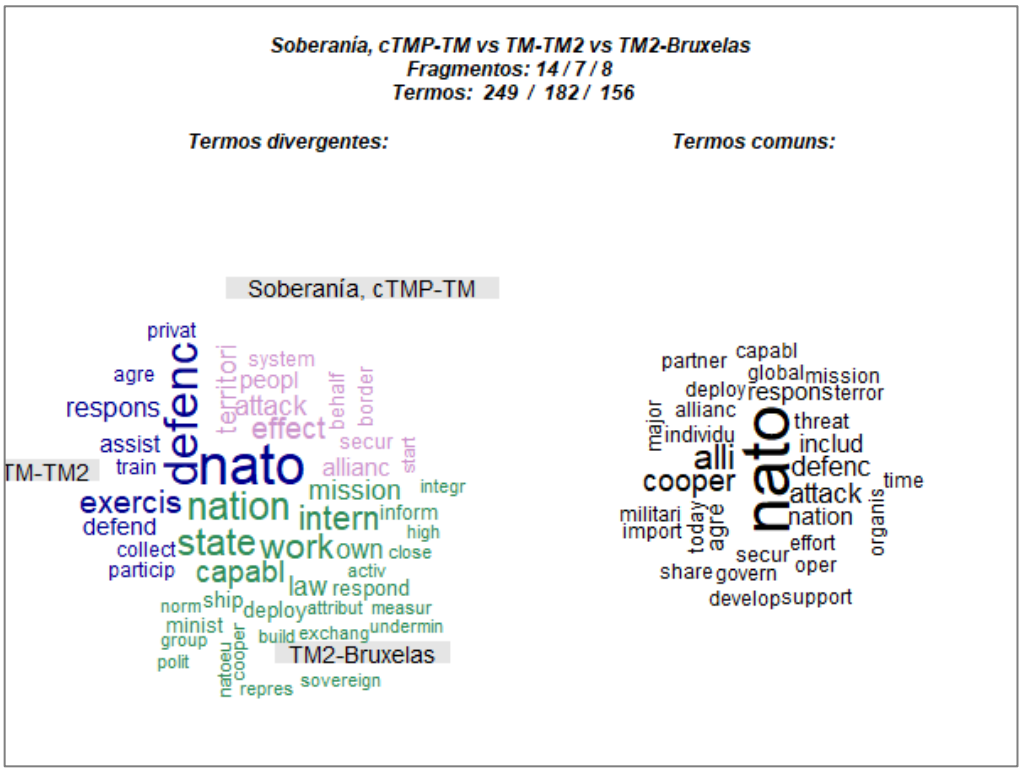


Figura 6 – Soberania: análise terminológica comparativa desde o começo do TMP até à cimeira de Bruxelas.

Fonte: (Autor, 2019)

Antes do começo do TMP, o vínculo territorial para aplicar a soberania no ciberespaço também não estava claro. O que estava claro era o facto de que a defesa da NATO demandava atuar além das fronteiras geográficas e no ciberespaço, o que se

[5] Retornando à figura 5, os termos "*outlin*" e "*role*" são muito pouco comuns no total do período analisado, o que se verifica ao observar que não aparecem na nuvem *Termos comuns*. Porém, estes termos são muito mais comuns na primeira etapa do período do que nas etapas seguintes, como se observa pelo seu tamanho e cor na nuvem *Termos divergentes*. Assim, aquela foi uma etapa de "delineamento de papeis" em que os termos empregues no contexto da soberania foram significativamente diferentes dos empregues nas três etapas seguintes (observe-se o grande tamanho dos termos nesta etapa em contraste com o tamanho pequeno e uniforme dos termos nas três etapas seguintes).

apresentava como uma forma de tornar mais eficaz a defesa territorial clássica no processo de necessária transformação da NATO, e não como uma forma de ampliação da área de operações (Rasmussen, 2010f; Rasmussen, 2010g; NATO, 2010d). Contudo, o vínculo territorial do ciberespaço ainda estava indeterminado (Rasmussen, 2011b) e parecia quase não existir.

A questão do controlo fronteiriço teve o seu período alto desde o começo do TMP até à publicação do TM, onde se abordaram as dificuldades técnicas para efetivar o controlo fronteiriço salientando o papel da cooperação e da NATO para as mitigar (Rasmussen, 2010a; Rasmussen, 2010c) (Figura 6). A publicação do TM não envolveu uma vindicação imediata da soberania sobre o ciberespaço, e a assunção da difícil efetivação de um controlo fronteiriço eficaz começou a esboçar uma fronteira mais abrangente (Rasmussen, 2013c), uma fronteira de segurança. Nas proximidades da Cimeira de Varsóvia, e da publicação do TM2, a NATO alargou o leque de ameaças desrespeitosas das fronteiras que mereciam a sua atenção e voltou a enfatizar a necessidade de projetar estabilidade para além das suas fronteiras (Stoltenberg, 2016b).

Nos inícios do Processo também mereceram atenção as dificuldades de imputação decorrentes do papel de terceiros (Shea, 2010), mas seria depois da publicação do TM que se tornou mais explícita a responsabilidade nacional na segurança do ciberespaço e a necessidade de cooperação com o setor privado (Rasmussen, 2013c). O TM já apontara para a responsabilidade estatal pelos atos de terceiros.

Em termos de compatibilidade das prerrogativas da soberania com a imputação, a abordagem inicial do problema como uma questão transnacional onde a cooperação era imprescindível (Appathurai, 2010; Rasmussen, 2010h) foi delineando a forma de ultrapassar as dificuldades de imputação inerentes à multiplicidade jurisdicional presente em quase todos os ciberincidentes. Contudo, foi na Cimeira de Bruxelas que a NATO explicitou a imputação como uma prerrogativa da soberania nacional (NATO, 2018d), o que, para além de ser coerente com a regra 1.10 do TM2, que não reconhece estas prerrogativas às organizações internacionais, habilita a NATO a intervir sem assumir o risco de imputar.

Em termos de compatibilidade com a cooperação, a premissa da responsabilidade nacional da ciberdefesa não foi impedimento, quer para a procura permanente de formas de cooperação entre os membros da NATO, quer para a procura de vias para a NATO acrescentar o valor da ciberdefesa individual e coletiva. Sem renunciar à soberania de cada Estado, foram estabelecidos os mecanismos de cooperação e intercambio de informação

em tempo real dentro da NATO e, segundo se anunciou pouco depois de publicado o TM2, também entre os centros de resposta da NATO e da UE (Stoltenberg, 2017g). Também seria depois da publicação do TM2 que se aprofundaria nas formas de os Estados exercerem a soberania colocando cibercapacidades sob controlo da Aliança, como acontece com outros tipos de capacidades (Stoltenberg, 2017l). Assim na Cimeira de Bruxelas concordou-se como integrar o "ciberefeitos soberanos" nas operações da Aliança (NATO, 2018d).

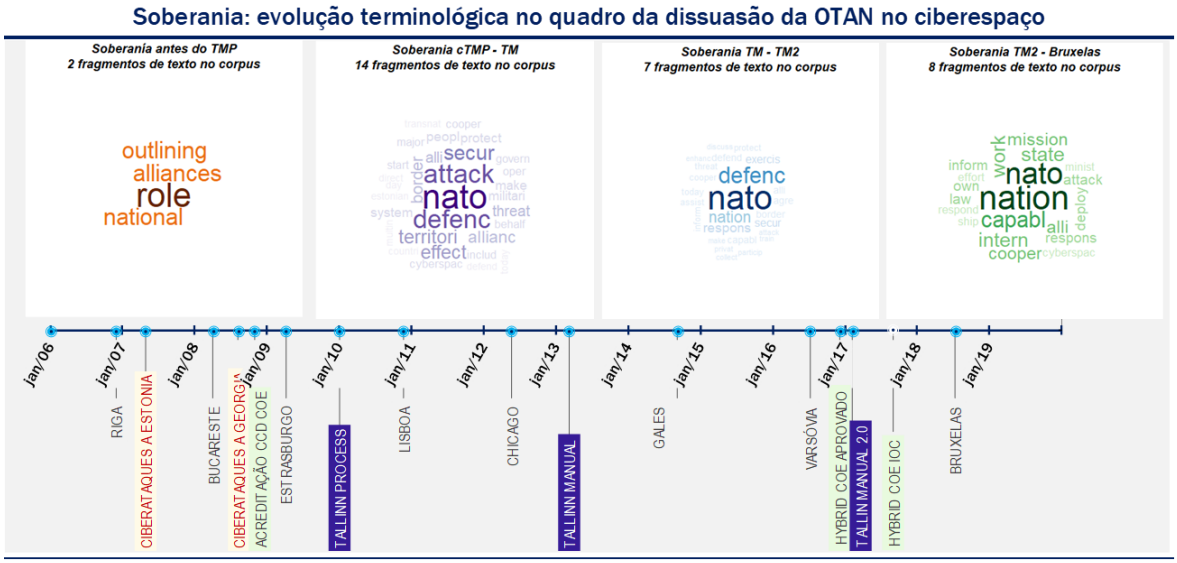


Figura 7 – Soberania: evolução terminológica[6] no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

Em conclusão, observou-se uma clara evolução do conceito de aplicação da soberania no quadro da estratégia da NATO no ciberespaço, que se reflete com claridade na análise terminológica decorrente da codificação do *corpus* de fontes primárias analisado (Figura 7).

Antes do começo do TMP, procurava-se encontrar o encaixe para os papéis da aliança e das nações frente a um problema de índole transnacional que ainda não era de grande interesse para a NATO. Na seguinte etapa, até à publicação do TM, a atenção focou-se no papel da Aliança frente aos ciberataques, na defesa territorial, nas fronteiras estatais e na fronteira de segurança. Depois da publicação do TM as responsabilidades

[6] Cada nuvem de palavras reflete os temas (termos significativos) mais abordados em cada período. Quanto maior é a frequência de um termo, maior é o seu tamanho na nuvem. As nuvens são calculadas com o algoritmo do Apêndice E. No cabeçalho de cada nuvem indica-se o número de fragmentos selecionados qualitativamente para cada período no corpus analisado.

nacionais na resposta frente aos ciberataques começaram a ganhar peso para atingir um papel fulcral depois da publicação do TM2, o que vem a confirmar a tendência para a renacionalização do ciberespaço que apontava Ágreda (2017).

2.2 A imputação na prática

A análise terminológica comparativa inicial (Figura 8) revela três aspetos importantes: uma notável focalização no conceito de ataque desde o começo do TMP até à publicação do TM, a identificação de um sujeito passivo da dissuasão depois da publicação do TM e a generalização, depois da publicação do TM2, de um novo conceito que reforça a imputação: "*hybrid*".

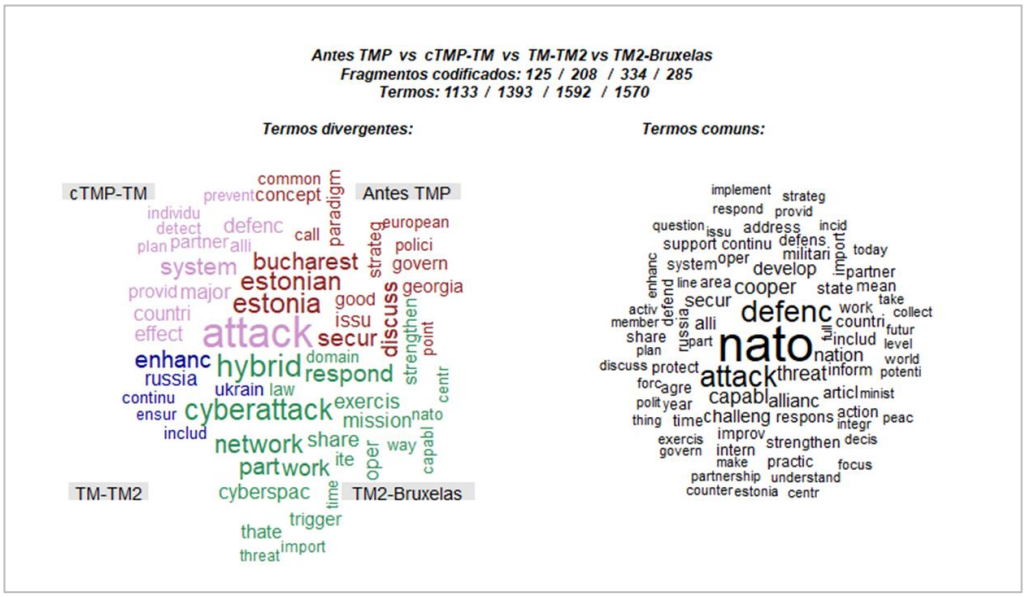


Figura 8 – Imputação: análise terminológica comparativa dos quatro períodos.

Fonte: (Autor, 2019)

O problema da imputação técnica e das interferências de terceiras partes foi abordado desde o começo do TMP (Shea, 2010), bem como a cooperação como caminho para ultrapassar os problemas de imputação técnica (Rasmussen, 2010d). Contudo, foi no ano da publicação do TM que se firmou o MoU do *Multinational Cyber Defence Capability Development*, que melhorou notavelmente os mecanismos de cooperação técnica (NATO, 2014a), contribuindo para ultrapassar algumas dificuldades de imputação. Também foi depois de publicado o TM que a NATO explicitou a determinação de atuar ainda em casos de imputação técnica imperfeita (Stoltenberg, 2015c). Já próximo da publicação do TM2, começou a contextualizar-se o problema ciber na guerra híbrida (Stoltenberg, 2016a), um contributo adicional para ultrapassar a imputação técnica imperfeita. Contudo, foi após a

publicação do TM2 que se generalizou a contextualização da questão ciber no domínio da guerra híbrida (Figura 9).

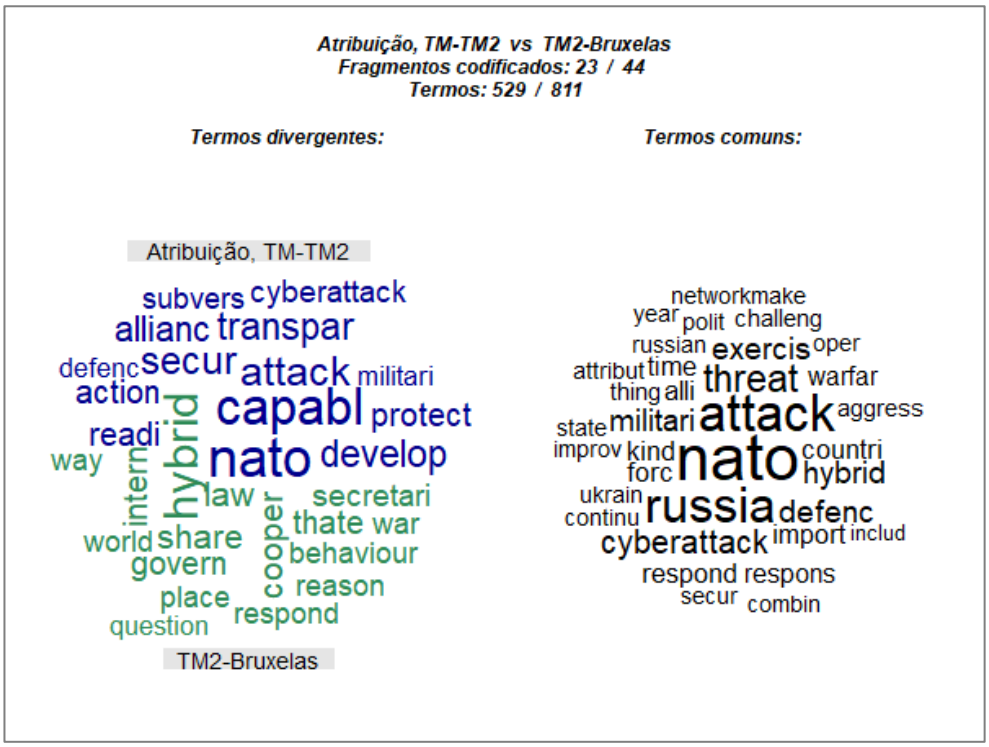


Figura 9 – Imputação: em torno da publicação do TM2.

Fonte: (Autor, 2019)

Assim, ao longo do processo foram-se estabelecendo os fundamentos para a imputação política.

A observação da Figura 10, levanta a questão de porque o termo *attack* atinge uma relevância tão elevada no *corpus* documental analisado depois de começado o TMP, quando apenas aparece nos dois anos mais próximos aos ciberataques a Estônia. Em todo o período próximo aos ciberataques[7] nenhum documento do *corpus* fez referência ao assunto na que se possa perceber alguma imputação dos ataques. O assunto ciber nem sequer se menciona na *NATO statement on Estónia*, (NATO, 2007a) e, quando questionada, a NATO elude responder (Appathurai, 2007a.). Fala-se nas caraterísticas dos ataques, mas não nas do atacante; fala-se da Rússia, mas sem a relacionar com os ciberataques (Appathurai, 2007b; Scheffer, 2007). Parece inexistente qualquer capacidade de imputação, nem sequer política. A questão muda subtilmente no caso da Geórgia, onde a NATO explicita, antes de os ciberataques terem finalizado, que contribuirá a esclarece-los (Scheffer, 2008g), mas

[7] Ocorridos entre 27/04/2007 e18/05/2007 (Artiles, 2010, p.178)

não se aprecia imputação alguma. Era necessário o debate sobre o que e como imputar, e o TMP alimentaria o debate.

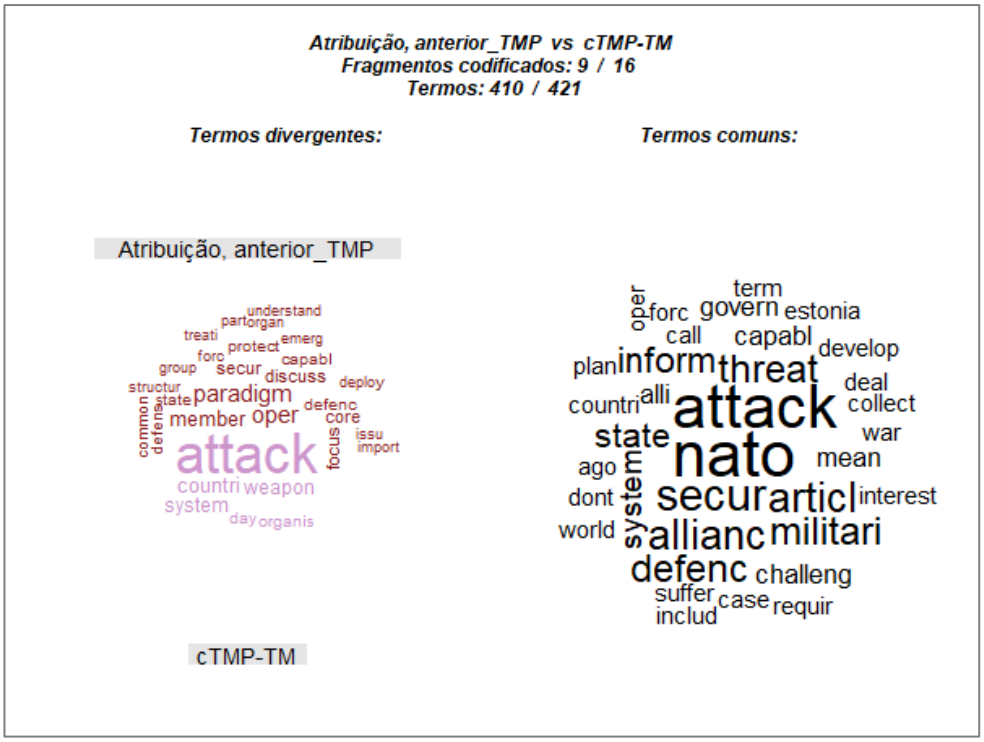


Figura 10 – Imputação: em torno do começo do TMP.

Fonte: (Autor, 2019)

Assim, foi depois de publicado o TM que apareceu no *corpus* analisado a primeira (Breedlove, 2014) de muitas imputações políticas a um Estado, Rússia (Figura 11). Na época do TM2, e do *Hybrid COE*, a imputação política continua, reforçada e contextualizada no quadro da guerra híbrida: "*First on the Russian … they are also active in cyber hybrid threats and actions against NATO Allied countries*." (Stoltenberg, 2017d).

Contra a estratégia híbrida de combinar agressões de distinta natureza que permite manter ao agressor um nível de negação elevado (Stoltenberg, 2017i), caso as agressões se considerem isoladamente, cabe a contextualização como instrumento para reforçar a imputação. Contudo, a imputação política mostra uma debilidade, serve para imputar atitudes agressivas globais que justificariam algumas respostas, mas falha para imputar ciberataques concretos, por exemplo o ciberataque à Letônia, coincidente com o *Russia Zapad 2017 Exercise*, ou os ciberataques às unidades alemãs na Lituânia (Stoltenberg, 2017i). Trata-se de imputar padrões de comportamento (Stoltenberg, 2018c; Stoltenberg, J., 2018d), não ciberataques concretos. O caráter indireto da imputação política também

não foi ultrapassado (Stoltenberg, 2017l). É um aliado que imputa e a NATO que aceita a imputação (NATO, 2018a; Stoltenberg e Johnson, 2018).

Finalmente, na cimeira de Bruxelas consolidou-se a posição de a imputação ser uma faculdade soberana de cada Estado aliado (NATO, 2018d), o que traz a vantagem de reduzir o desgaste político da NATO ao mesmo tempo que a legitima para responder.

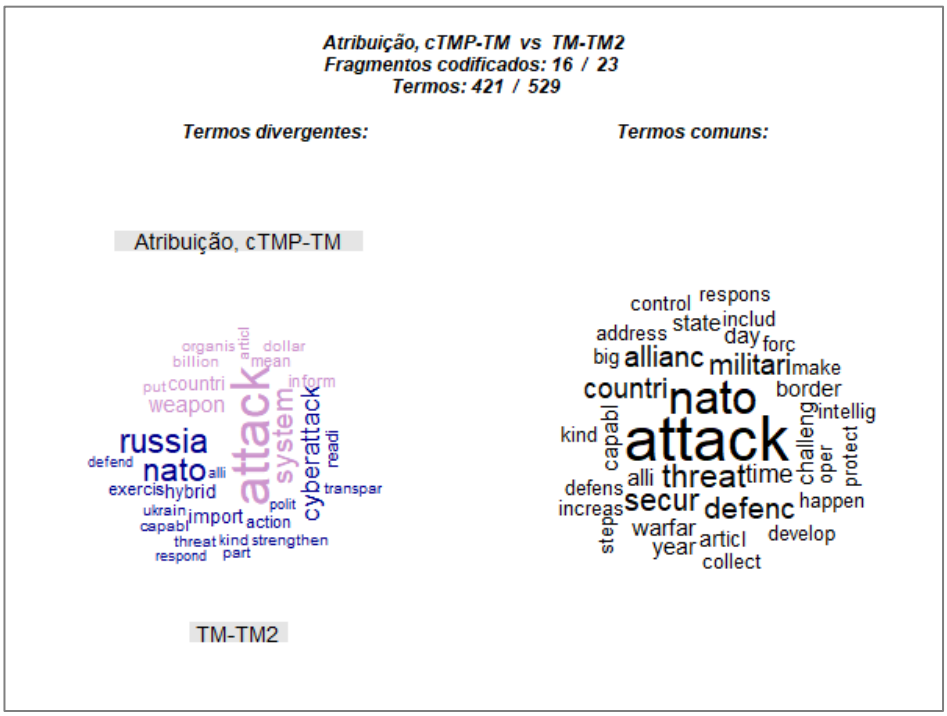


Figura 11 – Imputação: em torno da publicação do TM.

Fonte: (Autor, 2019)

A dificuldade de imputação facilita um elevadíssimo número de ciberataques de baixo nível, "*a new form of permanent, low-level warfare*" (Rasmussen, A.F., 2010e) que levou a NATO a procurar uma solução unificada ao problema desde os ciberataques à Estónia. Isto, unido à dificuldade prática de imputação aos Estados de atividades desenvolvidas por atores presumivelmente baixo o seu controlo, mantém alta a instabilidade no ciberespaço. (NATO, 2018a)

No começo do TMP a questão dos limiares de imputação no ciberespaço era inaplicável. Falava-se em "suicídio político" caso se abrisse o debate sobre a aplicação do Artigo 5 fora do contexto tradicional, em reinterpretar o Artigo 4 ou em orientar o assunto ciber pela via das sanções económicas (Wijk, 2009). Mas pouco depois de começado o TMP a questão dos limiares de imputação tinha progredido. Já se considerava a possibilidade de imputar ciberataques por cima do limiar de aplicação do Artigo 5 (NATO,

2010a) e se afirmava deles que "*they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability"* (NATO, 2010d; Rasmussen, 2010f). Ainda assim, o primeiro documento do nosso *corpus* que faz referência a ciberataques na escala de "ataques armados" é três meses posterior à publicação do TM (Vershbow, 2013).

O limiar do Artigo 5 seria estabelecido pela NATO explicita e oficialmente na Cimeira de Gales (NATO, 2014b).

Contudo, a indefinição dos limiares mais baixos obriga a um labor de comunicação importante que sensibilize a comunidade internacional para aceitar respostas neste contexto confuso de imputação.

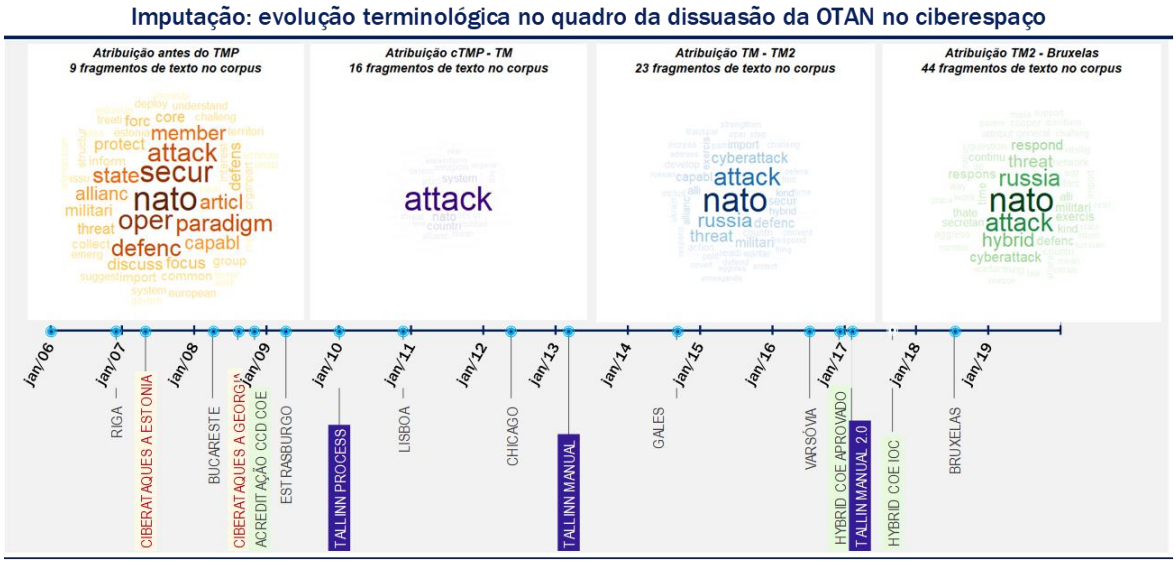


Figura 12 – Imputação: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

Na análise da evolução terminológica (Figura 12) é facilmente apreciável a grande diversidade terminológica que reflete o período exploratório em que se encontrava a NATO antes de o TMP começar. Era urgente encontrar uma solução para os problemas da imputação no ciberespaço. Começado o processo, o foco colocou-se no "que imputar". O TM trouxe muita luz ao assunto e abriu o caminho para a imputação política, que se começou a materializar sobre a Rússia. A necessidade de contextualização e de adicionar elementos de prova complementares a este tipo de imputação foi-se reforçando à medida em que evoluía o conhecimento das estratégias hibridas e se aproximava a publicação do TM2. Já na última etapa intensificaram-se as mensagens de imputação política à Rússia contextualizadas na estratégia hibrida que se lhe imputa.

2.3 Capacidade

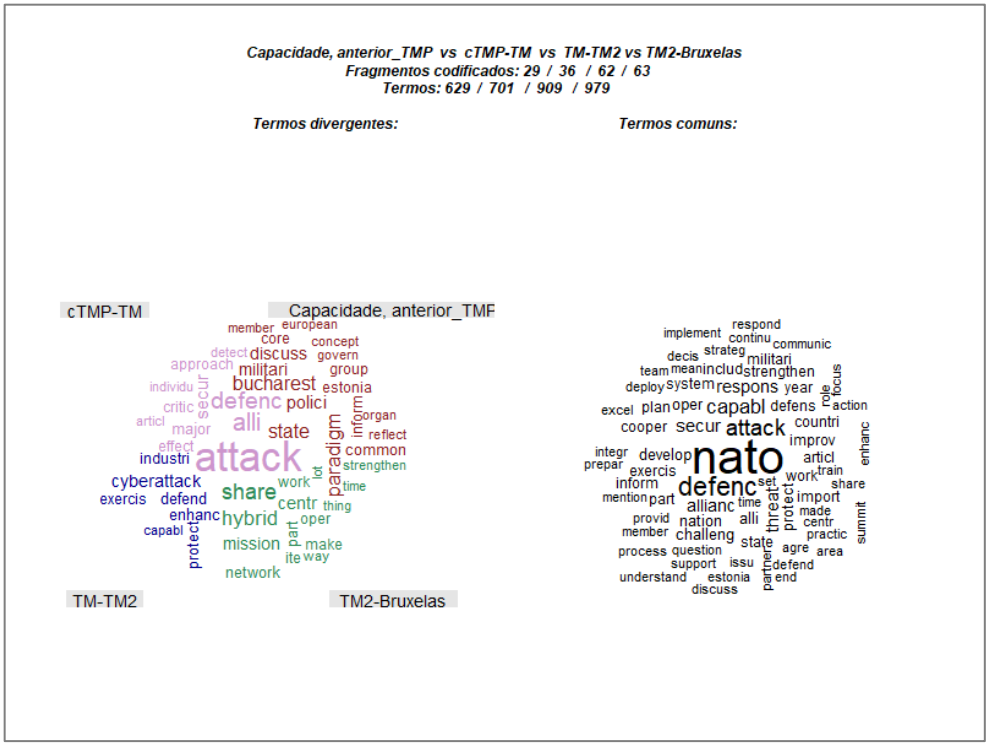


Figura 13 – Imputação: análise terminológica comparativa dos quatro períodos.

Fonte: (Autor, 2019)

No começo do processo a capacidade de ameaça era mínima (Shea, 2010) e não foi até à Cimeira de Gales que se materializou a capacidade de ameaçar com a invocação do artigo 5 (NATO, 2014b). A mensagem de que os ciberataques podem ativar a defesa coletiva foi persistente desde esse momento.

Em termos gerais, em todo o *corpus*, a ameaça do uso da força ou outras respostas não é explicita, nem orientada a um ator concreto, é apresentada como a resposta contra uma ameaça. Ainda depois de publicado o TM2, é mais comunicação do que ameaça (Stoltenberg, 2018d).

Em 2002 encontra-se a primeira referência explícita à quarta dimensão da guerra, a ciberguerra, e à necessidade de desenvolver capacidades para a ciberguerra no lado europeu da NATO (Naumann, 2002), embora haja documentos anteriores a considerar a ameaça de ciberguerra, por exemplo (Robertson, 2002). Contudo, seria poucos meses depois de publicado o TM que a NATO anunciava a capacidade operativa plena (FOC) das suas equipas de resposta ciber (Rasmussen, 2013c).

Porém, o passo adiante mais salientável no fortalecimento da capacidade de resposta no ciberespaço foi o seu reconhecimento como um domínio das operações, na Cimeira de Varsóvia (Stoltenberg, 2016b; Stoltenberg, 2016c). A consequência foi a atualização do

artigo 5, sem o reescrever, e a integração da dimensão ciber do conflito em igualdade de condições que as restantes (Stoltenberg, 2016j). Contudo, o primeiro reconhecimento pela NATO do emprego de ciberarmas ofensivas pelos seus membros que aparece no *corpus* é posterior à publicação do TM2 (Stoltenberg, 2017m), e foram empregues contra atores não estatais. A mesma conferência de imprensa serve para explicitar que a NATO empregará capacidades nacionais, baixo controlo nacional, para responder ofensivamente, para afirmar que os aliados da NATO já têm empregado com êxito estas capacidades e para anunciar que a NATO concorda a criação dum Centro de Ciber Operações na sua estrutura de comando. Para além das capacidades nacionais, a NATO contribui acrescentando outros valores como tecnologia, exercícios ou equipas de resposta a incidentes (Stoltenberg e Trudeau, 2018).

É de salientar, por quanto envolve de normalização das ciberoperações, o debate sobre a possibilidade de responder no ciberespaço a ilícitos cometidos no domínio físico e atribuídos apenas politicamente (Stoltenberg, 2018c).

Uma das vantagens da imputação política era a preservação de cibercapacidades próprias, pela desnecessidade de revelar as técnicas forenses. Esta será a única via de preservação de capacidades detetável no *corpus*, pois de se explicitar o emprego de cibercapacidades adiantadas ou ocultas em sistemas adversários, perderiam de imediato o seu valor, para além de colocar o proprietário em situação controvertida.

A capacidade de responder por debaixo do limiar do uso da força foi demonstrada desde antes do começo do TMP, embora apresentada como resposta a um padrão de comportamento inapropriado, sem concretizar em ciberataques e com medidas de alcance muito limitado. Foi o caso da suspensão de atividades ordinárias do *NATO-Russia Council* (NRC) em agosto de 2008 (NATO, 2008b). A necessidade de aplicar respostas coletivas, mas não militares, frente às novas ameaças foi abordado no processo de elaboração do Conceito Estratégico de 2010 (Scheffer, J.H., 2009). Naquela altura o Artigo 4 do Tratado de Washington apresentava-se como possível forma de resposta frente a agressões por debaixo do limiar da força e como via para ultrapassar as dificuldades que então apresentava o debate na aplicabilidade do Artigo 5 (Wijk, 2009). O objetivo era atingir uma capacidade de resposta em todo o espectro da crise (Rasmussen, 2010g).

A publicação do TM clarificou a questão dos limiares no plano teórico, e embora tenham sido aplicadas medidas de retorção mais intensas[8], estas não se tinham orientado a

[8] Sanções económicas, restrições ao comercio de armas e material de duplo uso, etc.

ilícitos concretos no ciberespaço, senão a um padrão de comportamento global (NATO, 2014b). A necessidade de treinar o nível político para decidir sobre este nível de baixa intensidade era evidente (Stoltenberg, 2015c), o que enlaça com o segundo pilar do TMP. Depois da publicação do TM2 a melhora da segurança e da resiliência continuaram a avaliar-se como a capacidade mais eficaz contra as formas brandas de agressão (Stoltenberg, 2018i). A novidade mais salientável foi a criação de uma nova capacidade, os "*counter-hybrid support teams*" (Stoltenberg, 2018k).

Por outro lado, a capacidade de comunicação estratégica, é uma importante via de resposta para elevar os custos do adversário em estratégias de tipo defensivo. É possível encontrar exemplos antes de começado o TMP (Shea, 2010), em relação à China. Contudo, seria depois do começo do processo que se explicitaram os riscos e ameaças que demandavam uma capacidade de resposta apropriada no domínio da informação (NATO, 2010a). Todavia, era necessário vindicar os princípios democráticos no ciberespaço, e convencer a muitos aliados do potencial das redes sociais (Babst, 2011). A necessidade de reforçar estas capacidades aumentou com a generalização das estratégias híbridas (NATO, 2014b). Depois de publicado o TM, o mecanismo continuou a ser o mesmo, evidenciar a atitude ofensiva e deslegitima do adversário, ao mesmo tempo que se destacava a eficácia própria autolimitada à defesa (Stoltenberg e Mikser, 2014).

Não se trata de combater a propaganda com propaganda, mas sim com dados certos (Stoltenberg, 2017i; Stoltenberg, 2017j). A legitimação do discurso próprio revela-se fulcral e a liberdade de discurso, apresentada como prova de veracidade, reforça a capacidade de comunicação de aqueles que a permitem frente aos que não (Stoltenberg, 2018i). Uma das vantagens práticas desta capacidade é que permite responder assentando as mensagens na imputação política indireta (Stoltenberg, 2017l).

A capacidade de resposta *sub-rosa*, é abordada escassamente no *corpus*, e não será até ao terceiro período em estudo que se explicite por primeira vez (NATO, 2016a) para enquadrá-la rapidamente na guerra híbrida (Stoltenberg, 2016e). Todavia, apenas se aborda como ameaça e não como capacidade de resposta.

Por fim, como era previsível, segundo a análise teórica, a questão do desarme e verificação nem sequer foi abordada desde pouco depois de começado o TMP (Shea, 2010).

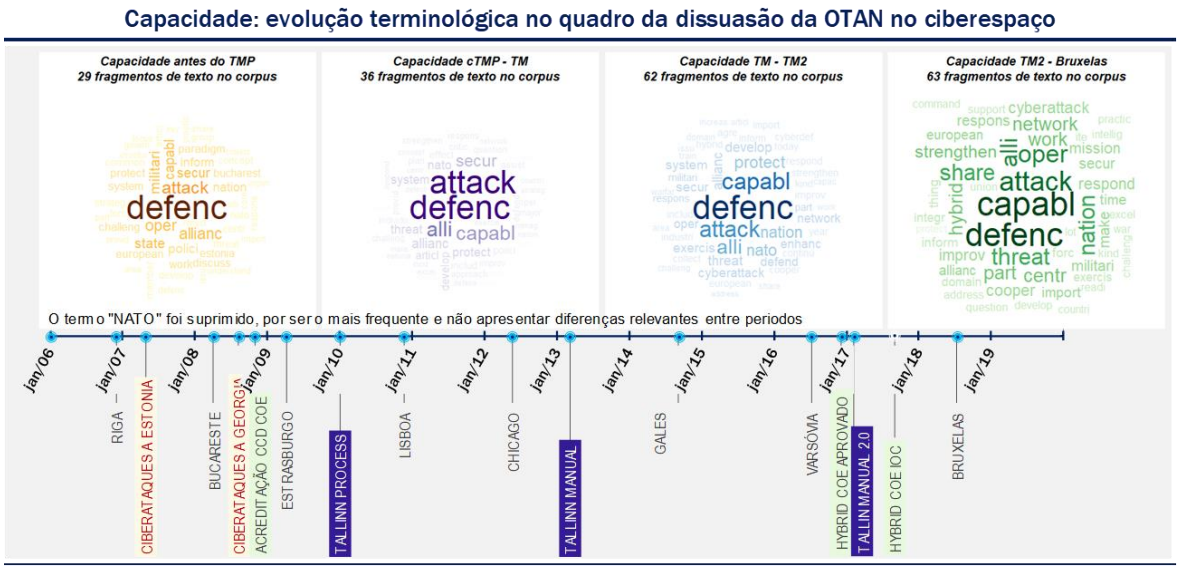


Figura 14 – Capacidade: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

Se nos parágrafos anteriores foram abordados os indicadores referentes à capacidade de resposta, na Figura 14 evidencia-se o papel fulcral da capacidade de defesa em todo o período. É de salientar que depois da publicação do TM o debate sobre como empregar as capacidades começou a ganhar intensidade, primeiro para determinar como a NATO podia adicionar valor às capacidades dos aliados, e depois para determinar a forma de emprego das capacidades nacionais. Assim, depois de publicado o TM2, ficou esclarecido que as capacidades ofensivas disponíveis seriam as dos Estados membros, sob controlo nacional, e aprovou-se a criação de um Centro de Ciber Operações para integrar estas capacidades nos diferentes níveis de planeamento e operações da NATO (Stoltenberg, 2017m).

2.4 Ambiguidade

A ambiguidade é a primeira variável para a que não foi possível encontrar evidências textuais no primeiro período em estudo. A análise comparativa inicial dos três períodos restantes (Figura 15), revela com claridade a ambiguidade em torno à aplicabilidade do Artigo 5 no período prévio à publicação do TM, totalmente atenuada nos dois períodos restantes. Contudo, esta ambiguidade enquadra-se melhor no intenso debate aberto em relação ao assunto, do que na ambiguidade planificada como elemento constituinte de uma estratégia de dissuasão. A questão jurídica não estava esclarecida, mas esta debilidade não podia ser reconhecida (Appathurai, 2010), e falava-se em “ambiguidade construtiva” como uma das grandes fortalezas do Artigo 5, assente em que os adversários nunca conhecessem exatamente a posição do limiar (Rasmussen, 2010g). Esclarecida a questão jurídica, e

declarada pela NATO a aplicabilidade do Artigo 5, conserva-se a ambiguidade ao ligá-la à decisão, caso a caso, do Conselho do Atlântico Norte (NAC) (NATO, 2014b).

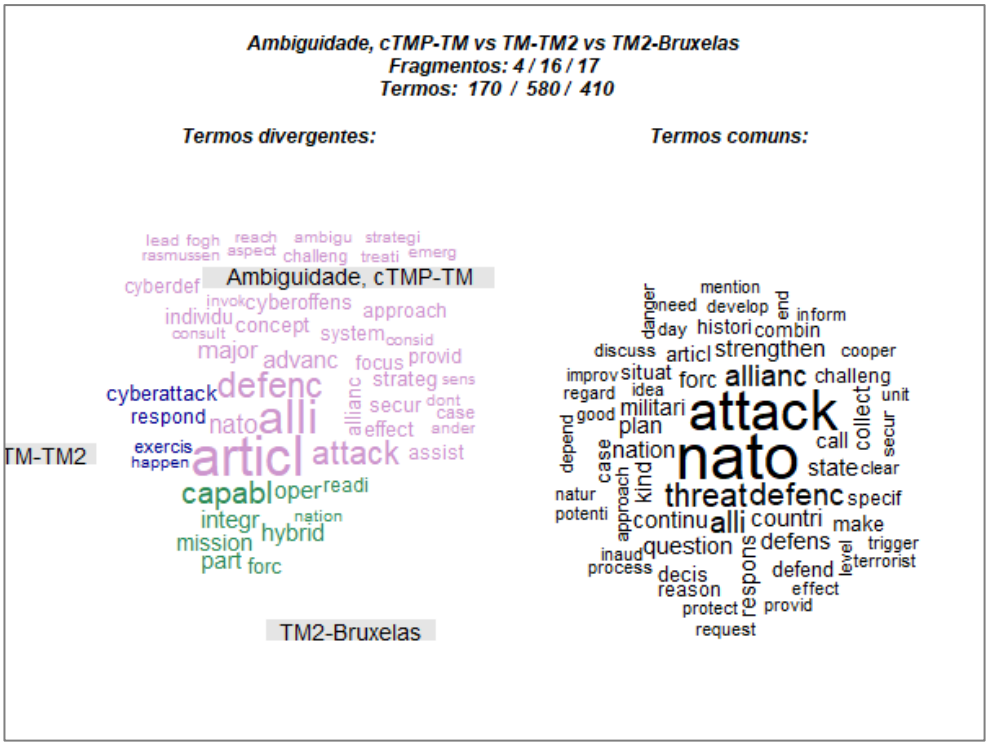


Figura 15 – Ambiguidade: análise terminológica comparativa desde o começo do TMP.

Fonte: (Autor, 2019)

Depois de publicado o TM, a ambiguidade é explicita e intencional, mas está ligada às mensagens de proporcionalidade necessárias para a estabilidade (Stoltenberg, 2015c; Vershbow, 2016a).

Quando três meses depois de publicado o TM se anunciava a proximidade da FOC das ciber equipas de resposta rápida, o anúncio aparecia ligado a uma ambiguidade quase surpreendente em relação a qual seria a forma de empregar esta e outras capacidades (Rasmussen, 2013c). Esta ambiguidade dificilmente pode ser compreendida fora de um contexto dissuasório de negação a potenciais adversários dos dados necessários para avaliar os custos.

A ambiguidade em relação às formas de resposta continua explicita ao mesmo tempo que se afirma estar a responder com contundência (Stoltenberg e Mikser, 2014). A negação de informação quanto à forma em que se está a responder aos ciberataques é deliberada e explícita (NATO, 2015b).

Na medida em que o processo se aproxima à publicação do TM2 o enquadramento das respostas no contexto da luta contra as estratégias híbridas torna desnecessária

qualquer explicação adicional quanto ao grande leque de capacidades de respostas disponíveis (Vershbow, 2016a). Ainda mais, a estratégia de dissuasão da NATO apresenta-se assente sobre todas as suas capacidades, sem diferenciar estratégias de dissuasão sectorial. Assim inclui capacidades convencionais, contra a guerra híbrida, ciber e resolutivas, incluídas as nucleares. (Stoltenberg, J., 2016f).

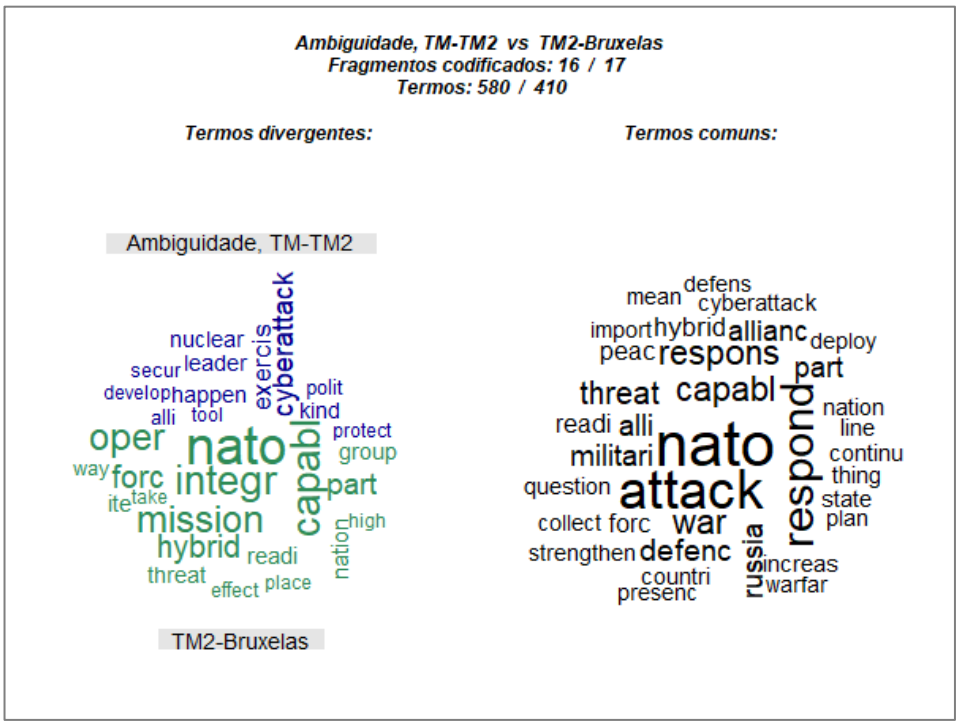


Figura 16 – Ambiguidade: análise terminológica em torno do TM2.

Fonte: (Autor, 2019)

A contextualização na guerra híbrida ainda acrescenta mais ambiguidade quanto à natureza da resposta, tendo como exemplo a *Nato Response Force* (Stoltenberg e Mogherini, 2015), ou o subtil vínculo entre ciber e presença avançada percetível, em palavras de Stoltenberg (2017i). Aliás, não se trata apenas de ser ambíguo quanto a qual será a capacidade com que se responderá, trata-se de responder com muitas medidas ao mesmo tempo (Stoltenberg, 2017j). Isto contribui adicionalmente para ultrapassar os efeitos secundários negativos da imputação política, de algumas respostas ciber, da preservação das capacidades forenses e da monitorização, entre outros. Contudo, foi depois do exercício de ambiguidade exposto que se acordaram o enquadramento e os princípios para a integração de cibercapacidades nas missões e operações da NATO (Stoltenberg, J., 2017m), nove meses depois de publicado o TM2 (Figura 16). Ora bem, quando se pergunta expressamente se serão empregues ciber efeitos no quadro da presença avançada, a

ambiguidade ressurge da mão da proporcionalidade e do respeito pelo Direito Internacional (Stoltenberg, 2017m). O mesmo acontece com a estrutura de comando sob a qual se articularão as capacidades, uma vez que o conceito geral não impede outras estruturas (NATO, 2018a), o que é muito relevante em relação à possível imputação de responsabilidades a quem aporta as capacidades de resposta.

A ambiguidade também se exercita quando se anunciam respostas com múltiplas medidas, não nomeadas, e vinculadas à imputação política indireta, "*We responded when Russia used hybrid tactics in Crimea, we are responding when we see cyber-attacks and we are responding in many different ways*." (Stoltenberg, 2018c).

Enfim, como explicita Stoltenberg (2018f), a NATO mantém a definição dos limiares e a natureza da resposta propositadamente difusas, respeitando os princípios de contenção e o Direito Internacional. Mas, como se declarou em Varsóvia, afirmando a determinação de utilizar todo o seu leque de capacidades contra as ciber ameaças (NATO, 2018d.).

Em concordância com a exigência de contiguidade na resposta aos ciberataques, decorrente da aplicação dos Manuais, não foi possível encontrar no *corpus* elementos relevantes de ambiguidade em termos de tempo.

Os elementos de ambiguidade quanto à origem geográfica são pouco frequentes, mas existem em relação à atuação das equipas de resposta desde as suas bases, em situações reais e exercícios.

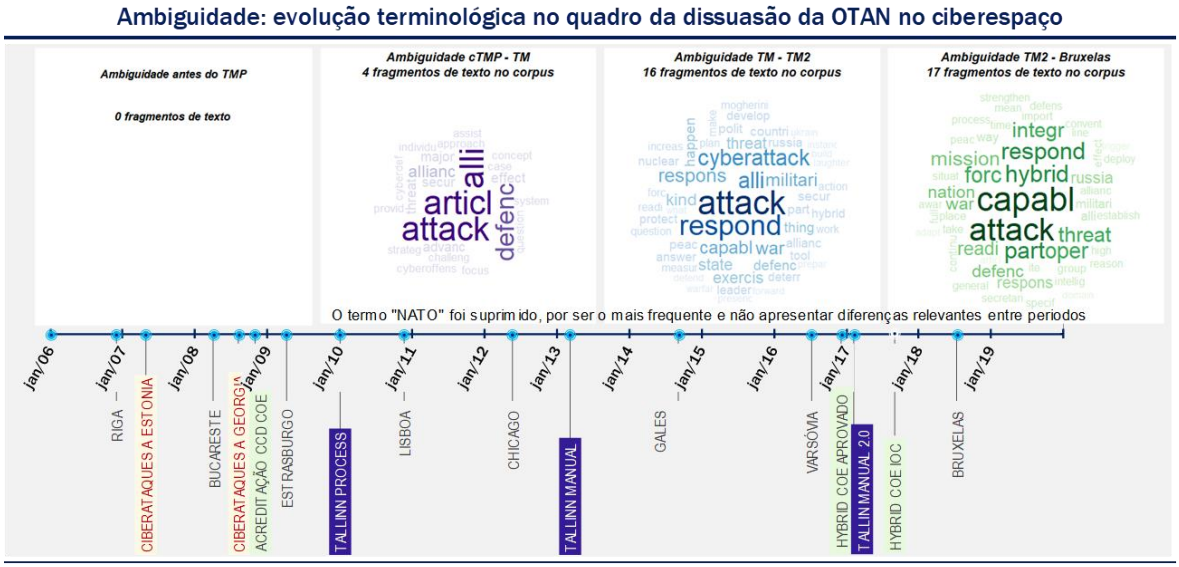


Figura 17 – Ambiguidade: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

Na Figura 17 observam-se mais uma vez o debate e a ambiguidade em torno à aplicabilidade do Artigo 5. Aclarado o assunto, depois de publicado o TM, a ambiguidade focaliza-se nas capacidades de resposta e na desnecessidade de responder em espécie. À medida em que nos aproximamos do último período em estudo a ambiguidade contextualiza-se no cenário da resposta contra a guerra híbrida, à desnecessidade de responder em espécie adiciona-se a determinação de responder com pacotes integrados por capacidades de distinta natureza. Já na última etapa do período analisado, a ambiguidade amplia-se ao enquadramento e controlo das cibercapacidades a integrar nas operações da NATO, e, portanto, reflete-se na listagem de capacidades que os aliados disponibilizarão.

2.5 Cooperação

A estratégia de cooperação para a dissuasão evoluiu no período em estudo, não isenta da influência de elementos do panorama internacional estranhos ao objeto de estudo. Assim, evoluiu-se de um cenário em que se procurava aproximação à Rússia, e cooperação também em ciber (Robertson, 2002), a um cenário em que a Rússia é identificada como ameaça, embora sem fechar as portas a uma aproximação, sob condição da mudança de atitude (Figura 18).

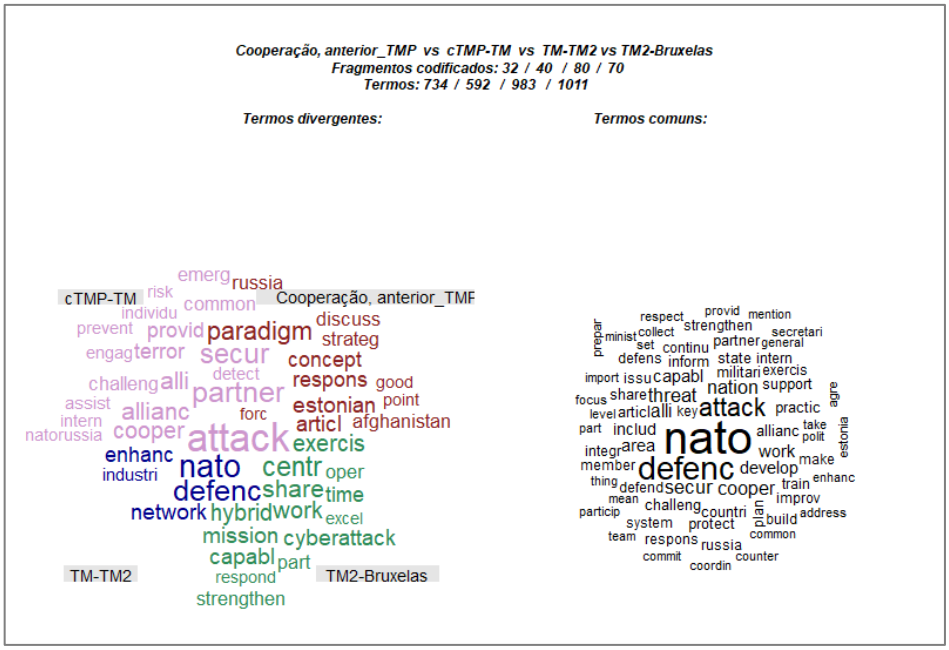


Figura 18 – Cooperação: análise terminológica comparativa dos quatro períodos.

Fonte: (Autor, 2019)

O desenvolvimento da *NATO Network Enabled Capability* (NATO,2006b) constituiu um dos primeiros exemplos de contribuição para a dissuasão alargada na perspetiva técnica, e também um exemplo de contributo para a imputação técnica prévio ao TMP.

Contudo os ciberataques à Estónia não tardariam em revelar a insuficiência destas medidas técnicas para resolver um problema estratégico. O silêncio em relação à ciber ofensiva em plena crise (NATO, 2007a), e as respostas elusivas (Appathurai, 2007a), eram paradigmáticos da necessidade de abordar um processo que permitisse estender ao ciberespaço o valor dissuasório do Artigo 5. Meses depois dos ciberataques a indefinição em relação à dissuasão alargada perdurava e, embora se apreciassem progressos na cooperação para a capacidade (Appathurai, 2007c; Scheffer, 2008c), era necessária a discussão jurídica. A necessidade de efetivar a defesa coletiva no ciberespaço, e o risco de não o fazer, tardaria quase um ano em se explicitar (Scheffer, 2008d), enquanto se procuravam formas de cooperação alternativas, económica, politica, e talvez militar (Scheffer, 2008e). Contudo, os eixos da nova política ciber anunciados na Cimeira de Bucareste, ainda abordavam a cooperação para a dissuasão alargada numa perspetiva muito limitada (NATO, 2008a).

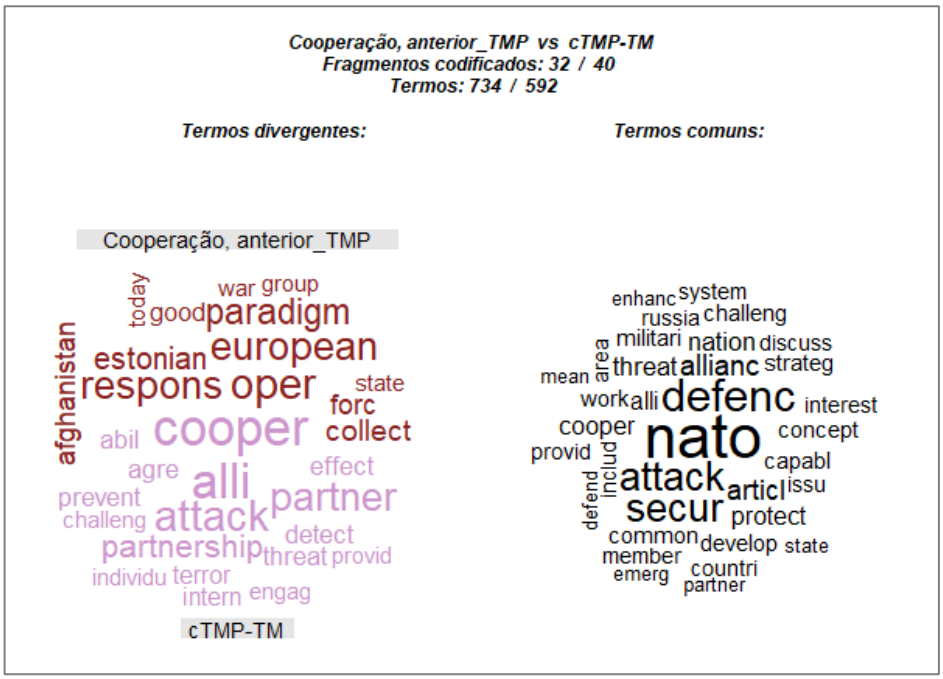


Figura 19 – Ambiguidade: análise terminológica em torno do começo do TMP.

Fonte: (Autor, 2019)

Iniciada quase em simultâneo com o TMP, a revisão do conceito estratégico incluía entre os seus objetivos fornecer uma nova interpretação da defesa coletiva (Scheffer, 2009). Contudo, seria na Cimeira de Gales, com o TM publicado, que se declararia o caráter fulcral da ciberdefesa na defesa coletiva e a aplicabilidade do Artigo 5 no ciberespaço (NATO, 2014b).

A procura da cooperação dentro da Aliança, com outras organizações internacionais e outros contribuidores relevantes para fornecer defesa e resiliência comum contra riscos e ameaças compartidos (Panizzi, 2011) é totalmente congruente com o conceito de segurança interdependente.

A cooperação técnica com a Estónia (Appathurai, 2007a), a Geórgia sob coordenação da *NATO-Georgia Commission* (Scheffer, 2008i) e a Ucrânia no quadro da *NATO-Ukraine Commission* (NATO, 2008c) iriam constituindo o quadro de cooperação da NATO com países parceiros (NATO, 2009b), ultrapassando a simples cooperação para a capacidade. Este quadro de cooperação abrangeu outras organizações como a UE (Rasmussen, 2010f) e de outros Estados situados muito longe do espaço euro-atlântico: Austrália, Nova Zelândia, Japão, Coreia do Sul… (Rasmussen, 2010e). Também não se podem omitir os esforços da NATO por incluir a Rússia no espaço de segurança euro-atlântico principalmente através do *NATO-Rússia Council*, ainda depois das crises da Estónia e da Geórgia (NATO, 2010a).

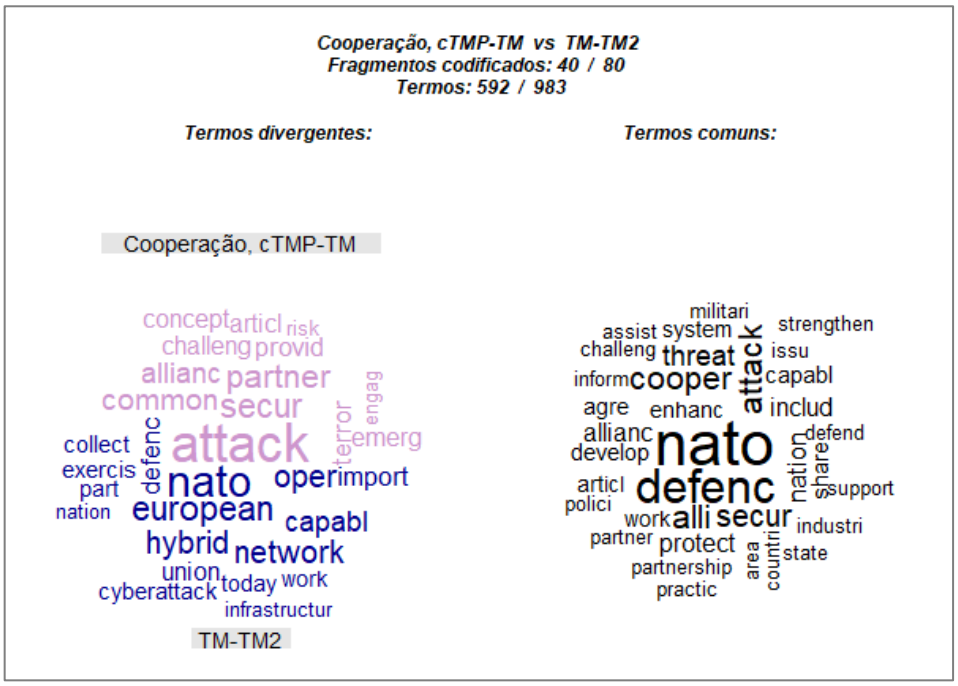


Figura 20 – Cooperação: análise terminológica em torno do TM.

Fonte: (Autor, 2019)

Contudo, no caminho para a Cimeira de Varsóvia a abrangência da segurança interdependente, estava a expandir-se na procura da resiliência geral contextualizada na luta contra as estratégias híbridas (Stoltenberg, 2015a). A persistência da Rússia nas suas estratégias ameaçava com deixá-la definitivamente fora da fronteira de segurança (Vershbow, 2016b), e obrigava a reforçar esta fronteira para leste (Vershbow, 2016c;

Vershbow, 2016d). Nos meses anteriores à Cimeira de Varsóvia, a NATO atingiria mais acordos de cooperação em ciber do que em toda a década anterior (Stoltenberg, 2016c), e antes de terminado o ano estreitar-se-ia ainda mais a cooperação com a UE (NATO, 2016h; NATO, 2017a). No início de 2018 seriam mais de quarenta as parcerias entre a NATO e os Estados não membros (NATO, 2018a).

Na Cimeira de Chicago continuou a explicitar-se a vontade de cooperação com Estados e organizações (NATO, 2012e), enquanto o NRC continuou a contribuir para a estabilidade, ao constituir um foro para evitar mal-entendidos e mitigar as interferências de terceiras partes (NATO, 2012d). A segurança interdependente continuou a ser fulcral: "*Cyber-defence is only as effective as the weakest link in the chain. By working together, we strengthen the chain"* (Rasmussen, 2013c).

Falando noutros atores relevantes, a importância da cooperação com o setor privado e a aplicação de conceitos de segurança interdependente começou a evidenciar-se já na altura do começo do TMP (Rasmussen, 2009), seria reforçado com a política de ciberdefesa de 2014 (Rasmussen, 2014a) (Figura 18), e continuaria posteriormente consolidando iniciativas como a *NATO Industry Cyber Partnership*[9] (NATO, 2016f).

Em relação à imputação, a NATO assumiu a sua responsabilidade na contribuição para a cooperação internacional, necessária para ultrapassar os problemas decorrentes da transnacionalidade do ciberespaço (Rasmussen, 2010a; Rasmussen, 2010c). Os primeiros contributos assentaram na melhoria das capacidades de detecção (NATO, 2010a), intercambio de informação e consciência situacional (NATO, 2010d; NATO, 2010e). Assim, os contributos para a imputação técnica foram acrescentando-se durante todo o processo (Stoltenberg, 2017g), mas não seria quase até à publicação do TM2 que se começaram a evidenciar contributos para a imputação política (Stoltenberg e Mogherini, 2016).

Os contributos da cooperação para a capacidade evidenciam-se desde antes do TMP, também se evidencia a importância das capacidades para uma cooperação apropriada (Naumann, 2002).

Em 2010 já se falava em desenvolvimento de capacidades para a deteção e dissuasão efetiva (NATO, 2010a). Contudo, a politica de ciberdefesa de 2011 trouxe contributos como a gestão centralizada, a inclusão de ciberdefesa no ciclo de planeamento da NATO[10],

[9] Iniciada em 2014 (Gottemoeller, 2017b)
[10] Efetivada em 2013 (NATO, 2014a)

a coordenação para acrescentar a resiliência, a possibilidade de destacar *NATO's Rapid Reaction Teams* em apoio de aliados individuais e a melhora da instrução e adestramento principalmente através do CCD COE (NATO, 2012c), aspeto onde o TMP se tornou fulcral. Mas a forma de empregar estas capacidades não estava clara e a NATO evitava responder às questões mais complexas (Rasmussen, 2012b), algumas das quais não seriam abordadas até ao TM2 (Regra 18).

Da nova política de ciberdefesa de 2014, já posterior ao TM, para além da inclusão da ciberdefesa no núcleo da defesa coletiva, destacava-se a melhoria das linhas de ação da de 2011 e o fortalecimento de aspetos como a cooperação com o setor privado[11] (Rasmussen, 2014a). Da nova política também se destacava que refletia uma abordagem internacional mais ampla para a questão da ciberdefesa (NATO, 2015a), o que, embora não se explicitasse, é de difícil compreensão se não se consideram os logros atingidos pelo TMP nessa altura.

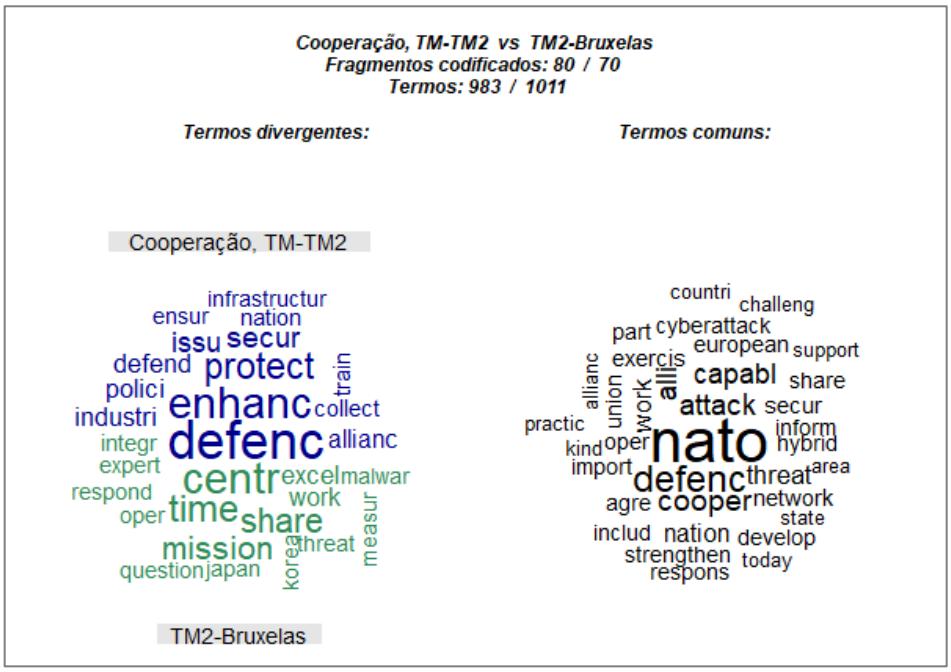


Figura 21 – Cooperação: análise terminológica em torno do TM2.

Fonte: (Autor, 2019)

Depois de publicado o TM, o foco das capacidades continuava a centrar-se em garantir a fortaleza de cada elo da cadeia de ciberdefesa (Rasmussen, 2013e). A segurança interdependente importava e na Cimeira de Varsóvia confirmava-se que o maior contributo

[11] Materializado em iniciativas como o *Framework for NATO-Industry Engagement* (Vershbow, 2014)

de cada aliado para a resiliência comum consistia em acrescentar a sua própria resiliência. A NATO acrescentaria valências adicionais (NATO, 2016f).

A atualização do *NATO Cyber Defence Plan* e a definição da folha de rota para a implementação do ciberespaço como domínio, quase coincidentes com a publicação do TM2, são fulcrais para a partilha de informação e o desenvolvimento de capacidades (Stoltenberg, 2017a). Contudo, só se fala em capacidades defensivas. A resiliência é fulcral, mas agora, o esforço e a cooperação para abranger as ameaças híbridas são intensos (Stoltenberg e Mogherini, 2017). Neste contexto é necessário coordenar os esforços nacionais, da NATO e da UE (Stoltenberg, 2017i), doutras organizações internacionais e também da indústria (Gottemoeller, 2017b). Para além dos contributos para a resiliência, o modelo de integração de capacidade ciber finalmente adotado foi o mesmo que para as capacidades nos outros domínios: propriedade nacional e participação em missões da NATO quando concordado (Stoltenberg, 2017l). A criação do *Cyber Operations Centre* na *NATO Command Structure* será fulcral para a integração de umas capacidades sobre as que as nações mantêm a propriedade e o controlo (Stoltenberg, 2017m) (Figura 21). A estrutura e os princípios de integração de capacidades em missões e operações de NATO foram anunciados em novembro de 2017 (Stoltenberg, 2017m), apesar do discurso desenvolvido durante anos sobre este assunto. Contudo, o acordo sobre a integração de "ciberefeitos soberanos" nas operações da Aliança não chegaria até às vésperas da Cimeira de Bruxelas (Stoltenberg, 2018i; NATO, 2018d).

Ao longo do período estudado (Figura 22) a cooperação para a resiliência esteve mais orientada para a segurança dos sistemas, antes do TM, e para a resiliência general, depois de se publicar. A obtenção de capacidades abordou primeiro a construção de capacidades nacionais e da NATO, depois a cooperação para a construção de capacidades de aliados e parceiros e finalmente a integração de capacidades nacionais nas operações da Aliança. A cooperação com a indústria e outros parceiros na procura da segurança interdependente seguiu um percurso ascendente ao longo de todo o período. Por fim, assistiu-se à procura de uma base de aceitação internacional crescente dos princípios e normas para a ciberdefesa, à que o TMP não foi alheio. Em particular, o CCD COE, promotor do TMP, demonstrou a sua utilidade como ferramenta de cooperação entre a NATO e a UE, capaz de ultrapassar as dificuldades políticas entre ambas organizações, possivelmente pelo facto de não pertencer a nenhuma delas (NATO, 2018b).

Figura 22 – Cooperação: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

2.6 Comunicação e sinalização

No início a comunicação da capacidade focava-se na questão técnica e de recursos, para incluir progressivamente questões de índole política e estratégica. Como era de esperar o resultado da análise deste indicador na dimensão prática, oferece resultados muito semelhantes aos da evolução da variável capacidade. (Figuras 14 e 23)

Figura 23 – Comunicação da Capacidade: evolução terminológica no quadro da dissuasão NATO no ciberespaço.

Fonte: (Autor, 2019)

Os resultados em relação com à comunicação da determinação não são muito diferentes (Figura 24).

Figura 24 – Comunicação da Determinação: evolução terminológica no quadro da dissuasão NATO no ciberespaço.

Fonte: (Autor, 2019)

Antes do começo do TMP há pouca evidência em termos de comunicação para a dissuasão. Ao contrário, a focalização das declarações na determinação para adquirir capacidades ou para desenvolver uma política ciber apropriada (Scheffer, 2008b), reforçam a ideia de carências contextuais para desenvolver uma estratégia dissuasória no ciberespaço.

À medida em que o contexto evoluía também o fez a comunicação para a determinação de empregar as capacidades disponíveis. Possivelmente, a decisão para empregar o Artigo 5 (NATO, 2014b; Stoltenberg, 2016j; Stoltenberg, 2018f), caso for necessário, seja o elemento de determinação mais relevante de todo o *corpus* analisado.

A determinação para respeitar a legalidade internacional e a estabilidade no ciberespaço foi transmitida inicialmente pela celebração dos trabalhos sobre o cumprimento voluntário das normas de responsabilidade estatal e sobre as medidas de fortalecimento da confiança em relação ao ciberespaço (NATO, 2016f). Mais tarde, esta determinação foi transmitida pelas três formas em que a NATO afirma contribuir para a estabilidade no ciberespaço: reafirmação do império da lei e da contenção, resiliência nacional e cooperação (NATO, 2018a). Por fim, essa mesma determinação é transmitida ao reafirmar-se a necessidade de aplicar a legalidade internacional no ciberespaço e assumir-se um compromisso para encontrar a forma de o fazer.

Antes do começo do TMP, a sinalização estava orientada para as ameaças em termos genéricos e sem concretizar, como por exemplo no processo de desenvolvimento do novo

Conceito Estratégico (Scheffer, 2008e). Quando a ameaça se tornou mais concreta, as atitudes sinalizadas eram agrupadas e não individualizadas, como se verificou, por exemplo, a propósito da assistência no quadro da *NATO-Georgia Commission* (Scheffer, 2008i). Por fim, quando totalmente concretizado o alvo da sinalização, não o eram as atitudes desaprovadas, como sucedeu, por exemplo, aquando da suspensão de atividades no NRC em agosto de 2008 (NATO, 2008a).

O estabelecimento do CCD COE na Estónia podia ser avaliado como elemento de sinalização, mas identificar essa sinalização como orientada à Rússia seria excessivo. Como afirmava o presidente Ilves, "…*cyber it's rangeless. So it doesn't matter where you are*" (Rasmussen e Ilves, 2013).

Já com o TMP a andar, a mensagem para a Rússia era dupla: transmitia a desconformidade com as ações russas, mas também a dificuldade em perceber a sinalização russa (NATO, 2010a). Naquela altura a criação do *Emerging Security Challenges Division (ESCD)* no *NATO International Staff* constituía um sinal claro; contudo o ciber apenas constituía uma fração dos desafios almejados. Na altura, os exercícios de ciberdefesa também começariam a atingir uma verdadeira dimensão sinalizadora. O exercício *Cyber Coalition 2010* envolveu por primeira vez a NATO, os seus Estados membros e a colaboração interagências, em evolução crescente, desde que começara a série com o *Cyber Coalition 2008* que envolvia apenas corpos da NATO (NATO, 2010c). Os efeitos positivos sobre a credibilidade da participação externa crescente parecem indubitados. Em consequência, o *Cyber Coalition 2011* contou com a participação de seis parceiros e da UE (NATO, 2012c), sinal de uma fronteira de segurança em expansão e de capacidades reais. A poucos meses da publicação do TM o *Cyber Coalition 2012* em simultâneo com o *Crisis Management Exercise CMX 2012* atingiam um objetivo ainda mais ambicioso, no primeiro exercício de gestão de crise em larga escala e cenário complexo, que incluía o treino das autoridades políticas e acrescentava ainda mais a participação externa à NATO (NATO, 2012i; NATO, 2013a).

Cyber Coalition 2013 continuaria na mesma linha, e com grande parte de expertos participando remotamente desde as suas nações (NATO, 2014a) e assim sucessivamente (Stoltenberg e Mikser, 2014), incluindo em 2014 a participação da indústria (Stoltenberg e Paloméros, 2015). O passo seguinte seria incluir uma componente ciber relevante em exercícios convencionais, por exemplo o *Ex. Trident Juncture 2015* (NATO, 2015c). Por fim, começariam os exercícios *Locked Shields*, com ciberataques reais para testar os sistemas aliados (Stoltenberg, 2018f).

A crise na Ucrânia incrementou a sinalização e as petições de sinalização à Rússia (Figura 25), contudo, a complexidade da crise impede isolar a sinalização orientada para o ciber das orientadas para outros domínios (Breedlove, 2014), incluídas as sanções (NATO, 2014b). O habitual será sinalizar em pacote, (Vershbow, 2016a). Contudo a progressiva expulsão da Rússia da fronteira de segurança não deixa de ser um elemento sinalizador adicional. A sinalização era explícita e a contundência ao sinalizar, e ao comunicar a determinação, era acompanhada pela abertura ao diálogo (Vershbow, 2016b). Todavia, a imputação e a conseguinte sinalização ou resposta continuavam sem se individualizar em relação à ofensa (Vershbow, 2016d). A Cimeira de Varsóvia confirmaria esta postura dissuasória e esta forma de sinalizar (NATO, 2016f), que, se se explicitava, não devia ser percebida apenas como resposta a uma crise concreta, como a da Ucrânia (Stoltenberg, 2017d).

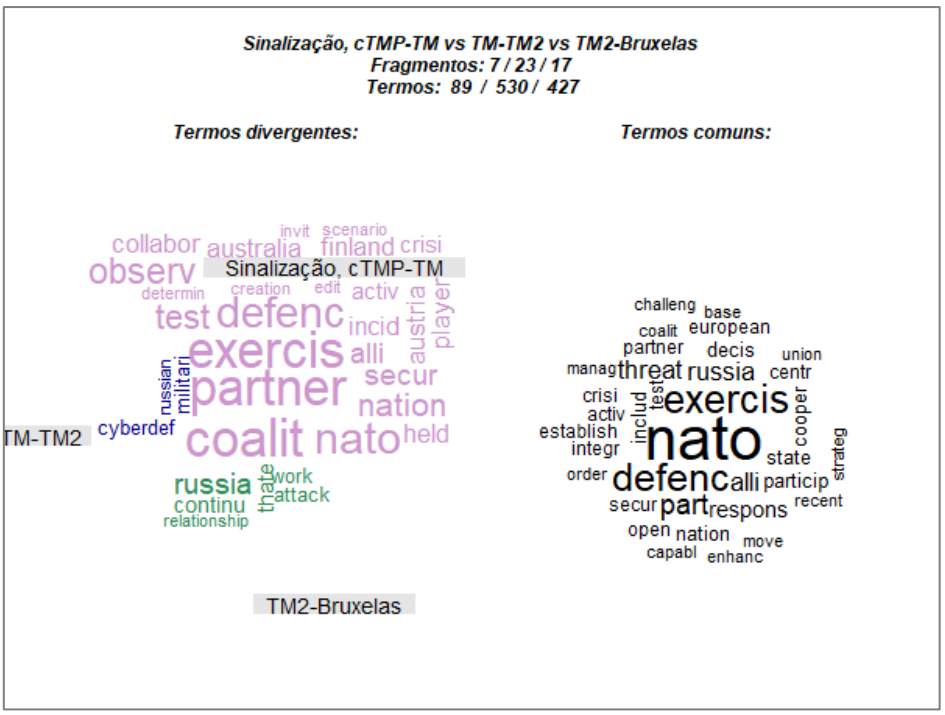


Figura 25 – Sinalização: análise terminológica comparativa desde o começo do TMP.

Fonte: (Autor, 2019)

Esta forma de sinalizar em pacote orientado a um adversário concreto prosseguiu até ao fim do período analisado (Stoltenberg, 2018c; Stoltenberg, 2018d; Stoltenberg, 2018g) e contrasta com a negativa em identificar o adversário no domínio específico dos ciberataques (Stoltenberg, 2017h).

Em resumo, está-se a transmitir que a determinação e as capacidades não são apenas discurso, são reais, e a resiliência obtida também. São os factos que se sinalizam e comunicam. A sinalização e mensagem dissuasória são claras, mas a mudança de linguagem e postura são lentas e deixam tempo e alternativas para o adversário adaptar as suas atitudes.

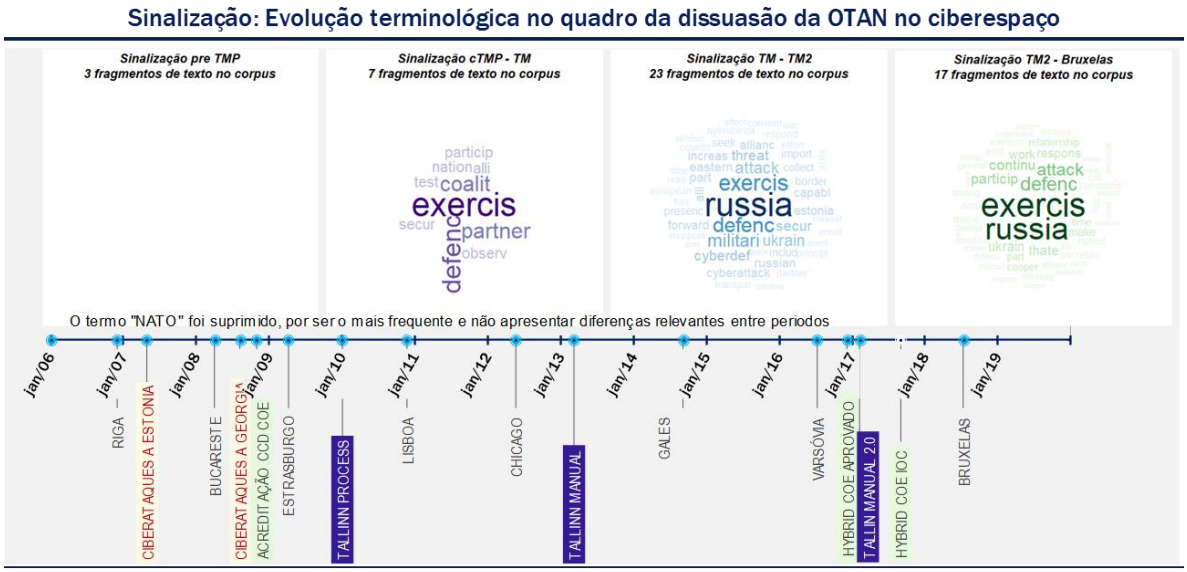


Figura 26 – Sinalização: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

Para responder à primeira pergunta derivada, ao longo deste capítulo analisou-se, a evolução das variáveis na sua dimensão prática, e em constante comparação com os marcos principais do TMP. Contudo, apesar de os marcos estabelecidos entre os períodos considerados serem nítidos, em modo algum seria lógico esperar um salto de continuidade brusco entre períodos. Porque a transição foi continua, e o conteúdo dos manuais não se manteve em segredo até à sua publicação, antes pelo contrário, ao longo da sua elaboração foi submetida ao escrutínio de uma amplia comunidade de juristas, no entorno dos grupos de trabalho do TMP, mas também mediante processos como o da Haia (ASSER Institute, 2016).

Neste contexto, o estudo permitiu verificar uma estreita correlação entre a evolução da posição do filtro de legitimidade determinada pelas teses dos manuais de Tallinn e a implementação prática dos elementos de dissuasão no ciberespaço.

Em consequência, fica completamente verificada a primeira hipótese, e respondida a primeira pergunta derivada, e ao mesmo tempo determinada a correlação entre o Processo

do Manual de Tallinn e a evolução de cada componente do problema da dissuasão no ciberespaço.

Fica agora por aclarar como é que se compatibiliza o Processo do Manual de Tallinn com a adoção de uma opção de dissuasão eficaz no ciberespaço, questão que se aborda no capítulo seguinte.

3 Compatibilidade do Processo de Tallinn com as opções de dissuasão

3.1 Dissuasão punitiva

Antes do começo do TMP o único elemento punitivo era a suspensão das atividades no NRC em reação à atitude Russa no conflito da Geórgia, incluindo explicitamente os ciberataques entre as muitas atividades reprovadas (Scheffer, 2008g).

A procura de uma opção de dissuasão apropriada evidenciou-se rapidamente e, apesar das dificuldades que apresentava o domínio cibernético, não se queria renunciar a uma componente punitiva na mistura. Contudo, a realidade técnica, legal e procedimental recomendavam a defesa (Shea, 2010). A possibilidade de invocar o Artigo 5 era apenas uma insinuação, e o desenvolvimento de um leque completo de cibercapacidades era apenas um propósito de intenção (NATO, 2010a). Em consequência, consolidou-se uma estratégia completamente defensiva e de assistência para segurar os sistemas dos aliados, e oficialmente a ciber-ofensiva não era considerada nem sequer quando questionados (Rasmussen, 2012b).

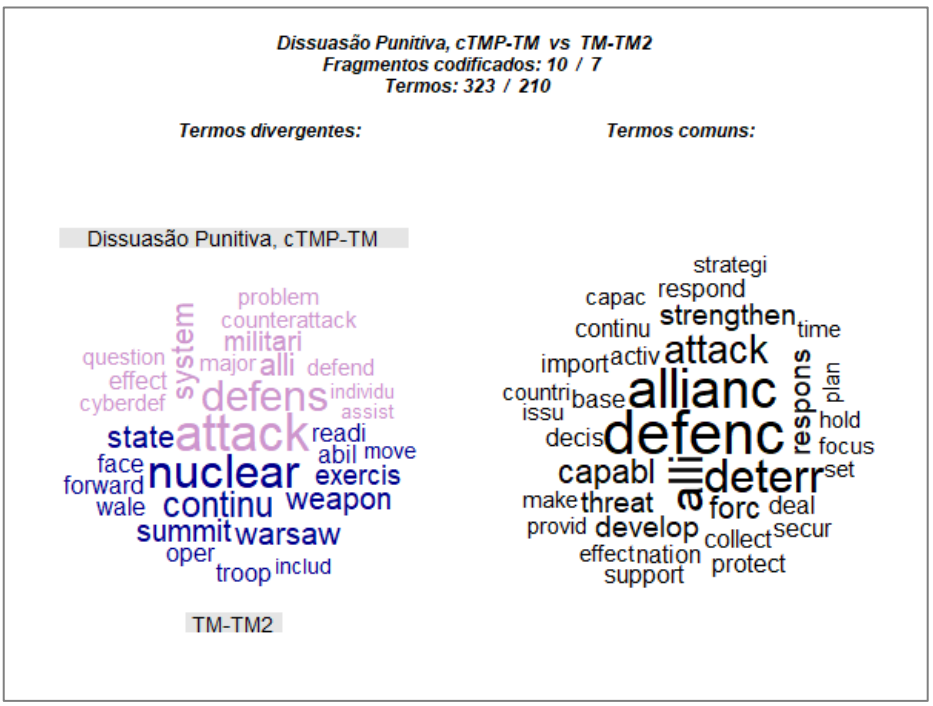


Figura 27 – Dissuasão Punitiva: análise terminológica comparativa em torno do TM.

Fonte: (Autor, 2019)

Com a Cimeira de Gales, depois de publicado o TM, a situação mudou (Figuras 27 e 28). A declaração de aplicabilidade do Artigo 5 no ciberespaço incluía um potente elemento punitivo na estratégia de dissuasão, mas apenas contra as ofensas mais graves

(Stoltenberg e Paloméros, 2015). Neste caso a panóplia não se limitava a cibercapacidades, porque a posição de dissuasão, reconfirmada na cimeira de Varsóvia, contemplava todas as opções, incluída a nuclear (Stoltenberg, 2016f) (Figuras 27 e 28).

Contudo, depois de publicado o TM2, reconhecia-se que a resposta com cibercapacidades podia ser mais proporcionada, daí o facto de estarem integradas cibercapacidades ofensivas, sob controlo nacional e em conformidade com o Direito Internacional, nas missões e operações da Aliança (Stoltenberg, 2017m) (Figura 28). No entanto, este modelo de integração trazia consigo as vantagens adicionais antes comentadas.

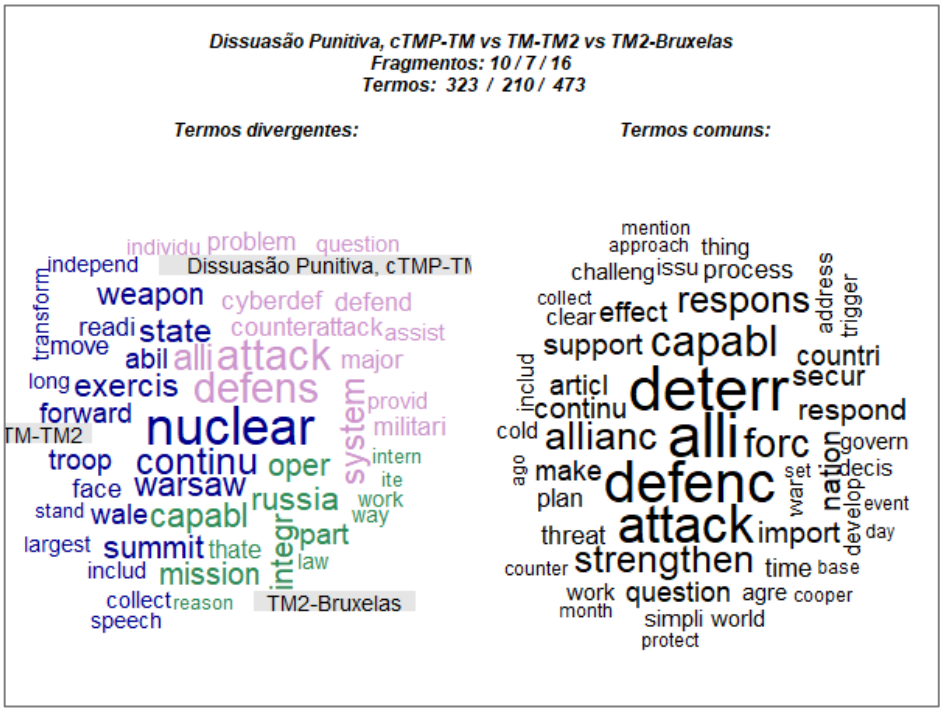


Figura 28 – Dissuasão Punitiva: análise terminológica comparativa desde o começo do TMP.

Fonte: (Autor, 2019)

Para agressões em limiares mais baixos, a componente punitiva limita-se para elevar os custos de um ataque que muito provavelmente não atingirá os seus objetivos. Para estes casos podem reservar-se respostas para além do ciber, diplomáticas, económicas, etc. recomendavelmente internacionais (NATO, 2018a). Contudo, há outras vias para elevar os custos, incluído o desenvolvimento do ciberespaço como domínio das operações (Stoltenberg, 2018f).

A contextualização de atitudes nas estratégias híbridas facilita a inclusão de elementos punitivos assim, o ciber também contou na decisão de reforçar a *NATO*

Response Force e estabelecer a *High Readiness Joint Task Force* (Stoltenberg, 2018c), ou na expulsão de diplomatas russos por alguns Estados da Aliança (Stoltenberg, 2018d).

Por fim, na Cimeira de Bruxelas, reafirmou-se a determinação de impor custos a quem prejudique a Aliança, considerando a resposta contra o leque completo de ameaças ciber, incluídas as componentes de estratégias híbridas (NATO, 2018d).

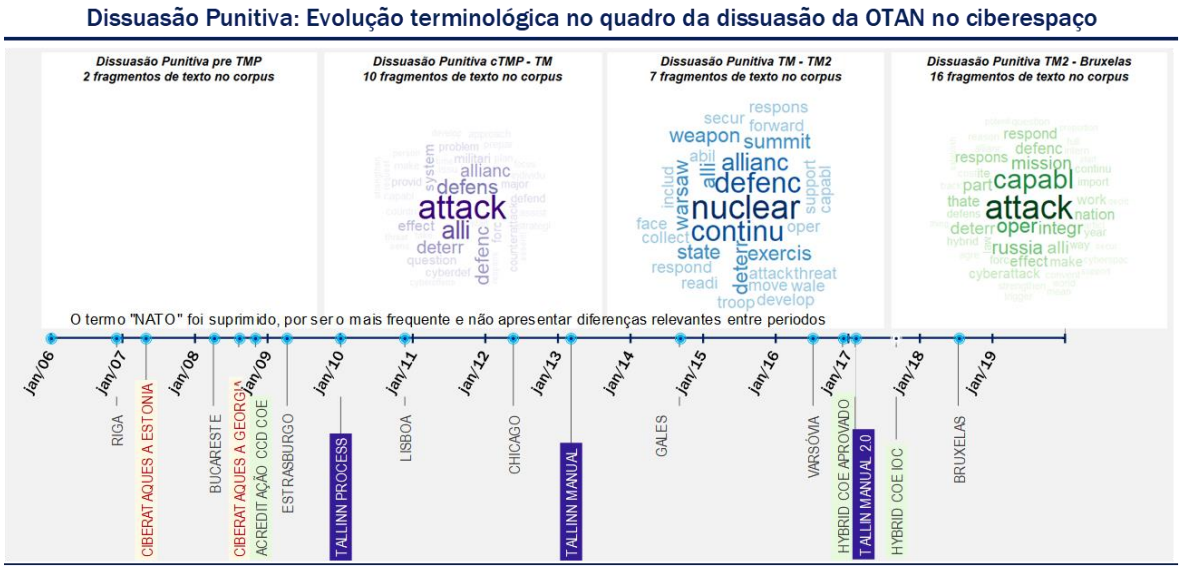


Figura 29 – Dissuasão Punitiva: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

3.2 Dissuasão defensiva

É possível apreciar elementos de dissuasão defensiva no ciberespaço muito antes do TMP ter começado, inclusive antes dos ciberataques à Estónia (NATO, 2003; NATO, 2006b). Contudo, o caso da Estónia revelaria a necessidade urgente de melhorar a proteção dos sistemas, e assim se concordaria na Cimeira de Riga (NATO, 2007b; Appathurai, 2007b). Além disso, os ciberataques são apresentados como um incentivo para acelerar e intensificar o fortalecimento dos sistemas, e em consequência o custo de futuros ciberataques adversários, reforçando a dissuasão (Flory, 2008). Em Bucareste confirmava-se esta postura defensiva (NATO, 2008a), e em Estrasburgo, para além de se confirmar que o fortalecimento dos sistemas aliados estava a acelerar-se, anunciava-se a expansão da fronteira de segurança para além das fronteiras dos Estados membros, com a inclusão de parceiros (NATO, 2009b). Com o TMP iniciado, a estratégia puramente defensiva continuava inalterada na declaração da Cimeira de Chicago (NATO, 2012e).

Os trabalhos de desenvolvimento do novo Conceito Estratégico insistiam na necessária aceleração do processo de fortalecimento da defesa, mas também na

necessidade de desenvolver um leque completo de capacidades passivas e ativas, orientadas à deteção e à dissuasão (NATO, 2010a). A política de ciberdefesa e o processo de planeamento da NATO eram orientados para os mesmos objetivos (NATO, 2012c). Contudo, os princípios adotados para o Conceito Estratégico seriam puramente defensivos: prevenção, resiliência e defesa dos ativos cibernéticos críticos (Panizzi, 2011). A opção da NATO de fornecer a defesa enquanto algum dos aliados exercesse a ofensiva no ciberespaço, não se considerava (Rasmussen, 2012b), pelo menos publicamente.

Com o TM recém-publicado, a mensagem continuava a incluir os dois elementos clássicos da dissuasão defensiva: a persistência nos ataques dos transgressores da legitimidade internacional e o êxito defensivo dos sistemas robustos da Aliança (Rasmussen e Ilves, 2013; Rasmussen, 2013c.). Todavia, a forma em que se estava a responder não se explicitava (Stoltenberg e Mikser, 2014). Os exercícios com participação externa à aliança reforçariam a mensagem de robustez, e a declaração de Gales confirmando a aplicabilidade do Artigo 5 no ciberespaço incluía o elemento punitivo para os ciberataques mais graves.

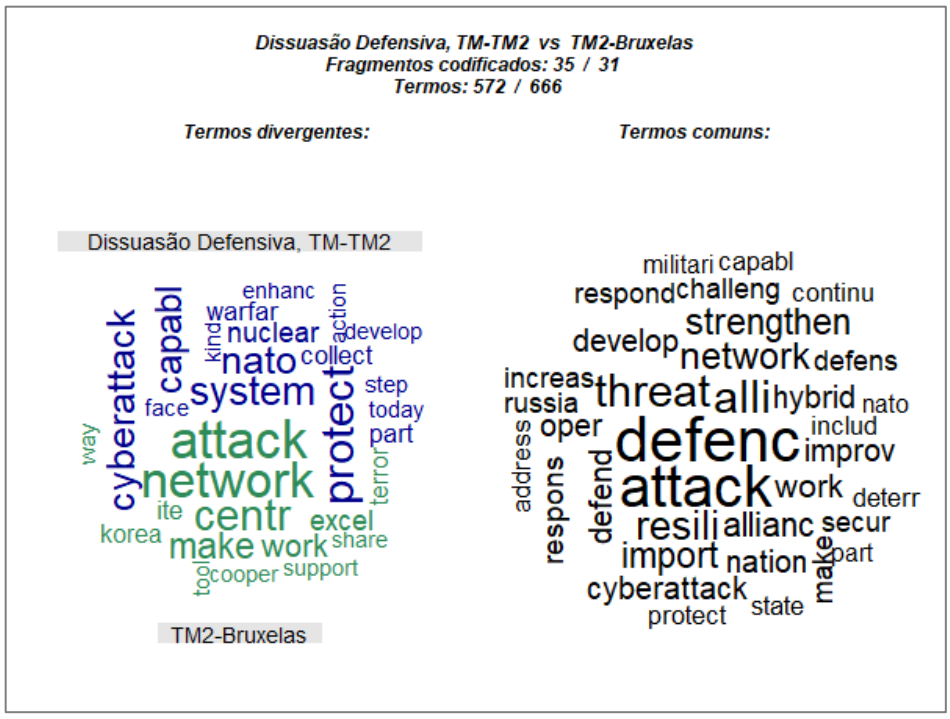


Figura 30 – Dissuasão Defensiva: análise terminológica comparativa em torno do TM2.

Fonte: (Autor, 2019)

Com a crise da Ucrânia, a postura dissuasória defensiva ampliou-se para acrescentar a resiliência geral contra as estratégias híbridas (Stoltenberg, 2015a; Vershbow, 2016a).

Contudo, o posicionamento ciberdissuasório permanecia defensivo. A NATO, como organização, afirmava não ter nem desenvolver cibercapacidades ofensivas (Stoltenberg, 2016c).

O passo seguinte foi reforçar a resiliência global, transpondo o carácter coletivo para colocar entre as prioridades a proteção das infraestruturas e redes nacionais (NATO, 2016c; NATO, 2016e). O que seria assumido por cada um dos aliados na Cimeira de Varsóvia (NATO, 2016f).

O TM2 traria abordagens muito interessantes para promover a estabilidade no ciberespaço em contexto híbrido. Foi quase na altura da sua publicação que a resiliência contra os ciberataques seria plenamente enquadrada no contexto mais abrangente da resiliência contra a guerra híbrida (Stoltenberg, 2017a) (Figura 30). Neste contexto, a imputação política indireta será mais explicita e frequente (Stoltenberg, 2017l) do que antes. As vantagens desta contextualização para a elevação de custos por desgaste do prestígio do adversário parecem lógicas. No fundo, o incremento de custos do adversário será resultado de uma luta pública de legitimidades, portanto é fulcral reforçar a mensagem do posicionamento defensivo da Aliança, e a negação de qualquer aspeto ofensivo (Stoltenberg, 2017e) exceto, claro está, para os limiares mais elevados. O alargamento da fronteira de segurança também contribui para a luta de legitimidades e, não menos importante, para acrescentar a resiliência efetiva e os riscos do atacante face à imputação técnica. O reforço da cooperação com a UE e de grande valor neste sentido (Stoltenberg, 2017h).

Em resumo, o posicionamento defensivo no ciberespaço passa a ser uma componente do posicionamento de dissuasão e defesa da NATO contra as ameaças híbridas, em cooperação com a UE e outros parceiros, assente na melhoria da consciência situacional, no aumento da prontidão das forças e na melhora da resiliência (Stoltenberg e Mogherini, 2017) em todo o espectro "*From tweets to tanks*" (Stoltenberg, 2017i), respeitando sempre os critérios de defesa, proporcionalidade e alinhamento com os compromissos internacionais (Gottemoeller, 2017b).

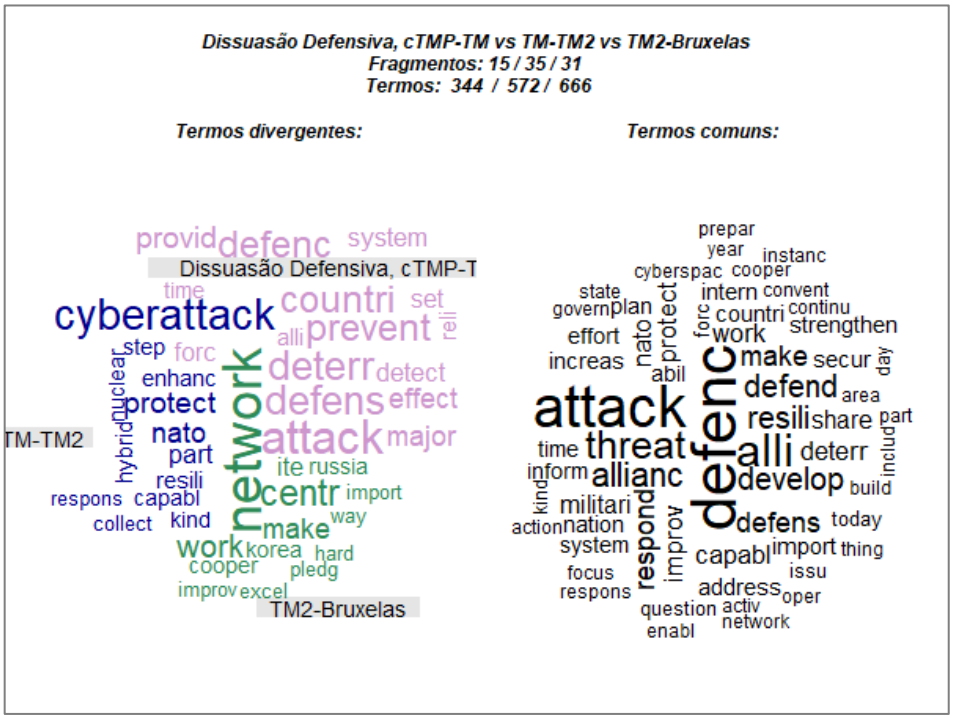


Figura 31 – Dissuasão Defensiva: análise terminológica comparativa desde o começo do TMP.

Fonte: (Autor, 2019)

Em relação à resiliência, esta pode ser abordada desde a perspetiva técnica, mas também desde a perspetiva social que faz alguns ataques muito mais impactantes. Portanto, para a estratégia ser apropriada, a face da guerra informacional e a face da segurança contra os ciberataques devem ser consideras em conjunto (NATO, 2018a).

Figura 32 – Dissuasão Defensiva: evolução terminológica no quadro da dissuasão da NATO no ciberespaço.

Fonte: (Autor, 2019)

3.3 Na procura de uma opção de dissuasão eficaz

Ao longo deste trabalho analisou-se o caminho percorrido pela NATO na procura de uma estratégia de dissuasão eficaz no ciberespaço. É difícil estabelecer uma data certa para o começo deste caminho. O primeiro documento do fundo documentário analisado data de 1969, mas o primeiro documento com elementos de interesse para a dissuasão no ciberespaço data de 2002. Contudo, não seria até depois dos ciberataques à Estónia que os documentos do *corpus* com referências ao ciberespaço e à dissuasão no ciberespaço começariam a crescer de forma explosiva, em termos absolutos e relativos (Figuras 33 e 34).

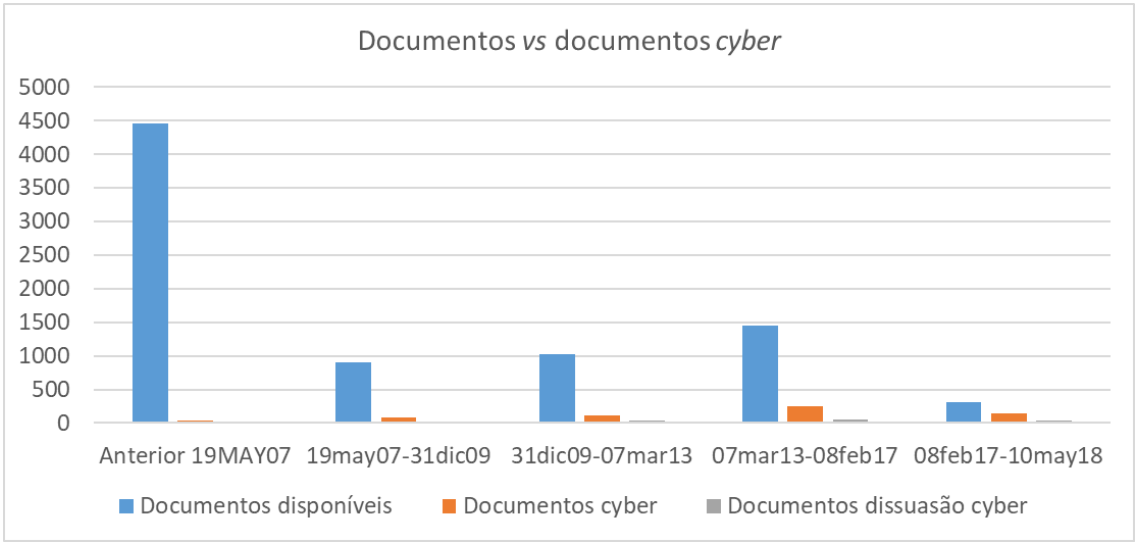


Figura 33 – Documentos totais do fundo documentário *vs* documentos *cyber* e documentos dissuasão *cyber*.

Fonte: (Autor, 2019)

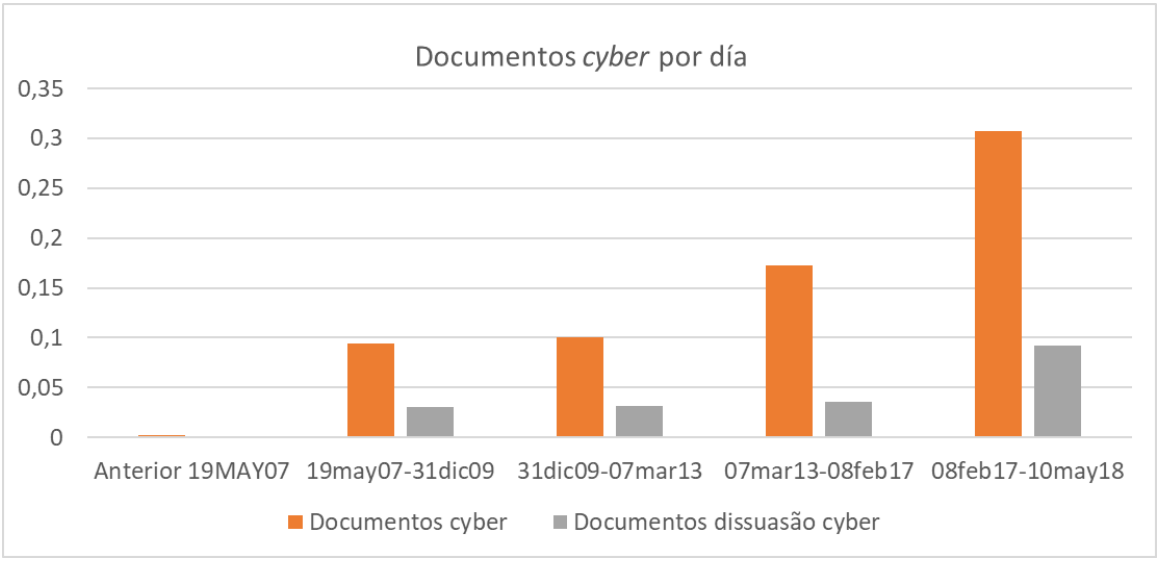


Figura 34 – Documentos ciber *vs* documentos dissuasão *cyber* por dia.

Fonte: (Autor, 2019)

Neste percurso a NATO foi sempre ciente da necessidade de respeitar a legalidade internacional como se percebe no discurso, mas também nos factos e na estratégia dissuasória desenvolvida. Assim, a necessidade de ser muito sensível na avaliação que a comunidade internacional pudesse fazer com respeito à possível violação da proibição do uso da força para a que referem os Manuais[12], foi alargada pela NATO para todo o leque de limiares a considerar.

Em consequência, no período prévio aos Manuais, de indefinição e de ausência de análises ou estudos jurídicos, aplicou-se uma estratégia completamente defensiva e de assistência para defender os sistemas dos aliados. Depois de publicado o TM, começaria a inclusão de elementos punitivos, primeiro contra as formas de ataque mais graves, também as mais claras, a declaração de aplicabilidade do Artigo 5, incluindo todo o leque de respostas, também a nuclear. Contudo, era necessário adicionar formas de elevar os custos dos ataques mais leves. Depois de publicado o TM2, avaliou-se a possível resposta com cibercapacidades, pela sua maior proporcionalidade, e em consequência a integração de cibercapacidades ofensivas sob controlo nacional e em conformidade com o Direito Internacional. Para agressões em limiares mais baixos incluíram-se outras respostas diplomáticas, económicas, etc., recomendavelmente internacionais, e que sem dúvida eram facilitadas pela promoção da aplicação no ciberespaço dos Regimes Especiais do Direito Internacional que fazia o TM2 Parte II. A contextualização dos ciberataques nas estratégias híbridas também facilitava a inclusão de elementos punitivos, em coerência com a análise contextualizada proposta pelo TM2.

A expansão da fronteira de segurança, o desgaste da credibilidade do adversário e a luta de legitimidades, estiveram presentes desde o começo, como corresponde a estes elementos próprios de opções defensivas. Contudo, estes elementos também evoluíram, e ganharam eficácia, em sincronia com a consolidação das interpretações jurídicas promovidas pelo TMP.

Em conclusão, a opção de dissuasão da NATO no ciberespaço assenta numa estratégia defensiva, sobre a que, para acrescentar os potenciais custos do adversário, se adicionam elementos punitivos na medida em que se percebem aceitáveis e legítimos pela comunidade internacional[13].

[12] Regras 11.8 do TM e 69.8 do TM2

[13] A descrição da opção de dissuasão da OTAN feita pelo Secretario General (Stoltenberg, 2018f) sumariza com claridade os elementos fulcrais da mesma.

O TMP constitui um importante elemento de referência no processo de decisão para incluir elementos na estratégia, daí a sincronia observável entre as interpretações dos Manuais e os elementos que passam a formar parte da opção de dissuasão.

Em consequência, o estudo permitiu responder à segunda pergunta derivada ao verificar a compatibilidade do Processo do Manual de Tallinn com a adoção de uma opção de dissuasão eficaz no ciberespaço. Além disso, confirma-se a segunda hipótese da investigação, verificando que o Processo do Manual de Tallinn é compatível com as sucessivas opções de dissuasão no ciberespaço que foram incluindo elementos na medida em que podiam ser avaliados como legítimos pela comunidade internacional, alinhando assim sinergicamente os contributos do TMP com as dificuldades a ultrapassar para atingir uma estratégia de dissuasão eficaz no ciberespaço.

Conclusões

O fracasso, no verão de 2017, do quinto GGE, alegadamente por sobrepor os interesses político-estratégicos às questões jurídicas, constitui um claro indicador do impacto que a consolidação das normas do Direito Internacional pode ter sobre a estratégia. A pugna por estabelecer uma ordem internacional favorável no ciberespaço, desenvolvida nas últimas duas décadas e cuja finalização ainda não se vislumbra, tem impulsionado a promoção de ordens jurídicas que vão de encontro aos interesses dos seus promotores relativamente aos conflitos no ciberespaço.

Esta confrontação afeta negativamente a estabilidade no ciberespaço, diminui as garantias de que os Estados não serão atacados e obriga-os a reforçar as suas estratégias dissuasórias, alinhadas com os posicionamentos jurídicos que defendem.

A NATO não é alheia a esta situação, e mantém um compromisso duplo, de manter a liberdade de ação e decisão no ciberespaço para garantir a sua capacidade de dissuasão e defesa e de atuar de acordo com a legalidade internacional. Mas estes compromissos não são independentes, porque o posicionamento em relação à legalidade internacional no ciberespaço, condicionará os recursos disponíveis para cumprir o primeiro compromisso.

Ao longo deste trabalho procurou-se compreender como o Processo do Manual de Tallinn influencia a estratégia de dissuasão da NATO no ciberespaço.

Para atingir este objetivo formulou-se a seguinte pergunta de partida:

Como é que o Processo do Manual de Tallinn influencia a dissuasão da NATO no ciberespaço?

Que se dividiu em duas perguntas derivadas:

PD1 - *Em que medida o Processo do Manual de Tallinn contribui para superar dificuldades específicas suscitadas com a aplicação de doutrinas de dissuasão no ciberespaço?*

PD2 - *Em que medida o Processo do Manual de Tallinn é compatível com a adoção de uma opção de dissuasão eficaz no ciberespaço?*

O problema abordou-se segundo um esquema de raciocínio hipotético dedutivo, assente numa metodologia de análise qualitativa e estratégia de estudo de caso, fundamentada em dados documentais. Com esta finalidade, criou-se um *corpus* de fontes primárias procedente da base de dados documental da NATO. Partindo de 8.158 documentos, depois da filtragem apropriada, incluíram-se no *corpus* 165 documentos, aos que se aplicaram as técnicas de análise expostas seguidamente.

Depois de colocar o problema, desenhou-se o modelo teórico. Adotando como ponto de partida o esquema teórico de Bustelo (2017), ajustou-se o modelo aos objetivos desta investigação, mediante um processo indutivo no qual se empregaram técnicas de codificação aberta e análise relacional.

O modelo desenvolvido permitiu aplicar o processo de dedução e teste para responder às perguntas de investigação. Este processo desenvolveu-se em duas etapas, e empregou técnicas de codificação aberta e mineração de texto, que se revelaram muito úteis para avaliar globalmente a evolução dos processos estudados, sem perder a conexão com os elementos particulares significativos.

A primeira pergunta derivada, abordou-se na primeira etapa, adotando como ponto de partida a seguinte hipótese:

HIP1 - *Os efeitos do Processo do Manual de Tallinn são distintos a nível de cada dificuldade de dissuasão no ciberespaço*.

Estabelecida a hipótese, desenvolveu-se o processo dedutivo de construção de explicações, nas dimensões teórica e da praxe internacional, cujas conclusões se sumarizam nos parágrafos seguintes.

Antes do começo do TMP a NATO procurava o encaixe das soberanias nacionais e da própria Aliança frente a um problema de índole transnacional ainda não incluído nas prioridades da NATO. Os ciberataques à Estónia mudaram a perspetiva, e até à publicação do TM, a atenção focou-se no papel da Aliança frente aos ciberataques, na defesa territorial, nas fronteiras estatais e na fronteira de segurança.

Com a publicação do TM estabeleceu-se uma referência interpretativa relevante sobre a soberania no ciberespaço em especial nos aspetos territoriais, fronteiriços e jurisdicionais. Contudo, o TM2 ainda aprofundaria mais estes aspetos, esclarecendo a aplicabilidade do princípio de soberania nas camadas física, lógica e social do ciberespaço; soberania que foi reforçada ao declarar que a consideração do ciberespaço como *global common* não é a mais correta, uma vez que assenta em infraestruturas e é utilizada por sujeitos que estão abrangidos por jurisdições e, como tal, pela soberania de um ou vários Estados. A questão jurisdicional também ficaria solidamente esclarecida frente aos problemas de dissuasão ao declarar-se a sua sujeição aos mesmos princípios gerais que qualquer outra forma de atividade. O detalhe e conteúdo das regras relativas à soberania e à jurisdição extraterritorial são em general completamente compatíveis com as necessidades

da dissuasão. E o facto de o TM2 não reconhecer as prerrogativas da soberania às organizações internacionais foi ultrapassado pela distribuição de responsabilidades estabelecida na Cimeira de Bruxelas.

Em consequência, depois da publicação do TM as responsabilidades nacionais na resposta frente aos ciberataques começaram a ganhar peso para atingir um papel fulcral depois da publicação do TM2, o que veio a confirmar uma tendência para a renacionalização do ciberespaço.

Em conclusão, observou-se uma clara evolução do conceito de aplicação da soberania no quadro da estratégia da NATO no ciberespaço, em sincronia com a interpretação jurídica promovida pelo Processo de Tallinn.

Em termos de imputação, depois do período exploratório prévio ao começo do TMP, o foco colocou-se em "o que imputar". Os Manuais estabeleceram uma escala de ilícitos imputáveis em cujo patamar mais alto está o "ataque armado" apresentado como caso agravado do "uso da força". A avaliação em termos de escala e efeitos foi o mecanismo adotado para avaliar o salto entre limiares. Adicionalmente, a sensibilidade para a avaliação que pudesse fazer a comunidade internacional de cada imputação foi adotada como critério complementar, o que se liga com o papel dos Manuais no processo de impulsão normativa.

A escada de limiares continua com a responsabilidade legal internacional imputável por "atuação ilegal" ou omissão da "diligencia devida", onde destaca o contributo do TM2 para declarar ilegais ações e omissões que outras interpretações podiam considerar num limbo jurídico. Contudo, a imputação das formas mais brandas e habituais de confrontação fica limitada. Porém, seria possível qualificar algumas combinações delas até como "uso da força".

No seguintes patamares encontramos a ação não amistosa, mais relevante no domínio político estratégico do que no jurídico, a aplicação do Direito Internacional Privado ou dos ordenamentos jurídicos internos dos Estados e três casos que sem requererem imputação podem anular a ilicitude de algumas respostas de Estado, o "estado de necessidade", a "causa de força maior" e a "emergência vital", de elevado valor para a dissuasão defensiva.

Em termos de sujeitos passivos da imputação, os Manuais contribuíram para a possibilidade de imputar a um Estado ilícitos no ciberespaço. É de salientar a interpretação extensiva de órgãos de Estado, a possibilidade de imputação a um Estado de ciberoperações executadas por atores não-estatais e a fundamentação da imputação política. A possibilidade de não revelar as técnicas forenses e de completar a falta de

inteligência técnica com a avaliação em contexto são contributos do TM2 para a imputação política.

Assim, o TM abriu o caminho para a imputação política, que se começou a materializar sobre a Rússia. A necessidade de contextualização e de adicionar elementos de prova complementares a este tipo de imputação foi-se reforçando à medida em que evoluía o conhecimento das estratégias hibridas e se aproximava a publicação do TM2. Depois de publicado, intensificaram-se as mensagens de imputação política à Rússia contextualizadas na estratégia hibrida que se lhe imputa. Em simultâneo, as mensagens de imputação técnica no discurso da NATO são quase inexistentes.

O primeiro paradoxo a ultrapassar para empregar capacidades de resposta seria legitimar a ameaça com o "uso da força", quando a priori estaria vedado pelo Artigo 2.4 da CNU. No início do processo a capacidade de ameaça era mínima, portanto, na dimensão prática, a ameaça do uso da força ou outras respostas não é explicita, nem orientada a um ator concreto, é apresentada como a resposta contra uma ameaça. Ainda depois de publicado o TM2, seria mais comunicação do que ameaça.

Na avaliação dos patamares de resposta concordantes com os respetivos patamares de imputação a primeira dificuldade estava na resposta com o "uso da força". Dificuldade que se ultrapassa respeitando os requisitos de necessidade, proporcionalidade, iminência, contiguidade e determinação *ex ante* do "ataque armado" e do atacante. O TM2 favoreceria as estratégias defensivas legitimando alegar o "estado de necessidade" para ultrapassar o último requisito. As modalidades de contrarretaliação automática são deslegitimadas e a possibilidade de empregar respostas encobertas (*sub-rosa*) ficava muito limitada. Na perspectiva da preservação de cibercapacidades próprias destaca a interpretação de não obrigatoriedade de revelar as técnicas de imputação forense.

Na prática, depois do reconhecimento de aplicabilidade do Artigo 5, o reconhecimento do ciberespaço como um domínio das operações, seria um grande avanço em termos de capacidade, que significava a atualização do artigo 5, sem o reescrever, e a integração da dimensão ciber do conflito em igualdade de condições que as restantes. Contudo, a NATO não reconheceria o emprego de ciberarmas ofensivas pelos seus membros até depois de o TM2 ter sido publicado. Também nessa altura, a NATO decidiria empregar capacidades nacionais, sob controlo nacional, para responder ofensivamente.

Por debaixo do limiar do uso da força a capacidade de resposta apenas se exerce sem concretizar em incidentes e com medidas de alcance muito limitado. Apesar de o TM clarificar a questão dos limiares no plano teórico, e de as medidas de retorção ser mais

intensas, estas não se orientaram a ilícitos concretos no ciberespaço, senão a um padrão de comportamento global. Ainda depois da publicação do TM2, segurança e resiliência continuam a avaliar-se como a capacidade mais eficaz contra as formas brandas de agressão.

A possibilidade de desenvolver campanhas de informação para construir uma mensagem efetiva que eleve os custos políticos do agressor também fica legitimada, sempre que não atinja o nível de "intervenção ilegal". Na prática, a legitimação do discurso próprio revela-se fulcral e a liberdade de discurso, apresentada como prova de veracidade, reforça a capacidade de comunicação daqueles que a permitem frente aos que não.

Na prática evidencia-se o papel fulcral da capacidade de defesa em todo o período. Depois da publicação do TM, o debate sobre a forma de emprego das capacidades começou a ganhar intensidade. Primeiro para a NATO adicionar valor às capacidades dos aliados, depois para integrar as cibercapacidades nacionais nas operações da Aliança.

Ao nos debruçarmos sobre a ambiguidade, antes de o TMP começar a possibilidade de aplicar o Artigo 5 no ciberespaço estava indefinida. Depois de o TM ter sido publicado e de se explicitar em Gales a determinação de empregar dito artigo, quando for necessário, a ambiguidade focalizou-se nas capacidades de resposta e na desnecessidade de responder em espécie. O TM, tinha deixado em nível tolerável a possibilidade de ser ambíguos quanto à interpretação dos limiares e quanto à origem da resposta, e praticamente irrestrita quanto à natureza das respostas. Estas vantagens foram aproveitadas pela NATO mantendo a definição dos limiares e a natureza das possíveis respostas propositadamente difusas, dentro dos limites da contenção e do Direito Internacional. Além disso, a Aliança afirmava a determinação de utilizar o seu leque completo de capacidades contra as ciberameaças.

Com o TM2 entravam em cena novas possibilidades de avaliação contextual. Também a possibilidade de avaliar em conjunto vários ciberataques para considerar ultrapassado um limiar que não ultrapassariam quando avaliados isoladamente. A possibilidade de aplicar no ciberespaço os Regimes Especiais do Direito Internacional trazia ainda um elemento de ambiguidade adicional. Assim, a ambiguidade foi contextualizando-se no cenário da resposta contra a guerra híbrida, e à desnecessidade de responder em espécie adicionou-se a determinação de responder com grupos integrados por capacidades de distinta natureza. Não se trata apenas de ser ambíguo em relação a qual será a capacidade com que se responderá, trata-se de responder com muitas medidas ao mesmo tempo, o que contribui para ultrapassar os efeitos secundários negativos da

imputação política, de algumas respostas ciber, da preservação das capacidades forenses, da monitorização, etc.

Em termos de cooperação a publicação do TM colocou em nível tolerável a filtragem de legitimidade para a dissuasão alargada, enquanto que trazia contributos relevantes para facilitar a imputação neste domínio complexo. A NATO não tardaria em declarar a aplicabilidade do Artigo 5, mas a estratégia de dissuasão no ciberespaço continuou fundamentalmente defensiva.

A publicação do TM2 facilitou mais a contribuição para a capacidade, e acrescentou a estabilidade em relação à segurança interdependente. Em consequência, abordou-se primeiro a construção de capacidades nacionais e da NATO, depois a cooperação para a construção de capacidades de aliados e parceiros e finalmente a integração de capacidades nacionais nas operações da Aliança. Em simultâneo, a cooperação com a indústria e outros parceiros na procura da segurança interdependente seguiu um percurso ascendente ao longo de todo o período. A procura de uma base de aceitação internacional crescente dos princípios e normas regentes do ciberespaço também foi um elemento permanente desta forma de segurança para o que o TMP contribuiu notavelmente.

Antes do começo do TMP há pouca evidência prática em termos de comunicação, o que reforça a ideia de carências contextuais para desenvolver uma estratégia dissuasória no ciberespaço. Porém, as interpretações do TM foram suficientes, pelo menos na teoria, para uma comunicação e sinalização apropriadas. A evolução prática da comunicação da capacidade e da determinação confirmou o que era previsível na perspectiva teórica. Possivelmente, a decisão para empregar o Artigo 5, seja o elemento de determinação mais relevante dos analisados. A determinação para respeitar, e exigir, a legalidade internacional e a estabilidade no ciberespaço foram uma constante em todo o período. O TM2 trouxe ainda contributos adicionais para a qualidade sinalizadora dos limiares e para a assimilabilidade das mensagens.

A evolução da sinalização correu paralela a estes avanços. Antes de o TMP ter começado a sinalização era difusa e estava orientada para as ameaças em termos genéricos. Já com o TMP a andar, o alvo estava mais concreto, mas as atitudes sinalizadas eram empacotadas e não individualizadas. A sinalização orientada à Rússia era dupla, de desconformidade com as suas ações e de dificuldade para perceber a sinalização russa, situação que se intensificou com a crise na Ucrânia. Entre outras medidas, os exercícios começariam a atingir uma verdadeira dimensão sinalizadora. Contudo, a complexidade das mensagens e dos atos sinalizadores impede isolar a sinalização orientada para o ciber das

orientadas para outros domínios. O habitual é sinalizar em pacote, mas com claridade, deixando sempre a porta aberta para o diálogo, marcando tempos e alternativas para o adversário adaptar as suas atitudes.

Em consequência, na dimensão teórica, o estudo permitiu verificar que os contributos dos manuais sobre as componentes do problema da dissuasão no ciberespaço são diferenciados a nível de indicador. Adicionalmente, permitiu ajustar a filtragem de legitimidade, para a inclusão de componentes numa estratégia dissuasória credível, também a nível de indicador.

Na dimensão da praxe internacional, o estudo permitiu verificar uma estreita correlação entre a inclusão e forma de aplicação dos elementos de dissuasão no ciberespaço e a evolução interpretativa da legitimidade na dimensão teórica.

Assim, ficou completamente verificada a primeira hipótese, e respondida a primeira pergunta derivada, entanto que ficou determinada a correlação temporária e a compatibilidade entre o Processo do Manual de Tallinn e a evolução de cada componente do problema da dissuasão no ciberespaço.

Depois de responder à primeira pergunta derivada, as respostas obtidas adotaram-se como base teórica para a segunda etapa de raciocínio dedutivo, que partiu da hipótese:

HIP2 - *A compatibilidade do Processo do Manual de Tallinn com as opções de dissuasão no ciberespaço decorre do seu impacto sobre as dificuldades de dissuasão consideradas e da adoção de uma opção de dissuasão alinhada sinergicamente com os contributos que o Processo traz para ultrapassar cada dificuldade.*

O processo dedutivo desenvolvido a partir da segunda hipótese permitiu verificar que a opção de dissuasão da NATO no ciberespaço assenta numa estratégia defensiva, sobre a que se adicionam elementos punitivos para acrescentar os custos potenciais do adversário. Todavia, este processo de adição não é livre, desde que está condicionado pela medida em que os elementos adicionados se percebam aceitáveis e legítimos pela comunidade internacional.

Em consequência, o estudo permitiu verificar a segunda hipótese no caso da dissuasão da NATO no ciberespaço, porque o Processo do Manual de Tallinn demonstrou-se compatível com as sucessivas opções de dissuasão adotadas no ciberespaço. Assim, ao longo do processo não se incluíram elementos na estratégia de dissuasão sem antes se apresentar os fundamentos que lhes permitissem ser legitimados pela comunidade

internacional. Este mecanismo permitiu o alinhamento sinérgico dos contributos do TMP para ultrapassar as dificuldades de dissuasão no ciberespaço com a fórmula adotada para construir em cada momento uma opção de dissuasão eficaz no ciberespaço.

Portanto, podemos responder à segunda pergunta de investigação afirmando que o TMP é plenamente compatível com a adoção de uma estratégia de dissuasão eficaz no ciberespaço. Ainda mais, o TMP constitui um importante elemento de referência no processo de decisão para incluir elementos na estratégia, o que se confirma observando a sincronia entre as interpretações dos Manuais e os elementos que passaram a formar parte da opção de dissuasão adotada em cada momento.

Até este ponto, respondeu-se à pergunta de partida, explicando em pormenor como é que a estratégia de dissuasão da NATO no ciberespaço se sincroniza com o Processo do Manual de Tallinn. Contudo, é necessário reconhecer que da estreita correlação entre as fundamentações jurídicas decorrentes do TMP e as opções de dissuasão adotadas pela NATO não é possível estabelecer uma relação causal. Sem dúvida, para afirmar ou infirmar a existência de uma tal relação causal seria necessária a análise da documentação classificada relativa ao assunto.

Adicionalmente, confirmou-se a importância de determinar as proporções em que se hão de adicionar os ingredientes na receita da dissuasão. Estas proporções evoluem com o tempo e com o contexto internacional, muito especialmente com perceção de legitimidade da comunidade internacional em relação aos assuntos em disputa. As Figuras 40, 41 e 42 (Apd-A) refletem a receita acumulada de todo o período em estudo, mas se consideramos períodos parciais obtemos variantes da receita condicionadas pelo contexto do período em que se enquadram.

Bibliografia.

Metodologia da investigação

Aracil, J. e Gordillo, F., 1997. *Dinámica de sistemas*. Reimpresão 2005, Madrid: Alianza Editorial.

Bryman, A., 2012. *Social Research Methods*. 4ª ed. Oxford: Oxford University Press.

Calduch C. R., 2014. *Métodos y técnicas de investigación internacional*.: [Livro electrónico] Madrid: Univiersidad Complutense de Madrid, 2ª Edición electrónica revisada y actualizada.

Csardi, G., 2015. *Package 'igraph' Documentation.* [Em linha] Disponível em: http://igraph.org/r/doc/igraph.pdf [Acedido em 08 Jul. 2018]

Fruchterman, TMJ e Reingold, E.M., 1991. Graph Drawing by Force-directed Placement. Software - *Practice and Experience*, 21(11):1129-1164. [Em linha] Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.13.8444&rep=rep1&type=pdf [Acedido em 08 Jul. 2018]

Kamada, T. e Kawai, S., 1989. An Algorithm for Drawing General Undirected Graphs. *Information Processing Letters*, 31/1, 7–15, 1989. [Em linha] Disponível em: https://pdfs.semanticscholar.org/b8d3/bca50ccc573c5cb99f7d201e8acce6618f04.pdf [Acedido em 08 Jul. 2018]

Neuman, W.L., 2007. *Basics of Social Research. Qualitative and Quantitative Aproaches.* Boston: Pearson Education, Inc. 2nd Ed.

Matias, R.M.X.F. dir., Santos, L.A.B., Proença Garcia, F.M.G.P., Monteiro, F.T., Vale Lima, J.M.M., Silva, N.M.P. Ferreira da Silva, J.C.V., Piedade, J.C.L., Pais dos Santos, R.J.R., Días Afonso, C.F.N.L., 2016. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação*. Lisboa: IUM.

Ognyanova, K., 2016. *Network Analysis and Visualization with R and igraph*. NetSciX 2016 School of Code Workshop, Wroclaw, Poland. [Em linha] Disponível em: http://www.kateto.net/wp-content/uploads/2016/01/NetSciX_2016_Workshop.pdf [Acedido em 09 Jul. 2018]

Popper, K., 1935. *The Logic of Scientific Discovery*. London: Routledge Classics, Ed. 2002.

Sampieri, R.H., Collado, C.F., Lucio, M.P.B., Valencia, S.M. e Torres, C.P.M., 2014a. *Metodología de la investigación.* México: McGRAW-HILL / Interamericana Editores, S.A. de C.V. Sexta edición.

Sampieri, R.H., Collado, C.F., Lucio, M.P.B., Valencia, S.M. e Torres, C.P.M., 2014b. *Metodología de la investigación. Cap. 4 del Centro de recursos online.* [Livro electrónico] México: McGRAW-HILL / Interamericana Editores, S.A. de C.V. Sexta edición. . [Em linha] Disponível em: http://highered.mheducation.com/sites/dl/free/1456223968/1058642/CAPITULO04.pdf [Acedido em 02 dic. 2017].

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research Methods for Business Students.* Essex: Pearson Education Limited. 6th ed.

Sigüeñas, S.M., *Técnicas de Minería de Textos para el Análisis de Discursos y Documentos.* Centro de Investigaciones Politológicas, Perú. [Em linha] Disponível em: http://independent.academia.edu/ManuelSig%C3%BCe%C3%B1as [Acedido em 04ago. 2018]

Strauss, A.L., Corbin, J.L., 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. London: SAGE Publications.

Torres, M.C., 2017. *Text Analytics para Procesado Semántico.* Trabajo Fin de Máster. Universidad de Vigo. [Em linha] Disponível em: http://eio.usc.es/pub/mte/descargas/ProyectosFinMaster/Proyecto_1475.pdf [Acedido em 05 ago. 2018].

Valdez, V., 2016. *Análisis de grafos usando R e igraph*. [Em linha] Disponível em: http://www.academia.edu/23701692/Análisis_de_grafos_usando_R_e_igraph [Acedido em 04jul. 2018]

Yin, R. K. (2013). *Case study research: Design and methods*. Thousand Oaks, EUA.: SAGE. (5ª. ed.)

Monografías

Artiles, N.G., 2010. La situación de la ciberseguridad en el ámbito internacional y en la OTAN. Em: Aguilar L.J., 2010. *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Madrid: Ministerio de Defensa.

Baptista, E.C., 2003. *O Poder Público Bélico em Direito Intenacional: o uso da força pelas Nações Unidas em Especial*. Coimbra: Almedina.

Barret, M., Bedford, D., Skinner, E., Vergles, E., 2011. *Assured access to the global commons*. Norfolk: Supreme Allied Command Transformation. North Atlantic Treaty Organization.

Bascoy, J.D. e Bouzá-Abril, B., 2017. War-Like Activities in the Cyberspace: Applicability of the Law of Armed Conflicts. Em: Ramirez, J.M. e Garcia-Segura, L.A., eds., 2017. *Cyberspace Risks and Benefits for Society, Security and Development*. s.l.: Springer International Publishing. Part III, pp.243-257.

Boulos, S., 2017. The Tallinn Manual and Jus ad bellum: Some Critical Notes.. Em: Ramirez, J.M. e Garcia-Segura, L.A., eds., 2017. *Cyberspace Risks and Benefits for Society, Security and Development*. s.l.: Springer International Publishing. Part III, pp.231-243.

Bejtlich, J., 2005. El Tao de la monitorización de seguridad en redes. Traduzido do inglês por s.n. Madrid: Pearson Educación, Pretince Hall.

Brodie, B., 1946. *The Absolute Weapon: Atomic Power and World Order.* New Haven, Connecticut: Yale Institute of International Studies.

Carr, J. 2010. *Inside Cyber Warfare*. Sebastopol, USA: O'Reilly Media Inc. 2nd Ed. 2011.

Casar Corredera, J.R., pres.; Gómez de Ágreda, A., coord.; Feliu Ortega, L.; Enriquez González, C.; López de Turiso y Sánchez, J.; Pastor Acosta, O.; Pérez Cortés, M., 2012. *El ciberespacio. Nuevo escenario de Confrontación.* Monografías del CESEDEN, Nº 126. Madrid: Ministerio de Defensa.

Cimbala, S.J., 1998. *Coercive Military Strategy*. Texas: A&M University Press.

Cortés, M.P., 2012. Tecnologías para la defensa en el ciberespacio. Em: Casar Corredera, J.R., pres., 2012. *El ciberespacio. Nuevo escenario de Confrontación.* Monografías del CESEDEN, Nº 126. Madrid: Ministerio de Defensa. Cap. 6.

Couto, A.C. 1988. *Elementos de Estrategia. Vol. II.* Lisboa: IAEM.

Espada, C.G. 1987. *El estado de necesidad y el uso de la fuerza en derecho internacional*. Madrid: Tecnos.

Even, S. e Siman-Tov, D., 2012. *Cyber Warfare: Concepts and Strategic Trends.* Memorandum 117 INNS. Tel Aviv: The Institute for National Security Studies. [Livro electrónico] Disponível em: http://cdn.www.inss.org.il.reblazecdn.net/upload/(FILE)1337837176.pdf [Acedido em 03 feb. 2013]

George, A. e Smoke, R. 1974. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia Uníversity Press.

Gómez de Ágreda, A., 2012. El ciberespacio como escenario de conflictos. Indentificación de las amenazas. Em: Casar Corredera., J.R., pres., 2012. *El ciberespacio. Nuevo*

escenario de Confrontación. Monografías del CESEDEN, Nº 126. Madrid: Ministerio de Defensa. Cap. 4.

Gray, C., 2003. *Maintaining Efective Deterrence*. Strategic Studies Institute. [Livro electrónico] Disponível em: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB211.pdf [Acedido em 22mar. 2013]

Greathouse, C.B., 2014. Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? Em Kremer J.F. e Muller, B. ed,s., *Cyberespace and International Relations*. *Theory*, *Prospects and Challenges*. Bonn: Springer.

Haass, R.N., 1998. *Intervention: The Use of American Military Force in the Post-Cold War World*. Washington, D.C.: Carnegie Endowment for International Peace, 1994.

Haffa, J.R. 1992. Future of Conventional Deterrence: Strategies and Forces to Underwrite a New World Order. Em Guertener, G.L., Haffa, J.R. e Quester, G., 1992. *Conventional Forces and the Future of Deterrence*. Pennsylvania: SSI.

Hijmans, E. y Wester, F. (2009). *Comparing the case study with other methodologies. Encyclopedia of Case Study Research.* [Livro electrónico] SAGE Publications.

Libicki, M.C., 2009a. *Cyberdeterrence and cyberwar*. [Livro electrónico] Santa Mónica: RAND Corporation. Disponível em: http://www.rand.org/pubs/monographs/MG877.html [Acedido em 04 dic. 2016].

Libicki, M.C., 2012. *Crisis and Escalation in Cyberspace.* [Livro electrónico] Santa Monica: Rand Coporation. Disponível em: http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf [Acedido em 22 nov 2016].

Machado, J.E.M., 2013. *Direito Internacional. Do paradigma clásico ao pós-11 de setembro*. Coimbra: Coimbra Editora. 4ª Ed.

Medero, G.S., 2010. *Los Estados y la ciberguerra*. Boletín de información del CESEDEN Nº 317. Madrid: CESEDEN.

Miranda, J., 2016. *Curso de Direito Internacional Público*. Cascais: Principia Editora. 6ª Ed. revisada e atualizada.

Mulinen, F., 1987., *Handbook on th law of War for Armed Forces*. Geneva: International Committee of the Red Cross.

Morgan, P.M., 1977. *Deterrence. A Conceptual Analysis.* London: SAGE Publications.

Morgan, P.M., 2003. Deterrence Now. Cambridge: Cambridge University Press.

Pape, R.A. 1996. *Bombing to Win: Air Power and Coercion in War*. Ithaca, N.Y.: cornell University press.

Quackenbush, S., 2011. *Understanding General Deterrence. Theory and Aplication*. New York: Palgrave Macmillan.

Retter, L., Hall, A., Black, J. e Ryan, N., 2016. The moral component of cross-domain conflict. [Livro eletronico] Cambridge, UK: RAND Corporation Europe. Disponível em: https://www.rand.org/pubs/research_reports/RR1505.html [Acedido em 14 dic. 2016].

Ribeiro, A.S., 2009. *Teoria geral da estratégia. O essencial ao processo estratégico*. Coimbra: Edições Almedina S.A.

Sanchez, J.L.T. 2012. La evolución del conflicto hacia um nuevo escenario bélico. Em: Casar Corredera., J.R., pres., 2012. *El ciberespacio. Nuevo escenario de Confrontación.* Monografías del CESEDEN, Nº 126. Madrid: Ministerio de Defensa. Cap. 3.

Schelling, T.C., 1966. *Arms and Influence*. New Haven and London: Yale University Press. Ed. 2008.

Schmitt, M. N., dir., ed. lit., Tikk, E., coord., ed., Arimatsu, A., Bernatchz, G., Cumming, P., Geib, R., Gill, T.D., Kleffner, J., Melzer, N., Watkin, K., Geers, K. e Ottis, R. 2013. *Tallinn Manual on the International Law Aplicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, M. N., dir. ed., Vihul, L., coord. ed., Akande, D., Brown, G.D., Ducheine, P., Gill, T.D., Heinegg, W.H., Hernandez, G., Housen-Couriel, D., Huang, Z., Jensen, E.T., Kittichaisaree, K., Kozik, A.L., Kreb, C., McCormack, T., Nakatani, K., Rona, G., Spector, P., Wats, S. e Blumberg, B., 2017. *Tallinn Manual 2.0 on the International Law Aplicable to Cyber Operations*. Cambridge: Cambridge University Press.

Smith, J.G., 2009. A Unified Field Theory for Full-Spectrum Operations: Cyberpower and the Cognitive Domain. Em: Wentz, L.K., Barry, C.L. e Starr, S.H., eds,s. 2009. *Military Perspectives on Cyberpower*. [Livro electrónico] Washington: National Defense University Center for Technology and National Security Policy. Disponível em: http://ctnsp.dodlive.mil/files/2009/07/Military-Perspectives-on-Cyber-Power.pdf [Acedido em 02 dic. 2016]

Snyder, G.H., 1961. *Deterrence and Defense: Toward a Theory of National Security*. Princeton: Princeton University Press.

U.S. Army War College. 2016. *Strategic Cyberspace Operations Guide.* [Livro electrónico] Carlise: U.S. Army War College, Centre for Strategic Leadership. Disponível em: http://www.csl.army.mil/usacsl/Publications/Strategic_Cyberspace_Operations_Guide_1_June_2016.pdf [Acedido em 12 dic.2016].

U.S. DoD, 2001. Joint Publication 1-02. *Dictionary of Military and Associated Terms.* Washington: US Government Pinting Office.

Yin, R.K., 2009. *Case Study Research, Desing and Methods.* [Livro electrónico] California: SAGE Publications, Inc. (4ª. ed.)

Zagare, F.C. e Kilgour, D.M., 2000. *Perfect Deterrence*. Cambridge: Cambridge University Press.

Trabalhos de investigação e artigos científicos e na imprensa especializada.

Applegate, S.D., 2013. The Dawn of Kinetic Cyber. Em: Podins, K., Stinissen, J. e M. Maybaum M., eds., 2013. *5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications. [Em linha] Disponível em: https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf [Acedido em 14 jun. 17].

Arnold A., 2013. Cyber "Hostilities" and the War Powers Resolution. *Military Law Review*, Vol. 217, pp.174-192.

Bascoy, J.D., 2013. "Ciberguerra y derecho: El ius ad bellum y el ius in bello en el ciberespacio". *Revista Espanola de Derecho Militar*, No. 100, 2013, pp. 151–197.

Bascoy, J.D., 2015. La ciberseguridad: aspectos jurídicos internacionales. Em: Universidad del País Vasco, 2015. *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2014.* Navarra: Editorial Aranzadi, SA.

Bendiek, A., 2016. *Due Diligence in Cyberspace.* Traduzido do Alemão por Genrich, T., SWP Research Paper Nº 7. Berlim: SWP German Institute for International and Security Affairs.. [Em linha]Disponível em: https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf [Acedido em 09 dic. 2016].

Boebert, W.E., 2010. A Survey of Challenges in Attribution. Em: Committee on Deterring Cyberattacks, 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. [livro electronico]

Washington: The National Academies Press. Pp.41-52. Disponivel em: https://www.nap.edu/download/12997 [Acedido em 22 mar. 2017].

Brodie, B., 1958. *The Anatomy of Deterrence*. Research Memorandum. s.l.: Rand Corporation.

Bustelo, R.V., 2017. *Compatibilidade das regras contidas no Manual de Tallinn com uma estratégia eficaz de dissuasão no ciberespaço*. Trabalho de investigação individual Curso Estado Maior Conjunto. IUM.

Carlin, J.P., 2016. Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats. *Harvard National Security Journal* / Vol. 7, pp.391-436.

Chayes, A., 2015. Rethinking Warfare: The Ambiguity of Cyber Attacks. *Harvard National Security Journal* / Vol. 6, pp.474-519.

Cimbala, S.J., 2014. Nuclear Deterrence and Cyber. The Quest for Concept. *Air & Space Power Journal*, March-April 2014, pp.87-107.

Cimbala, S.J., 2016. Nuclear Deterrence in Cyber-ia. Challenges and Controversies. *Air & Space Power Journal*, Fall 2016, pp.54-63.

Colarik, A. e Janczewski, L. 2012. *Establishing Cyber Warfare Doctrine*. Journal of Strategic Security Volume 5 Issue 1 2012, pp.31-48.

Crosston, M. D., 2011. World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. *Strategic Studies Quarterly*, Spring 2011, pp.100-116.

Davis, P.K., 2014. *Toward Theory for Dissuasion (or Deterrence) by Denial. Using Simple Cognitive Models of the Adversary to Inform Strategy*. S.l.: RAND NSRD. [Em linha] Disponível em: http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf [Acedido em 22 MAR 2017].

Davis, P.K., 2015. *Deterrence, Influence, Cyber Attack ad Cyberwar*. International Law and Politics, Vol. 47, pp.327-355.

Denning, D.E., 2015. Rethinking the Cyber Domainand Deterrence. *Joint Force Quarterly* 77, 2nd Quarter 2015, pp.8-16.

Dev, P.R., 2015. "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response.*Texas International Law Journal*, Vol. 50, Issue 2. pp 379-399.

Finnemore, M. e Sikkink, K., 1998. International Norm Dynamics and Political Change. *International Organization, International Organization at Fifty: Exploration and*

Contestation in the Study of World Politics. (Autumn, 1998), Vol. 52, No. 4. pp. 887-917. [Em linha] Disponível em: http://links.jstor.org/sici?sici=0020-8183%28199823%2952%3A4%3C887%3AINDAPC%3E2.0.CO%3B2-M [Acedido em 27 mar. 2017]

Finnemore, M. e Hollis, D.B., 2016. Constructing Norms for Global Cybersecurity. *The American Journal of International Law*, Vol. 110, No. 3 (July 2016), pp. 425-479. [Em linha] Disponível em: https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf [Acedido em 27 ago. 2018]

Garrie, D. e Reeves, S.R., 2016. An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors. *Cardozo Law Review*, Vol. 37. pp. 1827-1866.

Geers, K., 2012. Strategic Cyber Defense: Which Way Forward? *Journal of Homeland Security and Emergency Management.* Volume 9, Issue 1, Article 2.

Geist, Edward., 2015. Deterrence Stability in the Cyber Age. *Strategic Studies Quarterly*, Winter 2015, pp.44-61.

Godwin, J.B., Kulpin, A., Rauscher, K.F., e Yaschenko, V., 2014. *Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity*. East-West Institute, Policy Report 2/2014. [Em linha] New York: East-West Institute. Disponível em: https://www.eastwest.ngo/idea/critical-terminology-foundations-2 [Acedido em 04 abr. 2017].

Goldman, A.K., 2015. Navigating Deterrence: Law, Strategy and Security in the Twenty-first Century. *Journal of International Law and Politics.* Vol. 44. pp. 311-325.

Goodman, W., *Cyber Deterrence Tougher in Theory than in Practice?* Strategic Studies Quarterly, Fall 2010, pp.102-135.

Haney, C.D. 2015. *Strategic Deterrence for the Future*. Air & Space Power Journal, July–August 2015, pp.4-8.

Hare, F., 2009. *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?.* Conference on "The Virtual Battlefield: Perspectives on Cyber Warfare". Tallinn: CCDCOE. [Em linha] Disponível em: The Virtual Battlefield: Perspectives on Cyber Warfare (Proceedings 2009) | CCDCOE [Acedido em 24 mar. 2017]

Harknett, R.J., Callaghan, J.P., Kauffman, R. 2010. Leaving Deterrence Behind: War-Fighting and National Cybersecurity. *Journal of Homeland Security and Emergency Management*, Volume 7, Issue 1 2010 Article 22.

Healey, J., 2011. *Beyond Attribution: Seeking National Responsibility for Cyber Attacks.* Washington: The Atlantic Council of the United States. 2012. [Em linha] Disponível em: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF [Acedido em 24 mar. 2017]

Hjortdal, M., 2011. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, Volume IV Issue 2 2011, pp. 1-24

Iasiello, E., 2013 Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*. [Em linha] Vol. 7, Nº1, Art. 6, pp.54-67. Disponível em: http://scholarcommons.usf.edu/jss/vol7/iss1/6/ [Acedido em 20 may. 2017]

Ilves, L.K., Evans, T.J., Cilluffo, F.J. e Nadeau A.A., 2016 European Union and NATO Global Cybersecurity Challenges. PRISM 6, no. 2, pp.127-141.

Jasper, Scott. 2015. *Deterring Malicious Behavior in Cyberspace*. Strategic Studies Quarterly, Spring 2015, pp.60-85.

Jensen, E.T., 2012. *Cyber Deterrence*. *Emory International Law Review*, Vol. 26, pp. 773-823.

Keen, J.F., 2015. Conventional Military Force as a Response to Cyber Capabilities: on Sending Packets and Receiving Missiles. The Air Foce Law Review, Volume 73, pp.111-150.

Khan, Z. 2016. Strategizing for Deterrence Stability in South Asia: Seeking a Holistic Approach. *The Korean Journal of Defense Analysis* Vol. 28, No. 3, September 2016, pp.467－484.

Kolini, F. e Janczewski, L. 2015. *Cyber Defense Capability Model: A Foundation Taxonomy*. (2015). CONF-IRM 2015 Proceedings. Paper 32. AIS Electronic Library. [Em linha] Disponível em: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2015&sei-redir=1&referer=http%3A%2F%2Fscholar.google.es%2Fscholar%3Fstart%3D20%26q%3DNATO%2C%2BReport%2Bon%2BCyber%2BDefence%2BTaxonomy%2Band%2BDefinitions%26hl%3Des%26as_sdt%3D0%2C5%26as_vis%3D1#search=%22NATO%2C%20Report%20Cyber%20Defence%20Taxonomy%20Definitions%22 [Acedido em 09 dic 2016].

Lan, T. e Xin, Z., 2010. The View from China: Can Cyber Deterrence Work? Em: Nagorski, A. ed. 2010. *Global Cyber Deterrence: Views from China, the U.S.,*

Russia, India, and Norway. New York: The EastWest Institute. [Em linha] Disponível em: https://www.eastwest.ngo/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf [Acedido em 29mar. 2017]

Larsen, G.L. e Wheeler, D.A., 2003. *Techniques for Cyber Attack Attribution*. Virginia: Instituite for Defense Analyses. [Em linha] Disponível em: https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution [Acedido em 29mar. 2017]

Lewis, J.A., 2013. *Raising the Bar for Cybersecurity*. Washington: Center for Strategic and International Studies. [Em linha] Disponível em: https://www.csis.org/analysis/raising-bar-cybersecurity [Acedido em 21may. 2017]

Lewis, J.A., 2015. *The Role of Ofensive Cyberoperations in NATO's Collective Defense.* Tallinn Paper No. 8. [Em linha] Disponível em: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf [Acedido em 03 12 2016].

Libicki, M.C., 2009b. Sub Rosa Cyber War. Em CCDCOE, 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare*. [Em linha] Tallin: CCDCOE. Disponível em: https://ccdcoe.org/sites/default/files/multimedia/pdf/03_LIBICKI_Sub%20Rosa%20Cyber%20War.pdf [Acedido em 04 abr. 2017].

Margulies, P., 2013. Sovereignty and Cyber Attacks: Technology's Challenge to The Law of State Responsibility. *Melbourne Journal of International Law*, Vol. 14, pp.496-519.

Millás, V.M. 2017. Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico espanhol. *Boletín del Instintituto Español de Estudios Estratégicos, ieee.es.* [Em linha] Doc. 21/2017 Disponível em: http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO21-2017_DirectivaNIS_VicenteMoret.pdf [Acedido em 15 mar. 2017].

Monteiro da Silva, N.A.M., 2012. *O Desemvolvimento de Capacidades de Ciberdefesa.* Trabalho de Investigação do Curso de Estado-Maior Conjunto. LISBOA: IUM.

Nye, J. 2017. Deterrence and Dissuasion in Cyberspace. *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71. [Em linha] Disponível em: http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266 [Acedido em 30 dic. 2017].

Ottis, R., 2009. Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. Em: ECIW. 2009. *Proceedings of the 8th European Conference on Information Warfare and Security*. Lisbon: Academic Publishing Limited, 2009. pp 177-182.

Patterson, R. 2015. Silencing the Call to Arms: A Shift Away From Cyber Attacks as Warfare. *Loyola of Los Angeles Law Review,* Vol. 48. pp.969-1015.

Rid, T. e Buchanan, B., 2015. Attributing Cyber Attacks. *The Journal of Strategic Studies*, [Em linha] Vol. 38, Nos. 1–2, 4–37 Disponível em: https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf [Acedido em 28 mar.2017].

Robles Carrillo, M. 2016. El concepto de arma cibernética en el marco internacional: una aproximación funcional. *Boletín del Instintituto Español de Estudios Estratégicos, ieee.es.* [Em linha] Doc. 101/2016 Disponível em: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf [Acedido em 22 nov. 2016].

Schmitt, M.N., 2012. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal Online*, [Em linha] Vol. 54, pp.13-37. Disponível em: www.harvardilj.org/2012/12/online-articles-online_54_schmitt/ [Acedido em 20 dic. 2016].

Snyder, G. H. 1960, "Deterrence and Power," *Journal of Conflict Resolution*. [Em linha] Vol. 4, No. 2, pp. 163-178. Disponível em: https://www.jstor.org/stable/172650?seq=1#page_scan_tab_contents [Acedido em 26 abr. 2017].

Solomon, J., 2011. Cyberdeterrence between Nation-States. Plausible Strategy or a Pipe Dream?. *Strategic Studies Quarterly*. [Em linha] Spring 2011. Disponível em: http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf [Acedido em 02 dic. 2016].

Sterner, Eric. 2011. Retaliatory Deterrence in Cyberspace. Strategic Studies Quarterly, Spring 2011, pp.62-80.

Stockton, P., 2014. Cyber Deterrence. Infrastructure Resilience, Continuity Planning: and The Emerging Nexus. *Homeland Security Today Magazine.* October/November 2014. pp. 28-29.

Tikk, E., 2011. *Comprehensive legal approach to cyber security*. Dissertação de Doutoramento em Direito. Universidade de Tartu, Estonia.[Em linha] Disponível em: http://dspace.ut.ee/handle/10062/17914?locale-attribute=en [Acedido em 02 ene.

2018].

Trujillo, C. 2014. The Limits of Cyberspace Deterrence. *Joint Force Quarterly*. [Em linha] Vol. 75, 4th Quarter 2014, pp.43-52. Disponível em: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf [Acedido em 05 dic. 2016]

Veenendaal, M., Kaska, K. e Brangetto, P., 2016. *Is NATO Ready to Cross the Rubicon on Cyber Defence?* Cyber Policy Brief. Tallin: CCDCOE

Waxman, M.C., 2011. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *The Yale Journal of International Law*. Vol. 36. pp. 421-459.

Wilner, A.S., 2011. Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. *Journal of Strategic Studies*. [Em linha] Vol.34, 3-37. Disponível em: http://dx.doi.org/10.1080/01402390.2011.541760 [Acedido em 07 abr. 2017].

Textos oficiais, textos legais e outras fontes primárias escritas

Klimburg, A., ed., 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCDCOE.

NATO, 2013. Primary Directive on CIS Security, dated 15 November 2013 (NU) AC/35-D/2004-REV3. Norflok: NATO.

SACT, 2014. *Cyber Defence Taxonomy and Definitions*. AC/322-N(2014)0072 (NU) Norfolk: NATO.

NIST, 2013. *NISTIR 7298 Revision 2 Glossary of Key Information Security Terms.* Gaithersburg: National Institute of Standards and Technology, U.S. Department of Commerce. [Em linha] Disponível em: http://dx.doi.org/10.6028/NIST.IR.7298r2 [Acedido em 02 dic. 2017].

UE. 2013. *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. JOIN(2013) 1 final. Bruselas, 07 feb. 2013. [Em linha] Disponível em:https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001&from=en [Acedido em 08 ago. 2018]

UE. 2014. *La política y la gobernanza de Internet. El papel de Europa en la configuración de la gobernanza de Internet*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. COM(2014) 72 final. Bruselas, 02 dic. 2014. [Em linha] Disponível em: https://eur-

lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52014DC0072&from=ES [Acedido em 08 ago. 2018]

UN, 2001. *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. Ed. 2008. [Em linha] Disponível em: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Acedido em 09 may. 2017].

UN. 2003. *Resolución A/RES/58/32. Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional.* [Em linha] Disponível em: https://undocs.org/sp/A/RES/58/32 [Acedido em 29 dic. 2017].

UN. 2005. *Informe del Secretario General A/60/202. Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional.* [Em linha] Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/453/66/PDF/N0545366.pdf?OpenElement [Acedido em 29 dic. 2017].

UN. 2010. *Nota del Secretario General A/65/201. Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional*. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/60/PDF/N1046960.pdf?OpenElement [Acedido em 29 dic. 2017].

UN, 2011a. *Carta A/66/359 de fecha 12 de septiembre de 2011 dirigida al Secretario General por los Representantes Permanentes de China, la Federación de Rusia, Tayikistán y Uzbekistán ante las Naciones Unidas. Código internacional de conducta para la seguridad de la información.* [Em linha] Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/59/PDF/N1149659.pdf?OpenElement [Acedido em 28 mar. 2017].

UN, 2011b. Letter A/66/359 dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. [Em linha] Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/pdf/N1149656.pdf?OpenElement [Acedido em 18 may 2017].

UN. 2013. *Nota del Secretario General A/68/98. Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en*

el Contexto de la Seguridad Internacional. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/69/PDF/N1337169.pdf?OpenElement [Acedido em 29 dic. 2017].

UN, 2015a. *Carta A/69/723 de fecha 9 de enero de 2015 dirigida al Secretario General por los Representantes Permanentes de China, la Federación de Rusia, Kazajstán, Kirgistán, Tayikistán y Uzbekistán ante las Naciones Unidas. Código internacional de conducta para la seguridad de la información.* [Em linha] Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/05/PDF/N1501405.pdf?OpenElement [Acedido em 28 mar 2017].

UN. 2015b. *Nota del Secretario General A/70/174. Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/38/PDF/N1522838.pdf?OpenElement [Acedido em 29 dic. 2017].

UN. 2015c. *Resolución A/RES/70/237. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*. Disponível em: https://undocs.org/sp/A/RES/70/237 [Acedido em 29 dic. 2017].

UN. 2017. *Informe del Secretario General A/72/327. Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/257/49/PDF/N1725749.pdf?OpenElement[Acedido em 29 dic. 2017].

U.S. Congress. 2014. *Cybersecurity Enhancement Act of 2014*. (Public Law 113–274—Dec. 18, 2014). Washington, DC: U.S. Government Information GPO. [Em linha] Disponível em: https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf [Acedido em 19may. 2016].

U.S. DoD. 2011. *Department of Defence Strategy for Operating in Cyberspace.* U.S. Department of Defense. [Em linha] Disponível em: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [Acedido em 07 abr.2017].

U.S. DoD, 2015. *Department of Defense Strategy for Operating in Cyberspace*. [Em linha] Disponível em:

http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Acedido em 07 12 2016].

U.S. DoD, 2006. *Deterrence Operations Joint Operating Concept. Version 2.0.*

U.S. Government. 2015. *Cyber War: Definitions, Deterrence, and Foreign Policy*. Hearing Before the Committee on Foreign Affairs House of Representatives, One Hundred Fourteenth Congress, First Session, Serial No. 114–106. Washington: U.S. Government Publishing Office.

U.S. President. 2011. International Strategy For Cyberspace. [Em linha] Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Acedido em 19may. 2016].

U.S. President. 2015. *Promoting Private Sector Cybersecurity Information Sharing*. (Executive Order 13691 of February 13, 2015). Washington, DC: Federal Register. [Em linha] Disponível em: https://www.federalregister.gov/d/2015-03714 [Acedido em 30abr. 2016].

U.S. President's Commission on Critical Infrastructure Protection. 1997. *Toward Deterrence in the Cyber Dimension.* Report to the President's Commision on Critical Infrastructure Protection. Disponível em: EBSCO.

Corpus de fontes primárias da NATO codificadas e analisadas com R

Babst, S., 2011. *Security policies 2.0. – can Facebook, Twitter & co make an impact? A snapshot from NATO by Dr. Stefanie Babst, NATO's Deputy Assistant Secretary for Public Diplomacy. 20 Dec. 2011*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/news_82269.htm?selectedLocale=en [Acedido em 04jun. 2018].

Breedlove, P., 2014. *Opening statement by the Supreme Allied Commander Europe General Philip M. Breedlove, at the joint press point following the 171st NATO Chiefs of Defence meeting, 22 May. 2014.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_110223.htm?selectedLocale=en [Acedido em 06jun. 2018].

Appathurai, J., 2007a. *Press briefing by NATO Spokesman, James Appathurai 23 May. 2007*. NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_8313.htm?selectedLocale=en [Acedido em 10 mai. 2018].

Appathurai, J., 2007b. *Press briefing by the NATO Spokesman, James Appathurai on the Meetings of NATO Defence Ministers on 14 and 15 June 2007*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_8747.htm?selectedLocale=en [Acedido em 10 mai. 2018].

Appathurai, J., 2007c. *Press conference by NATO Spokesman, James Appathurai, 25 Oct. 2007*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_8562.htm?selectedLocale=en [Acedido em 10 mai. 2018].

Appathurai, J., 2008a. Weekly press briefing by NATO Spokesman, James Appathurai, 30 Jan. 2008. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7395.htm?selectedLocale=en [Acedido em 02jun. 2018].

Appathurai, J., 2008b. *Pre-summit press briefing by the NATO Spokesman James Appathurai, 26 Mar. 2008.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7597.htm?selectedLocale=en [Acedido em 02jun. 2018].

Appathurai, J., 2008c. *Weekly press briefing by the NATO Spokesman James Appathurai. 09 Apr. 2008.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7800.htm?selectedLocale=en [Acedido em 02jun. 2018].

Appathurai, J., 2009. Press briefing by NATO Spokesman, *James Appathurai*, 03 Apr. 2009. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_52841.htm?selectedLocale=en [Acedido em 02jun. 2018].

Appathurai, J., 2010. Weekly press briefing by NATO Spokesman James Appathurai, 11 Oct. 2010. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_68071.htm?selectedLocale=en [Acedido em 03 jun. 2018].

Flory, P., 2008. *Interview with NATO Assistant Secretary General for Defence Investment Peter Flory on NATO's work on missile defence, defence against terrorism and cyber defence, all issues which are high on the agenda for the Bucharest Summit, 28 Mar.*

2008. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7598.htm?selectedLocale=en [Acedido em 02jun. 2018]

Gottemoeller, R., 2017a. *Remarks by NATO Deputy Secretary General Rose Gottemoeller at the Coalition Warrior Interoperability Exercise (CWIX) at the Joint Force Training Centre in Bydgoszcz, Poland, 22 Jun. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_145260.htm?selectedLocale=en [Acedido em 08 jun. 2018].

Gottemoeller, R., 2017b. *Keynote address by NATO Deputy Secretary General Rose Gottemoeller at the NATO Information Assurance Symposium (NIAS) Cyber Conference, 19 Oct. 2017*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_147867.htm?selectedLocale=en [Acedido em 08 jun. 2018].

Gottemoeller, R., 2018a. *Defending the Treasure of Peace and Security: Keynote address by NATO Deputy Secretary General Rose Gottemoeller at the National Defence University in Istanbul, Turkey, 23 Jan. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_150987.htm?selectedLocale=en [Acedido em 08 jun. 2018].

Gottemoeller, R., 2018b. *The NATO you might not know - security and defence beyond the old basics: Brief by NATO Deputy Secretary General Rose Gottemoeller at a townhall meeting with students hosted by the Greek Association for Atlantic and European Cooperation, 02 Mar. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_152520.htm?selectedLocale=en [Acedido em 08 jun. 2018].

Gottemoeller, R. e Pavel, F., 2017. Joint press point between NATO Deputy Secretary General Rose Gottemoeller and the Prime Minister of Moldova, Pavel Filip, 08 Dec. 2017. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_149835.htm?selectedLocale=en [Acedido em 08 jun. 2018].

NATO, 2002. *Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic. 21 Nov. 2002.* NATO Official texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_19552.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2003. *Final Communiqué: Ministerial meeting of the North Atlantic Council Issued on 03 Jun. 2003*. NATO Official texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_20291.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2006a. *Comprehensive Political Guidance, Endorsed by NATO Heads of State and Government on 29 November 2006.* NATO Official texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_56425.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO,2006b. *Riga Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006.* NATO Official Texts. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_37920.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2007a. *NATO statement on Estonia, 03 May. 2007*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/news_7270.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2007b. *Final Communiqué: Meeting of the North Atlantic Council in Defence Ministers Session, 14 Jun. 2007*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/news_47011.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2007c. *Final comunique: Ministerial meeting of the North Atlantic Council held at NATO headquarters, Brussels, 07 Dec. 2007*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/news_47011.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2008a. *Bucharest Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008*. NATO Press Release. [Em linha] Disponível em:

https://www.nato.int/cps/ic/natohq/official_texts_8443.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2008b. *Final communiqué: Meeting of the North Atlantic Council at the level of Foreign Ministers held at NATO Headquarters, Brussels: 03 Dec. 2008*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_46247.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2008c. *Chairman's statement: Meeting of the NATO-Ukraine Commission at the level of Foreign Ministers held at NATO Headquarters, Brussels, 03 Dec. 2008*. Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_46249.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2009a. *Declaration on Alliance Security: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl on 4 April 2009*. Press Release. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/news_52838.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2009b. Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 04 Apr. 2009. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/news_52837.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2010a. NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, 17 May. 2010. NATO Official Texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_63654.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2010b. *New NATO division to deal with Emerging Security Challenges, 04 Aug. 2010*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/en/natolive/news_65107.htm [Acedido em 08 mai. 2018].

NATO, 2010c. *"Cyber Coalition 2010" to exercise collaboration in cyber defence, 16 Nov. 2010 - 18 Nov. 2010*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/news_68205.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2010d. *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon, 19 Nov. 2010.* NATO Official Texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_68580.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2010e. *Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 Nov. 2010.* NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_68828.htm?selectedLocale=en [Acedido em 08mai. 2018].

NATO, 2011a. *Joint statement at the meeting of the NATO-Georgia Commission at the level of Foreign Ministers in Berlin, Germany, 15 Apr. 2011.* NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_72697.htm?selectedLocale=en [Acedido em 08mai. 2018].

NATO, 2011b. *Joint statement at the meeting of the NATO-Ukraine Commission at the level of Foreign Ministers in Berlin, 15 Apr. 2011* . NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_72730.htm?selectedLocale=en [Acedido em 08mai. 2018].

NATO, 2011c. Joint Statement Meeting of the NATO-Georgia Commission at the level of Ambassadors, with the participation of the Prime Minister of Georgia, 09 Nov. 2011. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_80593.htm?selectedLocale=en [Acedido em 08mai. 2018].

NATO, 2012a. *Australia-NATO Joint Political Declaration. 14 Jun. 2012.* NATO Official Texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_94097.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2012b. *NATO Secretary General to visit the Baltic States, 19 Jan. 2012 - 20 Jan. 2012*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/news_83261.htm?selectedLocale=en&mode=pressrelease [Acedido em 08 mai. 2018].

NATO, 2012c. *Secretary General's Annual Report 2011, 26 Jan. 2012*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_82646.htm?selectedLocale=en [Acedido em 06 jun. 2018].

NATO, 2012d. *Chairman's statement: Meeting of the NATO-Russia Council at the level of Foreign Ministers held in Brussels on 19 April 2012.* NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_86211.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2012e. *Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_87593.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2012f. *Deterrence and Defence Posture Review, 20 May. 2012.* NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_87597.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2012g. *Summit Declaration on Defence Capabilities: Toward NATO Forces 2020, 20 May. 2012*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_87594.htm?selectedLocale=en [Acedido em 08 mai. 2018].

NATO, 2012h. *Individual Partnership and Cooperation Programme between New Zealand and NATO, 04 Jun. 2012.* NATO Official Texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_88720.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2012i. *NATO conducts annual crisis management exercise (CMX) and cyber coalition exercise, 12 Nov. 2012 - 16 Nov. 2012*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/news_91115.htm?selectedLocale=en&mode=pressrelease [Acedido em 08 mai. 2018].

NATO, 2013a. *Secretary General's Annual Report 2012, 31 Jan. 2013.* NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_94220.htm?selectedLocale=en [Acedido em 06jun. 2018].

NATO, 2013b. *Joint Political Declaration between Japan and the North Atlantic Treaty Organisation, 13 Apr. 2013.* NATO Official Texts. [Em linha] Disponível em: https://www.nato.int/cps/su/natohq/official_texts_99562.htm?selectedLocale=en [Acedido em 10 mai. 2018].

NATO, 2014a. *Secretary General's Annual Report 2013. 27 Jan. 2014. Foreword, Future NATO: Towards the 2014 Summit.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_106247.htm?selectedLocale=en [Acedido em 06jun. 2018].

NATO, 2014b. *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 Sep. 2014*. NATO Official texts. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm?selectedLocale=en [Acedido em 02 dic. 2016].

NATO, 2015a. *The Secretary General's Annual Report 2014. 30 Jan. 2015. Foreword, Keeping NATO strong.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_116854.htm?selectedLocale=en [Acedido em 06jun. 2018].

NATO, *2015b. Zero-Sum? Russia, Power Politics, and the post-Cold War Era: Session at the Brussels Forum with participation of NATO Secretary General Jens Stoltenberg, 20 Mar. 2015.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_118347.htm?selectedLocale=en [Acedido em 06jun. 2018].

NATO, 2015c. *Press briefing on NATO exercise Trident Juncture 2015 by the NATO Spokesperson together with the Commander of JFC Brunssum and the Chief of Staff of Allied Command Transformation, 15 Jul. 2015.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_121821.htm?selectedLocale=en [Acedido em 06jun. 2018].

NATO, 2016a. *"The Global Security Outlook" Session at the World Economic Forum with participation of NATO Secretary General Jens Stoltenberg , 22 Jan. 2016*. NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_127412.htm?selectedLocale=en [Acedido em 06jun. 2018].

NATO, 2016b. *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization . 08 Jul. 2016*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_133163.htm?selectedLocale=en [Acedido em 08may. 2018].

NATO, 2016c. *Commitment to enhance resilience: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, 08 Jul. 2016*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_133180.htm?selectedLocale=en [Acedido em 08may. 2018].

NATO, 2016d. Joint statement of the NATO-Georgia Commission at the level of Foreign Ministers, 8 July 2016, Warsaw, Poland. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_133175.htm?selectedLocale=en [Acedido em 08may. 2018].

NATO, 2016e. *Cyber Defence Pledge, 08 Jul. 2016*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_133177.htm?selectedLocale=en [Acedido em 08may. 2018].

NATO, 2016f. *Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. NATO Press Release. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#def-det2 [Acedido em 02 dic. 2016].

NATO, 2016g. *The Warsaw declaration on Transatlantic Security. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_133168.htm?selectedLocale=en [Acedido em 08may. 2018].

NATO, 2016h. *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. 06 Dec. 2016.*

NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/ic/natohq/official_texts_138829.htm?selectedLocale=en [Acedido em 08may. 2018].

NATO, 2017a. *Redefining Europe's Security Agenda: Panel discussion with NATO Secretary General Jens Stoltenberg at World Economic Forum Annual Meeting in Davos, 19 Jan. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_140226.htm?selectedLocale=en [Acedido em 06 jun. 2018].

NATO 2017b. *NATO Secretary General announces dates for 2018 Brussels Summit, 20 Oct. 2017.* NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/news_147856.htm?selectedLocale=en [Acedido em 07may. 2018].

NATO 2017c. *Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 05 Dec. 2017.* NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/official_texts_149522.htm?selectedLocale=en [Acedido em 07may. 2018].

NATO, 2018a. *Keynote speech by NATO Deputy Secretary General Rose Gottemoeller at the joint German Marshall Fund – Microsoft event on Countering Hybrid Threats (followed by panel discussion), 15 Feb. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_152155.htm?selectedLocale=en [Acedido em 08 jun. 2018].

NATO, 2018b. *Panel Discussion: "Defence Cooperation in the EU and NATO: More European, More Connected, More Capable?" at 2018 Munich Security Conference with participation of NATO Deputy Secretary General Rose Gottemoeller, 16 Feb. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_152237.htm?selectedLocale=en [Acedido em 08 jun. 2018].

NATO, 2018c. Joint Declaration on EU-NATO Cooperation by the President of the European NATO, 2018. Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 10 Jul. 2018. NATO Press Release. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en [Acedido em 14 ago. 2018].

NATO, 2018d. Brussels Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, 11 Jul. 2018. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en [Acedido em 14 ago. 2018].

NATO, 2018e. Brussels Declaration on Transatlantic Security and Solidarity, 11 Jul. 2018. NATO Press Release. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/official_texts_156620.htm?selectedLocale=en [Acedido em 14 ago. 2018].

Nauman, K. 2002. *Speech by the former Chairman of the NATO Military Committee at the NATO/GMFUS Conference*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_19711.htm?selectedLocale=en [Acedido em 10mai. 2018].

Panizzi, M., 2011. *The emerging security challenges under NATO's New Strategic Concept: Speech given by Brig. Gen. Massimo Panizzi, IMS Public Affairs and Strategic Communications Advisor, 16 Nov. 2011*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_81033.htm?selectedLocale=en [Acedido em 04jun. 2018].

Rasmussen, A.F., 2009. *Speech by NATO Secretary General Anders Fogh Rasmussen on emerging security risks, Lloyd's of London, 01 Oct. 2009*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_57785.htm?selectedLocale=en [Acedido em 02jun. 2018].

Rasmussen, A.F., 2010a. *Speech by NATO Secretary General Anders Fogh Rasmussen at Georgetown University, 22 Feb. 2010.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_61566.htm?selectedLocale=en [Acedido em 02jun. 2018].

Rasmussen, A.F., 2010b. Remarks by NATO Secretary General Anders Fogh Rasmussen at the fourth Strategic Concept Seminar on Transformation and Capabilities,

Washington DC, 23 Feb. 2010. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_61647.htm?selectedLocale=en [Acedido em 02jun. 2018].

Rasmussen, A.F., 2010c. *Speech by NATO Secretary General Anders Fogh Rasmussen at NATO's New Strategic Concept - Global, Transatlantic and Regional Challenges and Tasks Ahead - Warsaw, Poland, 12 Mar. 2010*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_62143.htm?selectedLocale=en [Acedido em 02jun. 2018].

Rasmussen, A.F., 2010d. Meeting Future Challenges Together: Speech by NATO Secretary General Anders Fogh Rasmussen at the Bucharest University, 07 May. 2010. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_63307.htm?selectedLocale=en [Acedido em 02jun. 2018].

Rasmussen, A.F., 2010e. *"Renewing the Transatlantic security community in the age of globalisation": Speech by NATO Secretary General Anders Fogh Rasmussen at the Central Military Club, Sofia, Bulgaria, 20 May. 2010.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_63773.htm?selectedLocale=en [Acedido em 02jun. 2018].

Rasmussen, A.F., 2010f. *The New Strategic Concept: Active Engagement, Modern Defence: Speech by NATO Secretary General Anders Fogh Rasmussen at the German Marshall Fund of the United States (GMF), Brussels, 08 Oct. 2010.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_66727.htm?selectedLocale=en [Acedido em 03jun. 2018].

Rasmussen, A.F., 2010g. Monthly press briefing by NATO Secretary General Anders Fogh Rasmussen, 11 Oct. 2010. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_66734.htm?selectedLocale=en [Acedido em 03jun. 2018].

Rasmussen, A.F., 2010h. "NATO, the Strategic Concept and the way forward", Keynote address by NATO Secretary General Anders Fogh Rasmussen to the participants of

the Lisbon 2010 Young Atlanticist Summit, 19 Nov. 2010. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_68499.htm?selectedLocale=en [Acedido em 03jun. 2018].

Rasmussen, A.F., 2011a. *"NATO and the OSCE: building security together", Speech by NATO Secretary General Anders Fogh Rasmussen at the OSCE in Vienna, 30 Jun. 2011*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_75886.htm?selectedLocale=en [Acedido em 04jun. 2018].

Rasmussen, A.F., 2011b. Towards NATO's Chicago Summit. Speech by NATO Secretary General Anders Fogh Rasmussen at the European Policy Centre, Brussels, 30 Sep. 2011. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_78600.htm?selectedLocale=en [Acedido em 04jun. 2018].

Rasmussen, A.F., 2012a. NATO – delivering security in the 21st century. Speech by NATO Secretary General Anders Fogh Rasmussen, Chatham House, London, 04 Jul. 2012. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_88886.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2012b. *Monthly press conference by the NATO Secretary General, 05 Nov. 2012*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_91135.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2012c. *Switzerland and NATO : partners in security. Speech by NATO Secretary General Anders Fogh Rasmussen at the Churchill Symposium in Zürich, Switzerland , 22 Nov. 2012*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_91490.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2013a. *NATO after ISAF – staying successful together: Remarks by NATO Secretary General Anders Fogh Rasmussen at the Munich Security Conference, 02 Feb. 2013*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_94321.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2013b. *Opening remarks by NATO Secretary General Anders Fogh Rasmussen at the meeting of the North Atlantic Council in Defence Ministers session, 04 Jun. 2013*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_101100.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2013c. *Press conference by NATO Secretary General Anders Fogh Rasmussen following the NATO Defence Ministers meeting on 4 June 2013.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_101151.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2013d. NATO: Ready, Robust, Rebalanced. Speech by NATO Secretary General Anders Fogh Rasmussen at the Carnegie Europe Event. 19 Sep. 2013. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_103231.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2013e. *Press conference by NATO Secretary General Anders Fogh Rasmussen following the meeting of the North Atlantic Council in Defence Ministers session. 22 Oct. 2013.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_104257.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2014a. Press conference by NATO Secretary General Anders Fogh Rasmussen following the first day of meetings of NATO Defence Ministers, 03 Jun. 2014. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_110618.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F., 2014b. *Press Conference by NATO Secretary General Anders Fogh Rasmussen following the meeting of the North Atlantic Council at the level of Heads of State and Government during the NATO Wales Summit, 05 Sep. 2014.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_112871.htm?selectedLocale=en [Acedido em 06jun. 2018].

Rasmussen, A.F. e Ilves, T.H., 2013. *Joint press point with NATO Secretary General Anders Fogh Rasmussen and President Ilves of Estonia, 18 Mar. 2013.* NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_99168.htm?selectedLocale=en [Acedido em 06jun. 2018].

Robertson, L., 2002. *"Building Security in an Uncertain World"*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_19884.htm?selectedLocale=en [Acedido em 09 ago. 2018].

Scheffer, J.H., 2007. Speech by NATO Secretary General, Jaap de Hoop Scheffer at the Conférence de Montréal (13th International Economic Forum of the Americas), 21 Jun. 2007. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_8780.htm?selectedLocale=en [Acedido em 10 mai. 2018].

Scheffer, J.H., 2008a. *Speech by NATO Secretary General, Jaap de Hoop Scheffer at the annual press reception on the occasion of the New Year, 10 Jan. 2008*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7374.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008b. *Looking ahead to NATO's Bucharest Summit: Speech by NATO Secretary General Jaap de Hoop Scheffer at Bucharest University, Romania, 11 Jan. 2008.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_1298.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008c. *Press conference by NATO Secretary General, Jaap de Hoop Scheffer following the informal meeting of NATO Defence Ministers, 08 Feb. 2008.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7523.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008d. *Speech by NATO Secretary General, Jaap de Hoop Scheffer, at the 44th Munich Security Conference, 09 Feb. 2008.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7527.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008e. *Beyond the Bucharest Summit: Speech by NATO Secretary General, Jaap de Hoop Scheffer, at the Brussels Forum of the George Marshall Fund (GMF), 15 Mar. 2008.* NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_7566.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008f. Press conference by NATO Secretary General Jaap de Hoop Scheffer, following the North Atlantic Council Summit meeting, 03 Apr. 2008. . NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7619.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008g. *Press conference by NATO Secretary General Jaap de Hoop Scheffer after the Meeting of the North Atlantic Council at the level of Foreign Ministers, 19 Aug. 2008*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_7903.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2008h. *Today's NATO, and why it matters: Speech by NATO Secretary General Jaap de Hoop Scheffer Lloyd's City Dinner, 05 Sep. 2007*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_8471.htm?selectedLocale=en [Acedido em 10 mai. 2018].

Scheffer, J.H., 2008i. *Opening statement by NATO Secretary General Jaap de Hoop Scheffer at the meeting of the NATO-Georgia Commission with invitees, 09 Oct. 2008*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_47175.htm?selectedLocale=en [Acedido em 02jun. 2018].

Scheffer, J.H., 2009. *Speech by NATO Secretary General Jaap de Hoop Scheffer at the meeting of the NATO Parliamentary Assembly, Oslo, 26 May 2009.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_55133.htm?selectedLocale=en [Acedido em 02jun. 2018].

Shea, J., 2009. *Lecture 3 - International terrorism: is it still a strategic threat? by Dr Jamie Shea, Director of Policy Planning in the Private Office of the Secretary General, 22 Dec. 2009*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_84764.htm?selectedLocale=en [Acedido em 02jun. 2018].

Shea, J., 2010. *Lecture 6 - Cyber attacks: hype or an increasing headache for open societies? by Dr Jamie Shea, Director of Policy Planning in the Private Office of the*

Secretary General, 02 Feb. 2010. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_84768.htm?selectedLocale=en [Acedido em 02jun. 2018].

Stoltenberg, J., 2015a. *Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar, 25 Mar. 2015.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_118435.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2015b. *Remarks by NATO Secretary General Jens Stoltenberg before the European Parliament's Foreign Affairs Committee and Sub-committee on Security and Defence (followed by Q&A session), 30 Mar. 2015.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_118576.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2015c. *Adapting to a changed security environment Speech by NATO Secretary General Jens Stoltenberg at the Center for Strategic and International Studies (CSIS) in Washington D.C. (incl. Q&A session), 27 May. 2015.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_120166.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016a. *Remarks by NATO Secretary General Jens Stoltenberg at the European Parliament Committee on Foreign Affairs and its Subcommittee on Security and Defence, 23 Feb. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_128311.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016b. The Warsaw Summit: Strengthening NATO in turbulent times: Speech by NATO Secretary General Jens Stoltenberg at Warsaw University, 31 May. 2016. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_131724.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016c. Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers

"Projecting stability", 15 Jun. 2016. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_132492.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016d. *Press conference by NATO Secretary General Jens Stoltenberg following the meetings of the North Atlantic Council at the level of Heads of State and Government, 08 Jul. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_133276.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016e. *The Three Ages of NATO: An Evolving Alliance. Speech by NATO Secretary General Jens Stoltenberg at the Harvard Kennedy School, 23 Sep. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_135317.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016f. *A strong transatlantic bond in uncertain times. Speech by NATO Secretary General Jens Stoltenberg at an event hosted by the German Marshall Fund of the United States (GMF), 18 Nov. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_137727.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016g. *Address by NATO Secretary General Jens Stoltenberg at the Plenary session of the NATO Parliamentary Assembly Fall session in Turkey, 21 Nov. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_137787.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016h. *Keynote speech by NATO Secretary General Jens Stoltenberg at the Oxford Union, 24 Nov. 2016*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_137882.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016i. *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the NATO-Ukraine Commission at the level of Foreign Ministers, 07 Dec. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_138760.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2016j. *Keynote address by NATO Secretary General Jens Stoltenberg to commemorate the 60th anniversary of the Three Wise Men Report, Norway House, Brussels, 13 Dec. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_139357.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2017a. *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers, 16 Feb. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_141340.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2017b. *Press conference by the NATO Secretary General Jens Stoltenberg at the launch of his Annual Report for 2016, 13 Mar. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_142141.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2017c. *Press conference by NATO Secretary General Jens Stoltenberg following the meetings of the North Atlantic Council and the NATO-Ukraine Commission at the level of Foreign Ministers, 31 Mar. 2017*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_142789.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2017d. *Remarks by NATO Secretary General Jens Stoltenberg at the Elliott School of International Affairs, George Washington University, 13 Apr. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_143137.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2017e. *Speech by NATO Deputy Secretary General Rose Gottemoeller at the NATO Parliamentary Assembly session, 29 May. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_144090.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J., 2017f. *Press conference by NATO Secretary General Jens Stoltenberg ahead of the meeting of NATO Defence Ministers, 28 Jun. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017g. Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers. 29 Jun. 2017. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_145385.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017h. *Doorstep by NATO Secretary General Jens Stoltenberg prior to the informal meeting of EU Ministers of Defence, Tallinn, Estonia. 07 Sep. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_146642.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017i. *Speech by NATO Secretary General Jens Stoltenberg at the Plenary session at the NATO Parliamentary Assembly in Bucharest, 09 Oct. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_147635.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017j. *The geography of danger has shifted: Speech by NATO Secretary General Jens Stoltenberg at the Japan National Press Club, 31 Oct. 2017*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_148125.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017k. *Press point by NATO Secretary General Jens Stoltenberg at ASAN Institute for Policy Studies, Seoul, Repubic of Korea, 02 Nov. 2017*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_148211.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017l. *Pre-ministerial press conference by NATO Secretary General Jens Stoltenberg before the meeting of the North Atlantic Council at the level of Defence Ministers, 07 Nov. 2017*. NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_148359.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017m. *Press conference by NATO Secretary General Jens Stoltenberg following the the meeting of the North Atlantic Council at the level of Defence Ministers, 08 Nov. 2017*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_148417.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017n. Doorstep statement by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Foreign Ministers, 05 Dec. 2017. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_149332.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2017o. Adapting NATO in an Unpredictable World, Speech by NATO Secretary General Jens Stoltenberg at the École militaire in Paris, 19 Dec. 2017. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_150337.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018a. Continually adapting to a changing world: Lecture by NATO Secretary General Jens Stoltenberg at the Centro Superior de Estudios de la Defensa Nacional in Madrid, 25 Jan. 2018. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_151093.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018b. *Press conference by NATO Secretary General Jens Stoltenberg after a meeting of NATO defence ministers, 14 Feb. 2018.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_151504.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018c. *Press conference by the NATO Secretary General Jens Stoltenberg at the launch of his Annual Report for 2017, 15 Mar. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_152678.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018d. *Remarks by NATO Secretary General Jens Stoltenberg at a Town Hall event at the University of Ottawa, 04 Apr. 2018.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_153389.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018e. *Remarks by NATO Secretary General Jens Stoltenberg at the Town Hall Event at the Southern Methodist University in Dallas, 05 Apr. 2018.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_153429.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018f. *Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris), 15 May. 2018.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_154462.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J., 2018g. *Address by NATO Secretary General Jens Stoltenberg to the NATO Parliamentary Assembly, Warsaw, Poland, 28 May. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_154899.htm?selectedLocale=en [Acedido em 14ago. 2018].

Stoltenberg, J., 2018h. *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council (NAC) in Defence Ministers' session, 07 Jun. 2018*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_155264.htm?selectedLocale=en [Acedido em 14ago. 2018].

Stoltenberg, J., 2018i. *Speech by NATO Secretary General Jens Stoltenberg (hosted by the Foreign and Commonwealth Office at Lancaster House), 21 Jun. 2018.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_156142.htm?selectedLocale=en [Acedido em 14ago. 2018].

Stoltenberg, J., 2018k. Press conference by NATO Secretary General Jens Stoltenberg ahead of the NATO Summit Brussels, 10 Jul. 2018. NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_156729.htm?selectedLocale=en [Acedido em 14ago. 2018].

Stoltenberg, J., 2018l. Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Heads of State and Government (NATO Summit Brussels), 11 Jul. 2018. Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_156733.htm?selectedLocale=en [Acedido em 14ago. 2018].

Stoltenberg, J. e Johnson, B., 2018. *Joint press point with NATO Secretary General Jens Stoltenberg and UK Foreign Secretary Boris Johnson, 19 Mar. 2018.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_153049.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J. e Ilves, T.H., 2014. *Doorstep statement by NATO Secretary General Jens Stoltenberg meeting with President Toomas Ilves of Estonia, 20 Nov. 2014*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_114973.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J. e Mikser, S., 2014. *Joint press point with NATO Secretary General Jens Stoltenberg and Sven Mikser, Minister of Defence of Estonia, 20 Nov. 2014.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_115063.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J. e Mogherini, F., 2015. *Doorstep statements by NATO Secretary General Jens Stoltenberg and EU High Representative Federica Mogherini before the meeting of NATO Foreign Ministers on cooperation with the European Union, 20 May. 2016*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_131283.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J. e Mogherini, F., 2016. *Doorstep statements by NATO Secretary General Jens Stoltenberg and EU High Representative Federica Mogherini before the meeting of NATO Foreign Ministers on cooperation with the European Union, 20 May. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: *https://www.nato.int/cps/en/natohq/opinions_131283.htm?selectedLocale=en*

[Acedido em 08jun. 2018].

Stoltenberg, J. e Mogherini, F., 2017. *Remarks by NATO Secretary General Jens Stoltenberg at the Inauguration of the Helsinki Centre of Excellence for Countering Hybrid Threats, with EU High Representative Federica Mogherini, 02 Oct. 2017.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_147499.htm?selectedLocale=en [Acedido em 08jun. 2018].

Stoltenberg, J. e Paloméros J-P., 2015. *Joint press conference with NATO Secretary General Jens Stoltenberg and Supreme Allied Commander Transformation General Jean-Paul Paloméros, 25 Mar. 2015*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_118436.htm?selectedLocale=en [Acedido em 06jun. 2018].

Stoltenberg, J. e Trudeau, J., 2018. *Joint press conference with NATO Secretary General Jens Stoltenberg and the Prime Minister of Canada, Justin Trudeau, 04 Apr. 2018. NATO Speeches & transcripts.* [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_153391.htm?selectedLocale=en [Acedido em 08jun. 2018].

Vershbow, A., 2013. *Challenges facing NATO and the Transatlantic Community post-2014. Address by Ambassador Alexander Vershbow NATO Deputy Secretary General at the 30th International Workshop on Global Security, Hôtel national des invalides – Paris, France, 24 June 2013*. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_101606.htm?selectedLocale=en [Acedido em 02jun. 2018].

Vershbow, A., 2014. *Opening remarques by NATO Deputy Secretary General Alexander Vershbow at the 2014 NATO Industry Forum, Croatia, 13 Nov. 2014.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_114729.htm?selectedLocale=en [Acedido em 06jun. 2018].

Vershbow, A., 2016a. 21st Century Deterrence: Remarks by NATO Deputy Secretary General Alexander Vershbow at the Snow Meeting in Trakai, Lithuania, 15 Jan. 2016. NATO Speeches & transcripts. [Em linha] Disponível em:

https://www.nato.int/cps/en/natohq/opinions_127099.htm?selectedLocale=en [Acedido em 06jun. 2018].

Vershbow, A., 2016b. *NATO at 67: What (complex) agenda for NATO's Warsaw Summit? Remarks by NATO Deputy Secretary General Alexander Vershbow to The Netherlands Atlantic Association and Netherlands Atlantic Youth, The Hague, 08 Apr. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_129816.htm?selectedLocale=en [Acedido em 06jun. 2018].

Vershbow, A., 2016c. *NATO stands with Ukraine. Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Kyiv Security Forum, Kyiv, Ukraine, 14 Apr. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_129964.htm?selectedLocale=en [Acedido em 06jun. 2018].

Vershbow, A., 2016d. *Remarks by NATO Deputy Secretary General Ambassador Alexander Vershbow at The National Library of Romania, Bucharest, 26 Apr. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_130415.htm?selectedLocale=en [Acedido em 06jun. 2018].

Vershbow, A., 2016e. *An Alliance For Our Times: NATO and its Partners in a "World Disrupted": Keynote address by NATO Deputy Secretary General Alexander Vershbow at the International Security Forum, Geneva, 13 Jun. 2016.* NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_132337.htm?selectedLocale=en [Acedido em 06jun. 2018].

Vershbow, A., 2016f. NATO in Transatlantic Security Policy. Keynote Address by NATO Deputy Secretary General Ambassador Alexander Vershbow at the 3rd Annual Helsinki Summer Session Finnish Institute of International Affairs, Helsinki. 01 Sep. 2016. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_134541.htm?selectedLocale=en [Acedido em 02jun. 2018].

Wijk, R., 2009. Speech by Prof. Dr. Rob de Wijk on NATO's new Strategic Concept, MCCS Lisbon, 19 Sep. 2009. NATO Speeches & transcripts. [Em linha] Disponível em: https://www.nato.int/cps/en/natohq/opinions_58107.htm?selectedLocale=en [Acedido em 02jun. 2018].

Entrevistas e declarações

Alexander, K., 2010. Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command. [Em linha] Disponível em: https://fas.org/irp/congress/2010_hr/041510alexander-qfr.pdf [Acedido em 31 mar. 17].

Ágreda, A.G., 2017. *Entrevista al Ilmo. Sr. Coronel Angel Gómez de Ágreda, Jefe de Área de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa del Ministerio de Defensa de España.* Madrid (11 dic. 2017)

Bascoy, J.D., 2017. *Entrevista al Excmo. Sr. General Auditor Jerónimo Dominguez Bascoy, Vocal Togado del Tribunal Militar Central.* Madrid (14 dic. 2017)

Cubeiro C., E. 2017 *Entrevista al Capitán de Navío Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa.* Madrid (11 dic. 2017)

Rodriguez, M., 2017. *Declaration by Miguel Rodríguez, Representative of Cuba, at The Final Session of Group of Governmental Experts on Developments in The Field of Information and Telecommunications in The Context of International Security*. New York, (23 jun. 2017). [Em linha] Disponível em: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf [Acedido em 01 ene. 2018].

Thomas, T.L. 2017. Statement on Russia's Information War Concepts. Em: U.S. House of Representatives, Armed Services Committee. *Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment.* [Em linha] Disponível em: https://armedservices.house.gov/legislation/hearings/crafting-information-warfare-and-counter-propaganda-strategy-emerging-security [Acedido em 10 abr. 2017]

Páginas web e artigos

ASSER Institute, 2016. *The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime*. ASSER Institute, Centre for International and European Law. [Em linha] Disponível em: http://www.asser.nl/media/2878/report-on-the-tallinn-manual-20-and-the-hague-process-3-feb-2016.pdf [Acesso em 29 dic. 2017].

CCDCOE, s.d.a. *Cyber Defence Training*. Tallinn: CCDCOE. [Em linha]Disponível em: https://ccdcoe.org/training.html [Acesso em 03 dic. 2016].

CCDCOE, s.d.b. *Research*. Tallinn: CCDCOE. [Em linha] Disponível em: https://ccdcoe.org/research.html [Acedido em 03 dic. 2016].

CCDCOE, s.d.c. *Tallinn Manual Process*. Tallinn: CCDCOE. [Em linha] Disponível em: https://ccdcoe.org/tallinn-manual.html [Acedido em 03 dic. 2016].

CCDCOE, s.d.d. *Tallinn Manual Process*. Tallinn: CCDCOE. [Em linha] Disponível em: https://ccdcoe.org/tallinn-manual.html [Acedido em 29 dic. 2017].

CCDCOE, 2015. *Legal Order as Deterrence in Cyberspace*. Tallinn: CCDCOE. [Em linha] Disponível em: https://ccdcoe.org/legal-order-deterrence-cyberspace.html [Acedido em 29 dic. 2017].

CCDCOE, 2016. *Over 50 States Consult Tallinn Manual 2.0.* Tallinn: CCDCOE. [Em linha] Disponível em: https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html [Acedido em 13 dic. 2017].

Codner, M., 2009. *Defining Deterrence. Framing Deterrence in the 21st Century.* Pre-conference Note. London:RUSI. [Em linha] Disponível em: https://rusi.org/system/files/Defining_Deterrence_-_A_Pre-Conference_Note.pdf [Acedido em 22 mar. 2017].

Deeks, A. 2015. Tallinn 2.0 and a Chinese View on the Tallinn Process. Lawfare. [Em linha] Disponível em: https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process# [Acedido em 03 dic. 2016].

Flanagan, B., 2011. Former CIA chief speaks out on Iran Stuxnet attack. *The National*. [Em linha] Vol. 15Dec.2015. Disponível em: . http://www.thenational.ae/thenationalconversation/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack [Acedido em 5 abr. 2017].

Hvistendahl, M., 2016. The Decline in Chinese Cyberattacks: The Story Behind the Numbers. *MIT Technology Review*. [Em linha] Disponível em: https://www.technologyreview.com/s/602705/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers/ [Acedido em 24 mar. 2017]

Knopf, J.W., 2010. The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, [Em linha] Vol.31, No.1 (April 2010), pp.1–33 Disponível em: http://hdl.handle.net/10945/38341 [Acedido em 20may. 2017]

Lynn III, W.L. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *United States Cyber Comand: Cyber Security* [Em linha] Disponível em:

http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx [Acedido em 04 mar. 2013].

Rõigas, H. 2015. An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?. *CCDCOE INCYDER database.* [Em linha] Doc. 101/2016 Disponível em: https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html [Acedido em 12 dic. 2016].

Schmitt, M. e Vihul, M., 2017. *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms.* New York: Just Security. [Em linha] Disponível em: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [Acedido em 07 dic. 2017].

Stark, H., 2011. Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War. *Spiegel Online International*. [Em linha] Vol. 08Ago.2011. Disponível em: http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912-2.html [Acedido em 05 abr. 2017].

Waxman, M. e Shany, Y., 2017. *Approaches to International Cyberlaw: A View from Israel. S.l.: The Lawfare Institute*. [Em linha] Disponível em: https://www.lawfareblog.com/approaches-international-cyberlaw-view-israel [Acedido em 28 dic. 2017].

Anexo A — Variáveis e fundamentação de indicadores de Bustelo (2017, Apd-B)

B.1. O problema da ambiguidade

Os limiares entre os espaços de manobra de dois atores com interesses em conflito normalmente assentam em questões legais, em precedentes e em analogias, mas também têm uma componente de arbitrariedade. Devem permitir reconhecer a cada oponente o espaço de manobra que lhe é permitido e distinguir as novas iniciativas do adversário daquelas que já vinha desenvolvendo. Portanto, cada oponente procurará conhecer com a maior exatidão possível onde é que o adversário colocou o limiar. Com essa finalidade, realizarão atividades de reconhecimento das capacidades e determinações dos adversários, com o conseguinte risco de escalada da tensão. Para deter estas atividades o defensor deve transmitir imprevisibilidade nas suas respostas para escalar a confrontação, de forma a manter o adversário longe do último patamar para atingir a guerra. (Schelling, 1966, p.93,96,135)

Portanto, num ambiente de grande complexidade como o ciberespaço, onde não é fácil fixar o limiar desencadeante da represália, a ambiguidade permite flexibilidade situacional ao defensor. Mas também contribui para a credibilidade, pois se o limiar fosse nítido, e quando ultrapassado não houvesse represália, a credibilidade decairia. (Solomon, 2011, p.3)

A maior necessidade de flexibilidade situacional no ciberespaço decorre da disjunção entre o propósito do atacante, os efeitos reais e a percepção do acontecido pelo atacado, mas também da dificuldade de identificar autores, alvos e intenções (Libicki, 2012, pp.iii,26).

B.2. Ataque armado

Desde que não há uma norma internacional que defina o que é um ciberataque nem quais as condições que constituem um "ataque armado", o limiar desencadeante da represália pode ser definido em relação aos princípios do direito internacional, mas no ciberespaço são possíveis muitas formas de ataque que não atingem esse limiar, e outras que sendo potencialmente muito graves deviam permitir uma equiparação, por exemplo a implantação de ciberarmas nos sistemas dos potenciais oponentes (Cortés, 2012, pp.274,275). Portanto, sendo o leque de gravidade das agressões a dissuadir muito extenso, também o deve ser o de possíveis respostas (U.S. President, 2011, pp.13,14).

Por outro lado, em alguns casos, o atacante visando erodir com o ataque certas capacidades, económicas, diplomáticas, etc., procurará ocultar o ataque, colocando assim ao defensor, caso o detecte, numa situação difícil para justificar uma possível represália. Outras vezes pode ser o defensor, quem simule não ter detectado o ataque, para eludir responder sem perder credibilidade por não o fazer. (Solomon, 2011, p.12,13)

B.3. A dificuldade de atribuição

Este problema está inerente na própria estrutura do ciberespaço, originariamente pouco orientado à segurança. Com a expansão do domínio, e a aparição dos primeiros ciberincidentes, começaram a empregar-se meios técnicos de informática forense para identificar aos autores materiais, mas logo começaram a revelar-se insuficientes, agravando-se a situação à medida que os Estados começaram a orientar estratégias para o ciberconflito.

Duma perspectiva técnica, as limitações para a atribuição inerentes ao ciberespaço incluem a demora do processo de atribuição, a impossibilidade de atribuir o ataque e a atribuição incorreta, sendo que esta última pode ser consequência da intencionalidade direta do atacante, por exemplo para envolver terceiros no conflito. Adicionalmente apresentam-se outras dificuldades como a necessidade de tecnologia de difícil acesso, os elevados custos, as limitações legais ou políticas para o emprego de todos os meios disponíveis, o carácter invasivo ou ofensivo de algumas técnicas forenses ou a necessidade de respeitar a privacidade e a liberdade de discurso (Larsen e Wheeler, 2003). Todavia, se o processo forense tivesse êxito, revelar a técnica empregue dificultaria a sua reutilização e contribuiria para melhor a técnica do atacante, e para acrescentar o seu esforço para apagar as evidências forenses (Libicki, 2009a, pp.49,50).

O aumento da ameaça e a previsão de as dificuldades técnicas se prolongar no futuro demandam novas abordagens de caráter mais político. A capacidade de atribuição é fulcral para qualquer estratégia de dissuasão, mas a atribuição técnica perfeita não é imprescindível (Boebert, 2010, pp.50-51). A atribuição deve avaliar-se a nível técnico, mas também a nível operacional para compreender o ataque, e a nível estratégico para decidir a resposta. Aqui o Estado deve definir a atribuição em função do jogo político. (Rid e Buchanan, 2015, pp. 4,7,34)

Partindo de uma abordagem política, Jason Healey (2011) propõe aplicar um esquema de atribuição imperfeita assente numa escala de responsabilidade estatal de dez níveis. A aplicação deste critério permitiria aos Estados aplicar as respostas coercitivas tradicionais, e retornar à simetria Estado-Estado no ciberespaço. Em troca exige grandes esforços em políticas de cibersegurança para se proteger das culpas decorrentes de ações dos seus cidadãos ou de elementos incontrolados desde o ciberespaço sob a sua soberania. Também

obrigaria a cooperar com aqueles países incapazes de aplicar políticas de segurança adequadas. E ainda podia ser o pretexto para alguns governos censurarem os direitos civis. Para além disso obrigaria o setor privado a aplicar políticas de segurança muito custosas, para dar resposta a um assunto por eles considerado como inerentemente militar ou de segurança pública (Solomon, 2011, p.7), embora as dimensões da cibersegurança corporativa e da ciberdefesa sejam dificilmente dissociáveis (Garrie e Reeves, 2016, pp.1852).

B.4. O problema da capacidade

No quadro da dissuasão nuclear, embora aplicável a qualquer estratégia de dissuasão, Brodie (1958, p.5) salientava a anomalia da dissuasão quanto às capacidades: O êxito de qualquer estratégia de dissuasão assenta em que não chegue a ser preciso o emprego da capacidade de retaliação, contraditoriamente, para o garantir é preciso manter a capacidade de retaliação constantemente a alto nível e disposta para ser empregue, mas sem a empregar.

Mas no ciberespaço, manter a capacidade de retaliação apresenta grandes dificuldades porque as armas cibernéticas perdem eficácia com o uso e com o tempo, pelo que uma retaliação no presente dificulta ou impossibilita a retaliação com a mesma ciberarma no futuro. As vulnerabilidades exploradas pelas ciberarmas podem ser detectadas ao emprega-las ou por outros mecanismos, anulando em ambos casos as capacidades das ciberarmas que as exploram. Adicionalmente o atacante nunca poderá ter a certeza dos efeitos reais que terá o emprego da ciberarma, e quem sofrer um ataque de retaliação pode crer que uma vez corrigida a vulnerabilidade explorada pelo retaliador já está protegido contra futuras retaliações, falindo assim a credibilidade e obrigando a sucessivas retaliações. O resultado de sucessivos ataques e retaliações erodirá a capacidade de retaliação, mas fortalecerá a defesa ao revelar novas vulnerabilidades, portanto a capacidade de ataque e retaliação diminuíram com a repetição do ciclo. Além disso o atacante ainda há de assumir o custo da sua atitude perante o público. (Libicki, 2009a, pp.56-59).

A capacidade das ciberarmas ainda apresenta mais uma limitação no que concerne às armas convencionais ou nucleares, porque a capacidade das ciberarmas para destruir as do adversário é irrelevante, portanto a retaliação não serve para complementar a dissuasão com a destruição de cibercapacidades ofensivas. Em linha com isto, a defesa ativa, na sua modalidade de contra ciberoperação automática sobre computadores atacantes também não é aconselhável, pelo risco de envolver terceiros ou de ser vítima dum engano para obter informação sobre as capacidades de retaliação. Sendo assim a retaliação deixa de ser urgente,

podendo adaptar-se os tempos em função das necessidades para convencer ao adversário (Libicki, 2009a, 59-62).

Sem abordar as considerações legais que serão objeto dos capítulos seguintes, avaliaremos aqui a factibilidade de empregar ciberarmas para atingir a dissuasão.

As especiais caraterísticas do ciberespaço tornam impossível para os potenciais atacantes e defensores conhecer com a certeza apropriada quais serão os efeitos dum ciberataque, seja este iniciador ou retaliatório. Depois do ataque o problema persiste, sendo também impossível para o atacante e o atacado avaliar os danos produzidos com a precisão e rapidez necessária. Portanto, se a retaliação for anunciada e os danos não correspondessem ao esperado faliria a credibilidade. Ao contrário, e se a retaliação for previa e o anuncio adiado até confirmar o êxito da mesma, podia passar por uma agressão ou pela intenção de apropriar-se do ataque de terceiro. Assim não serve empregar a ameaça cibernética pretendendo atingir alvos ou efeitos específicos. Adicionalmente, não é possível garantir a proporcionalidade da resposta, nem controlar os danos colaterais, nem garantir que a mensagem correta, implícita no ataque, chega aos decisores políticos apropriados com o conteúdo apropriado (Libicki, 2009a, pp.52-56).

Por fim, é muito difícil sustentar a dissuasão em acordos de controlo de armamentos, para reduzir as capacidades ofensivas ou manter o *status quo*, porque a verificação não é viável (Solomon, 2011, p.7). Permiti-la facilitaria ao adversário aceder à informação necessária para replicar as ciberarmas, para melhorar a sua defesa e para detectar vulnerabilidades exploráveis no sistema verificado (Libicki, 2009a, pp.199-201).

B.5. As dificuldades de comunicação e sinalização

Os problemas de atribuição e avaliação de danos, prévia e posterior ao ataque, afetam negativamente os elementos de comunicação e sinalização, também a dificuldade para determinar quando se está a sofrer um ataque. Quando o defensor não pode ter a certeza de que os ataques são percebidos como tais e de que os sinais que envia ao potencial atacante estão a ser interpretados corretamente, a capacidade de dissuasão diminui (Libicki, 2009a, p.62,115-116).

Importa considerar que a ciberguerra é de natureza limitada (Greathouse, 2014, p. 29). Sendo assim, há dois assuntos em negociação, o resultado da confrontação e a forma de se confrontar. Trata-se dum processo tácito de regateio pelo que é imprescindível que a velocidade dos acontecimentos permita o tempo necessário entre sinais para materializar o reajuste. Como a comunicação assenta mais nos atos que nas palavras há pouca possibilidade

de ajuste exato, devendo ser os limites qualitativos, distintos, finitos, discretos (descontínuos), simples, naturais e óbvios (Schelling, 1966, p.119-138).

B.6. O problema da credibilidade

O estabelecimento adequado do liminar da represália, e a natureza anunciada para a resposta em relação ao tipo de ofensa que dissuadem, são determinantes para o êxito da estratégia dissuasória. Se o defensor considerasse anunciar uma resposta potente como única forma de dissuadir ofensas irritantes, mas de pouca gravidade, e no caso de se materializar a ofensa não executasse a represália, pelos custos ou acusações que lhe pudesse supor, perderia credibilidade em relação a todas as ameaças. Neste caso, o atacante poderia sentir-se convidado a continuar provando a determinação do defensor noutras áreas. (Solomon, 2011, p.11)

Portanto, a credibilidade está condicionada pela racionalidade das respostas disponíveis. Mas tal racionalidade pode falir em casos onde a possibilidade dum ataque se avalia iminente, e a tensão pode levar a descartar as estimativas de ganhos e perdas colapsando a dissuasão (Brodie, 1958, p.12).

B.7. O problema da soberania

Em direta relação com os problemas de atribuição, o problema da soberania é consequência do alto grau de interconectividade do ciberespaço, independentemente do território sobre o que se localizem os usuários e o nível físico. Adicionalmente, os domínios administrativos, delimitados pelos servidores que conectam a infraestrutura de rede dum administrador com o exterior, estão frequentemente distribuídos por vários Estados, o que acrescenta a dificuldade de adaptar o conceito tradicional de fronteira ao ciberespaço. (Hare, 2009, p.1 e Larsen, 2003, p.44,49)

Em consequência, avançar na atribuição faz necessária a cooperação entre Estados, mas há inconvenientes para cooperar. Porque é difícil assegurar que a cooperação para a atribuição não vai ser empregue para violar a privacidade ou para a recolha de informações sobre setores críticos, incluso entre aliados, quanto mais entre competidores. (Solomon, 2011, p.7)

Apêndice A — Afinamento indutivo do modelo conceitual mediante análise relacional

O ponto de partida para o estabelecimento da base conceitual da investigação foi o esquema conceitual estabelecido pelo mesmo autor (Bustelo, 2017), sobre a base de uma profunda revisão da literatura, naquele momento, para uma análise no plano puramente teórico.

Aquele quadro conceitual estabelecia nove variáveis independentes e 52 indicadores para avaliar a primeira hipótese. Ao aplicá-lo à análise teórica, era facilmente observável um elevado número de duplicidades, segundo a perspetiva adotada, e um elevado número de laços de realimentação entre conceitos, o que não levantava obstáculos de relevo para aquela tipologia de análise, mas podia tornar complexa demais a análise no plano de praxe das relações internacionais que se aborda neste trabalho. Portanto, para abordar o trabalho atual era imprescindível simplificar o modelo conceitual. É importante salientar que o processo de simplificação se focou na primeira hipótese, enquanto que as hipóteses são analisadas em cascata e a complexidade conceitual se apresenta para a avaliação da primeira.

Tabela 2 - Número de códigos disponíveis e assignados ao *corpus* de fontes primárias nos processos de codificação

		Codificação Inicial			Codificação Final		
		Teóricos Disponíveis	Efetivos	Sem ocorrências	Teóricos Disponíveis	Efetivos	Sem ocorrências
Códigos	Variáveis HIP 1	9	9	0	7	7	0
	Indicadores	52	25	27	36	31	5
	Códigos adicionais	Os necessários	7	0	Os necessários	6	0
Total		68	41	27	43	44	5

Fonte: (Autor, 2019)

O processo indutivo de afinamento do modelo começou com a codificação aberta do *corpus* conceitual. Partiu-se de 61 códigos iniciais (Tabela 2) com a possibilidade de acrescentar os códigos que se julgassem necessários, por se tratar de codificação aberta. Assim, foram acrescentados sete códigos contextuais. A primeira codificação revelou a existência de códigos que etiquetavam os mesmos conceitos, embora vistos na perspetiva de variáveis diferentes. Além disso, a codificação tendia a saturar o texto, motivo pelo que se aplicou uma codificação pouco exaustiva, codificando apenas os casos evidentes. Além disso, a codificação foi restritiva, codificando apenas os fragmentos diretamente referidos

ao conceito em questão e não ao parágrafo completo, pelo que a codificação apresentava uma baixa contextualização. Finalmente foram atribuídas 1214 codificações a fragmentos de texto segundo o quadro de frequências da Figura 35.

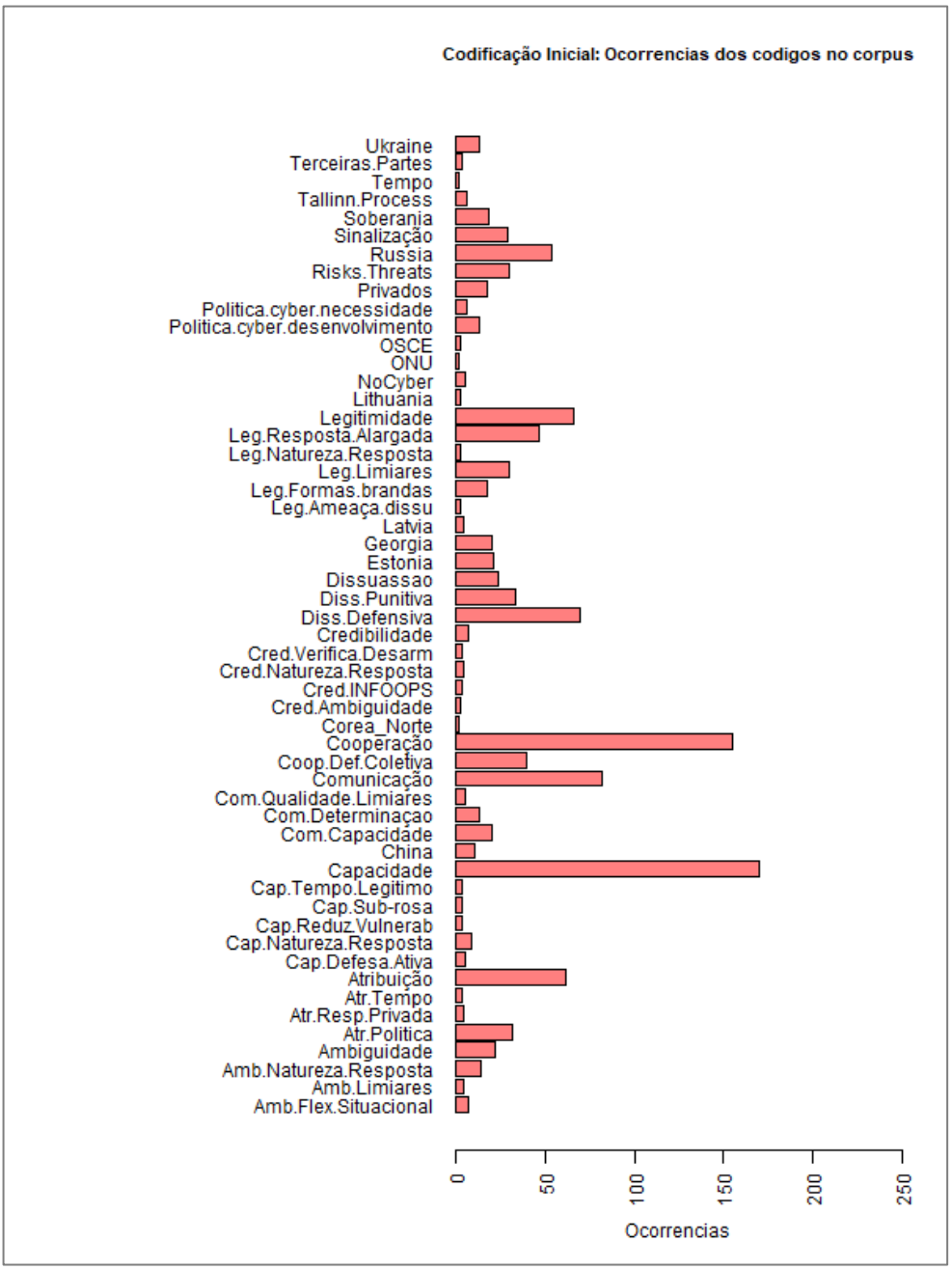


Figura 35 – Frequência dos códigos atribuídos na codificação inicial.

Fonte: (Autor, 2019)

Como era de esperar, os fragmentos de texto codificados não são desconexos, porque qualquer mensagem de relevância para a dissuasão tende a combinar vários elementos. Assim, a frequência com que dois códigos são atribuídos a um fragmento comum de texto

do *corpus* será um indicador da maior ou menor relação entre ambos conceitos na dimensão da praxe internacional. Adotando este critério de relação, procedeu-se à análise relacional dos conceitos codificados. A análise foi desenvolvida segundo vários algoritmos, cujo detalhe de implementação está disponível no *scrip* do Apêndice D, embora aqui apenas se apresentem os produtos que ofereceram resultados mais evidentes.

Como consequência do critério relacional adotado, códigos mais próximos indicam conceitos mais frequentemente apresentados juntos. Em consequência, o modelo de representação gráfica de Fruchterman-Reingold[14] parece o mais apropriado para a visualização do grafo de relações. Na Figura 36 observa-se que, em termos gerais, as variáveis ocupam a posição central e têm um maior volume que os indicadores, consequência do maior número de relações. Este resultado era previsível desde que, por norma, um fragmento de texto codificado com um indicador também é codificado com a variável correspondente. O grossor das linhas é proporcional ao número de vezes que os códigos enlaçados coincidem no *corpus*.

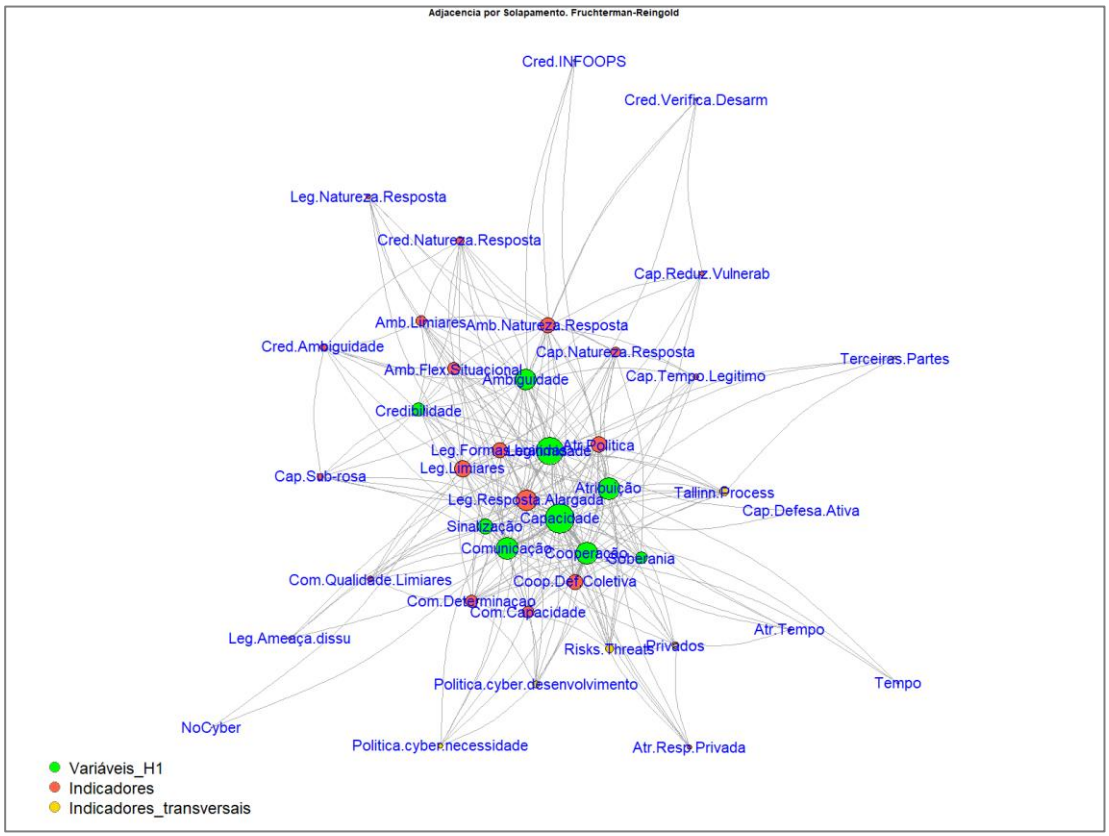


Figura 36 – Codificação inicial. Grafo de adjacência por solapamento (Fruchterman-Reingold)

Fonte: (Autor, 2019)

[14] O algoritmo de Fruchterman-Reingold (Fruchterman e Reingold, 1991) posiciona os vértices para atingir o equilíbrio de dois critérios: 1- Os vértices mais relacionados estão mais próximos, 2- A proximidade entre vértices acrescenta a repulsão entre eles segundo o modelo de repulsão elétrica.

Embora o sistema de representação de Fruchterman-Reingold seja o que melhor ajusta o modelo à realidade, a concentração dos vértices no centro da figura, maior quanto maior seja o grau de relações, dificulta a leitura. Para facilitar a visualização, apresenta-se o grafo segundo o modelo de Kamada e Kawai (1989), embora o fundamento da representação gráfica não se ajusta completamente à realidade representada[15].

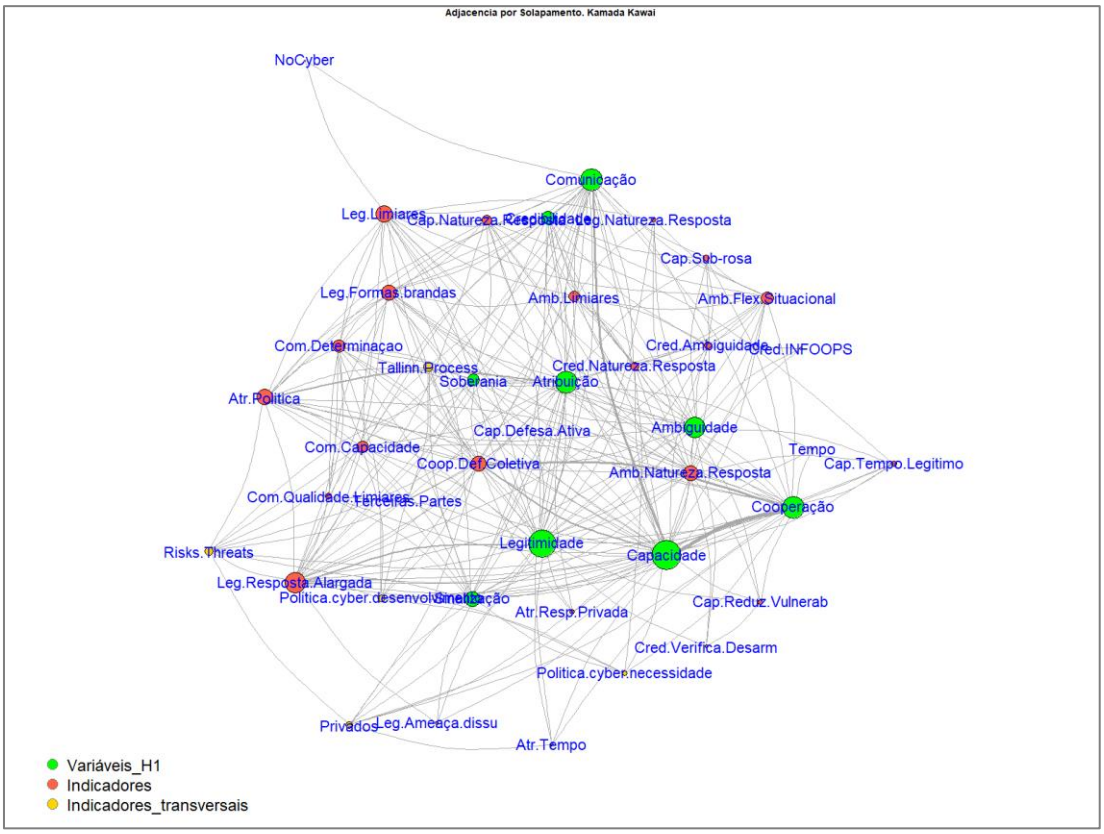


Figura 37 – Codificação inicial. Grafo de solapamentos (Kamada-Kawai)

Fonte: (Autor, 2019)

Como se pode observar na Figura 37, há uma estreita relação entre *capacidade* e *cooperação* assim como entre *capacidade* e *comunicação.* Contudo, o facto mais significativo é que apesar do elevado número de relações que estabelece o código *legitimidade*, observável pelo elevado volume do vértice, estas conexões são dispersas. Esta dispersão das relações e a ausência de arestas de elevado grossor com origem em

[15] Porque a distância entre vértices aumenta com o peso da aresta (Kamada e Kawai, 1989), quando na realidade que tratamos de apresentar acontece o contrário, quanto mais se solapam os códigos maior é o peso.

legitimidade apontam para a transversalidade deste conceito e indicam a necessidade de reconsiderar o seu encaixe no modelo teórico.

Para facilitar a interpretação dos grafos, de difícil leitura pela sua densidade, na Figura 38 apresenta-se o mapa de calor da matriz de adjacência. A maior intensidade da coloração vermelha apresenta um maior solapamento dos conceitos relacionados nos textos do *corpus*.

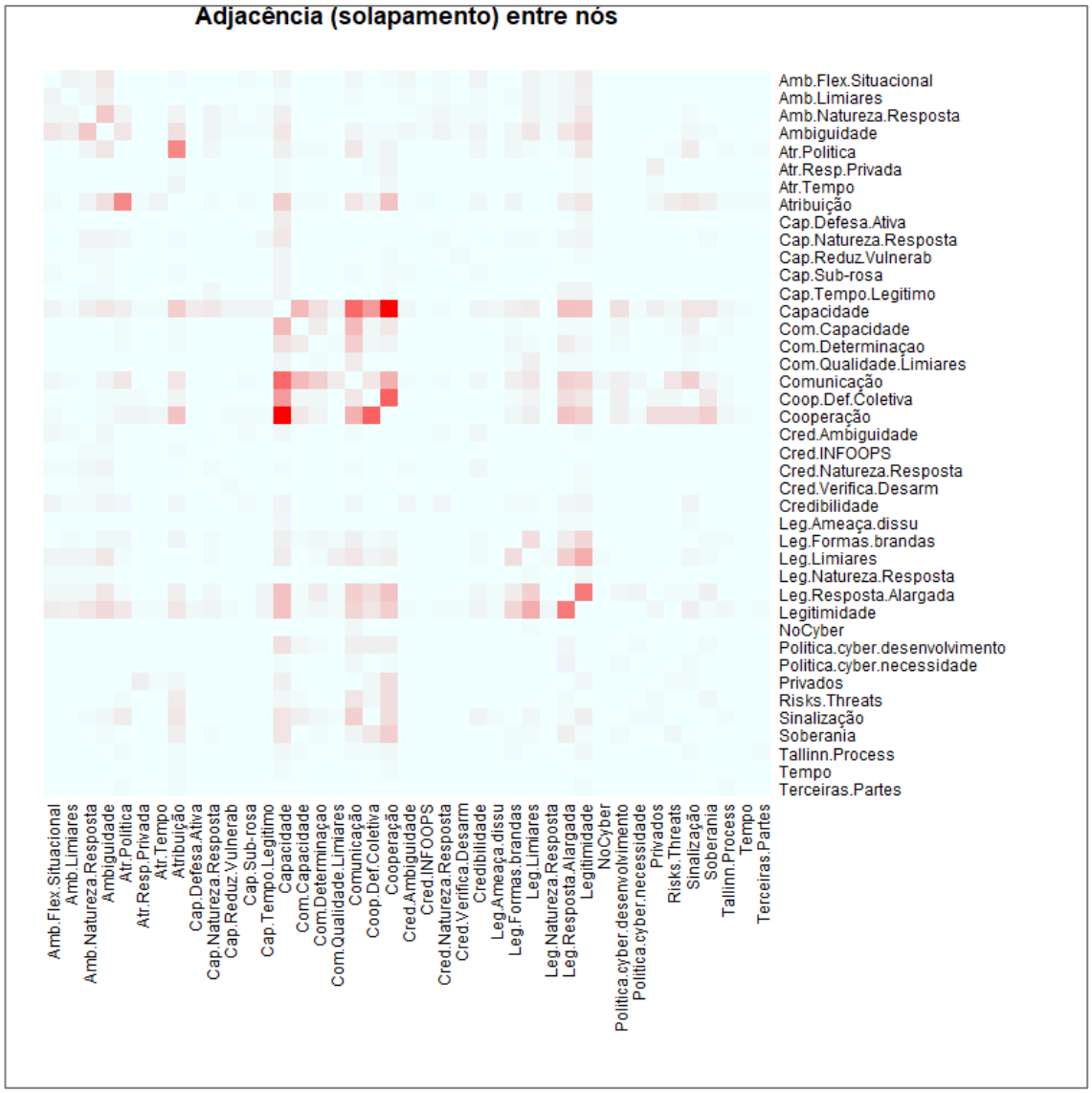


Figura 38 – Codificação inicial. Matriz de adjacência por solapamento (Mapa de calor)

Fonte: (Autor, 2019)

Contudo, a maior debilidade deste modelo de codificação inicial, é a baixa congruência das comunidades de códigos com o modelo teórico que se apresentou no Capítulo 1 (Figura 2).

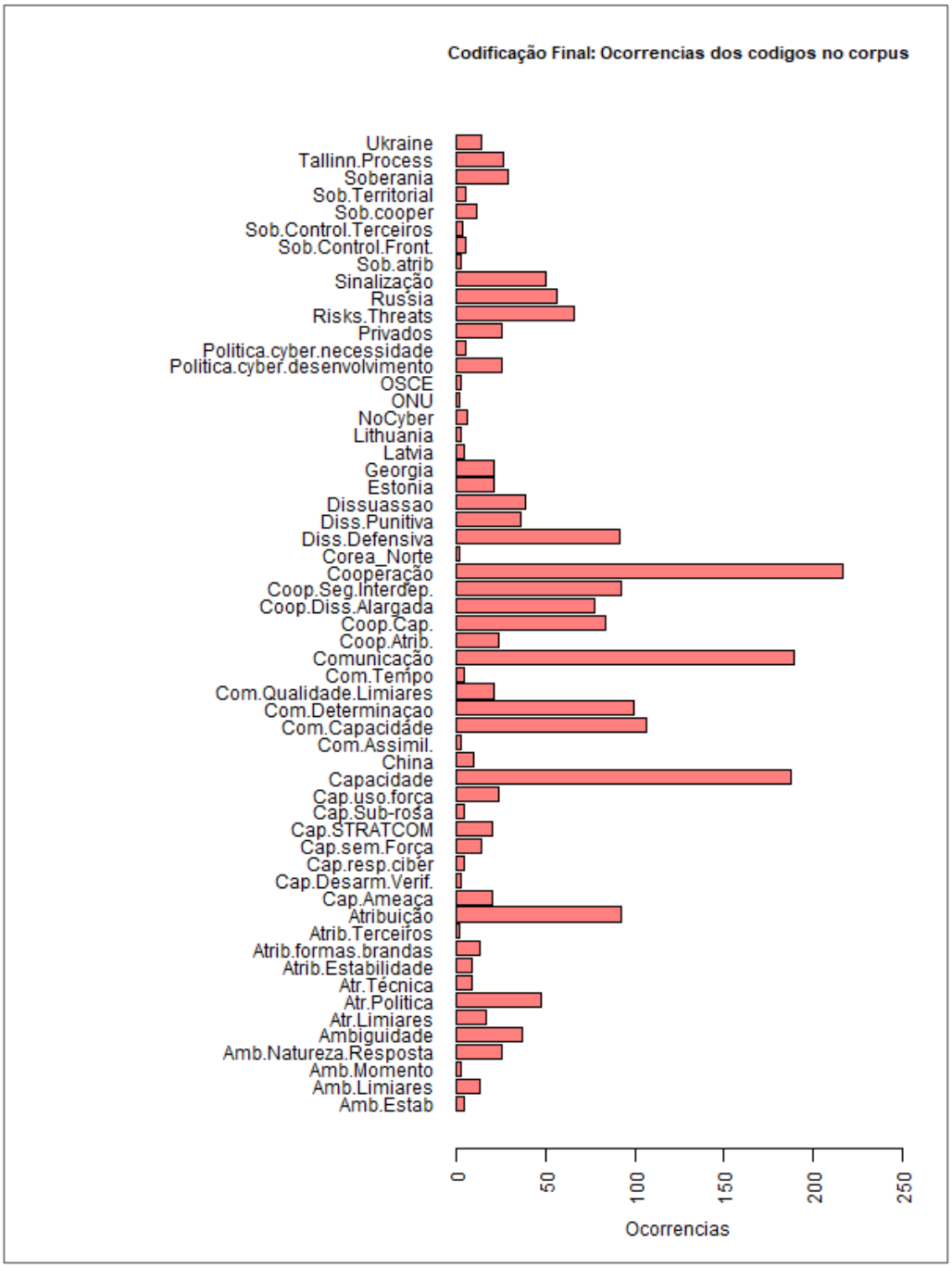


Figura 39 – Frequência dos códigos atribuídos na codificação final.

Fonte: (Autor, 2019)

Depois de vários ciclos, concluiu-se o processo de afinamento da codificação com 2008 etiquetas atribuídas a fragmentos de texto. Assim, a fase dedutiva abordou-se com estas 2008 codificações distribuídas segundo o quadro de frequências da Figura 39.

Este novo esquema de codificação, permitiu atingir duas vantagens sem sofrer em consequência um incremento explosivo do número de codificações. A primeira vantagem é que permitiu codificar também os casos menos evidentes, atingindo assim uma massa

crítica mínima para tirar conclusões úteis em relação à grande maioria de indicadores. A segunda vantagem é que permitiu codificar, como regra general, por parágrafos, garantindo uma contextualização adequada.

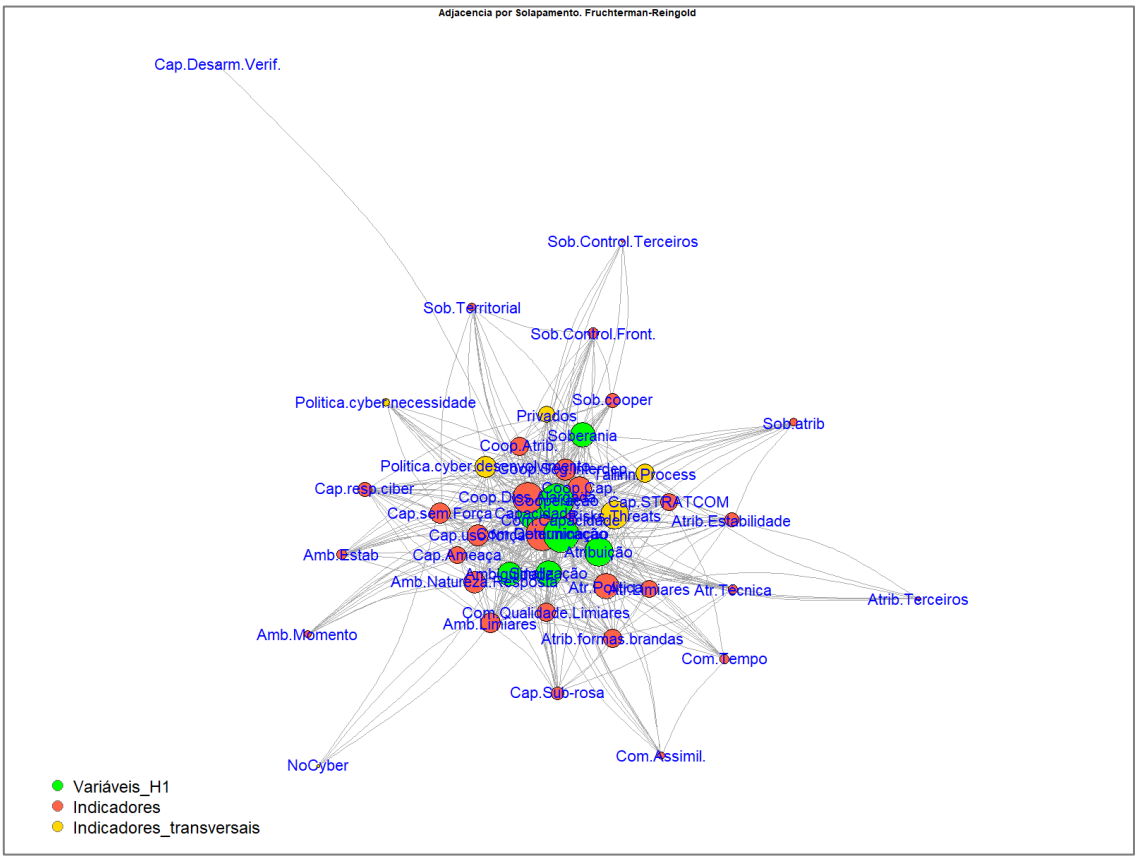


Figura 40 – Codificação Final. Grafo de solapamentos (Fruchterman-Reingold)

Fonte: (Autor, 2019)

Da observação dos grafos das Figuras 38 e 40 salta à vista a maior densidade do grafo correspondente à codificação final. Isto era previsível, porque o maior número de relações de solapamento é a consequência imediata do maior número de codificações e da maior extensão dos fragmentos codificados. Contudo, a congruência entre as duas codificações é elevada. Assim *comunicação*, *cooperação* e c*apacidade* continuam a ocupar posições fulcrais, e outras variáveis como *soberania* continuam a ocupar posições periféricas. Destaca entre as diferenças a maior relevância dos códigos adicionais, transversais ou contextuais, consequência da codificação mais exaustiva e extensa. Vemos assim que, os *riscos e ameaças* participam de elevado número de relações e estão muito próximas do núcleo da dissuasão, o que é lógico, desde que constituem parte essencial do contexto que justifica o desenvolvimento da estratégia dissuasória. Também podemos

observar que embora na codificação final o TMP está sensivelmente mais próximo do centro continua a ser periférico, o que é coerente com o carater não oficial dos Manuais.

A representação gráfica segundo o modelo de Kamada e Kawai, embora distâncias e posições não sejam representativas da realidade, facilita a visibilidade e permite tirar conclusões adicionais. Assim, o grossor das arestas e o diâmetro dos vértices permite verificar que há indicadores mais relevantes do que algumas variáveis. Destacam a *comunicação da determinação* e a *comunicação da capacidade*, a *cooperação para a dissuasão alargada* e a *imputação política*. Isto vem a confirmar a importância de determinar as proporções em que se hão de adicionar os ingredientes na receita da dissuasão, questão para a que já apontava Bustelo (2017, p.47).

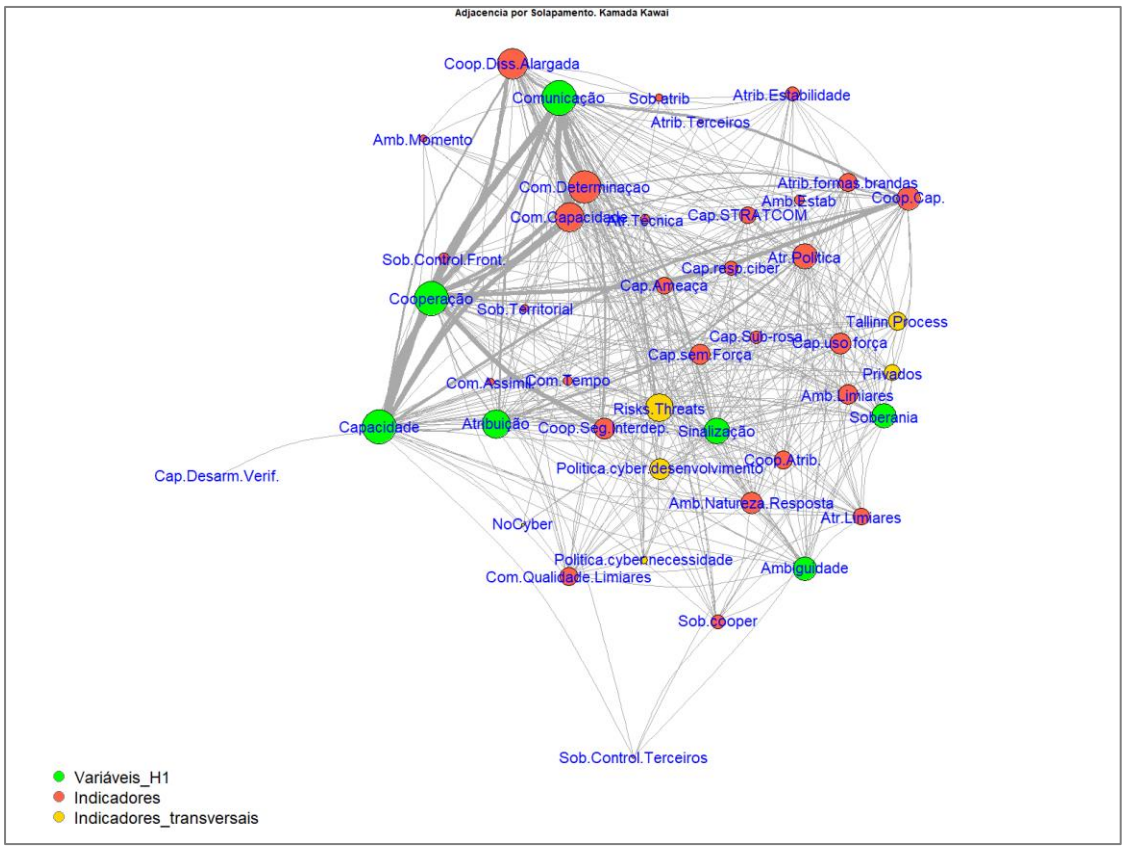


Figura 41 – Codificação Final. Grafo de solapamentos (Kamada- Kawai)

Fonte: (Autor, 2019)

A comparação das Figuras 37 e 41 confirma outra das vantagens da codificação final. Na primeira codificação o não havia grandes diferenças de peso entre arestas, mas a codificação intensiva e extensiva à que responde a segunda figura revela com muito maior contraste a relevância de umas relações frente a outras. Este maior contraste também é apreciável na comparação dos mapas de calor respetivos (Figuras 38 e 42).

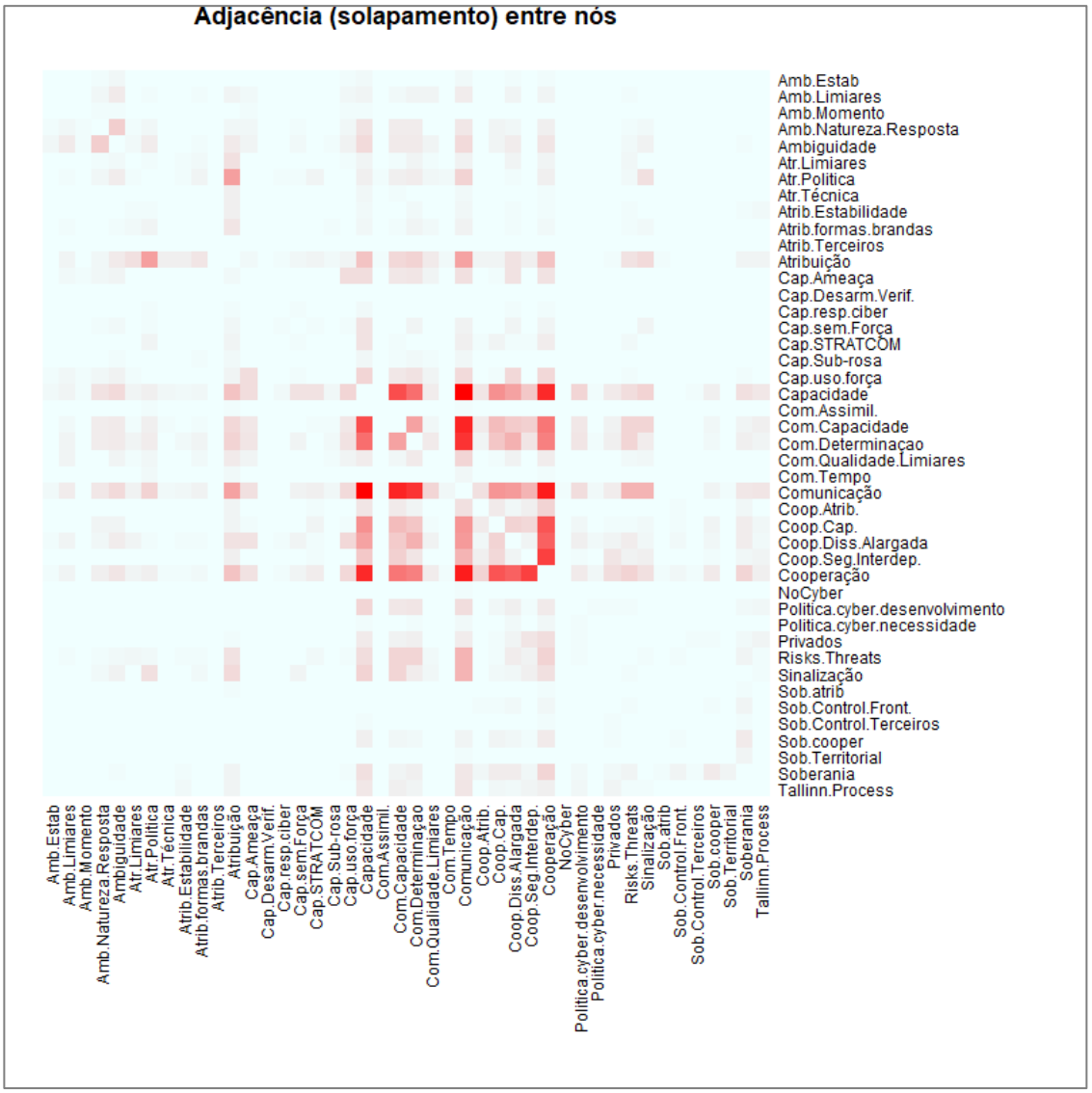


Figura 42 – Codificação Final. Matriz de adjacência por solapamento (Mapa de calor)

Fonte: (Autor, 2019)

Contudo, possivelmente a maior vantagem da codificação final frente à inicial seja o melhor ajuste ao modelo teórico da estrutura de comunidades do segundo esquema de codificação. Nas Figuras 2 e 3 do primeiro capítulo apresentavam-se os dendrogramas representativos destes esquemas de modularidade, nas Figura 43 e 44, apresentam-se ambos grafos e o primeiro nível da estrutura modular[16].

[16] A vermelho as relações intracomunitárias, em preto as relações intercomunitárias. As cores dos vértices correspondem-se com as das famílias representadas nos dendrogramas das Figuras 2 e 3.

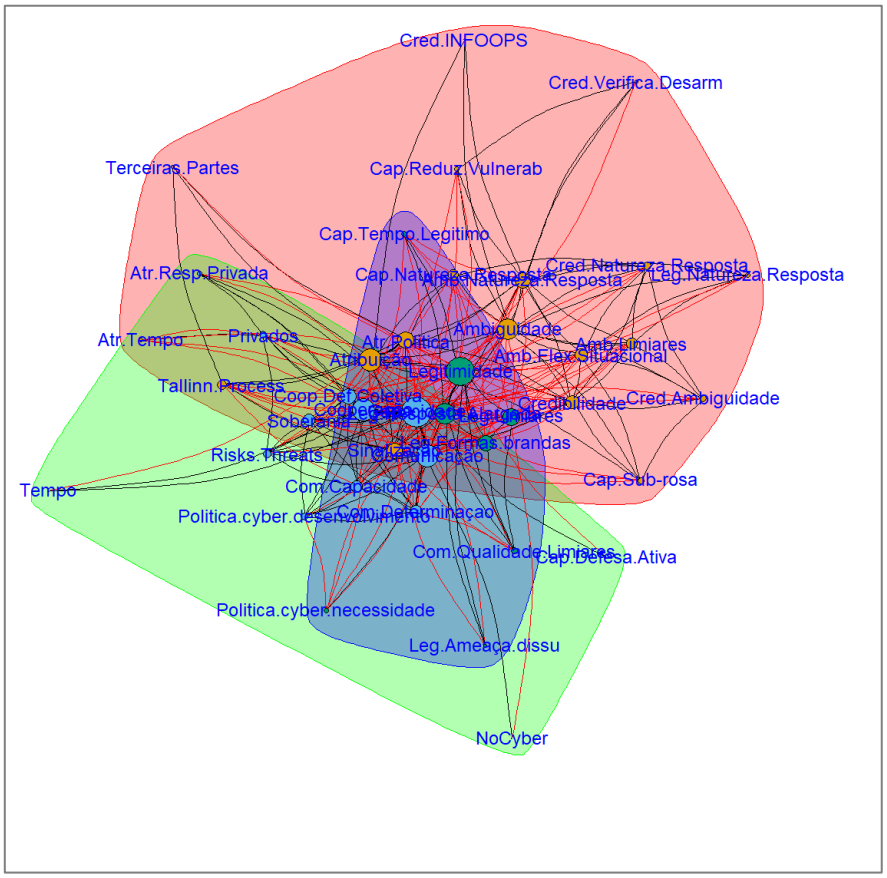


Figura 43 – Codificação Inicial. Comunidades de relação por solapamento (Algoritmo Greedy)

Fonte: (Autor, 2019)

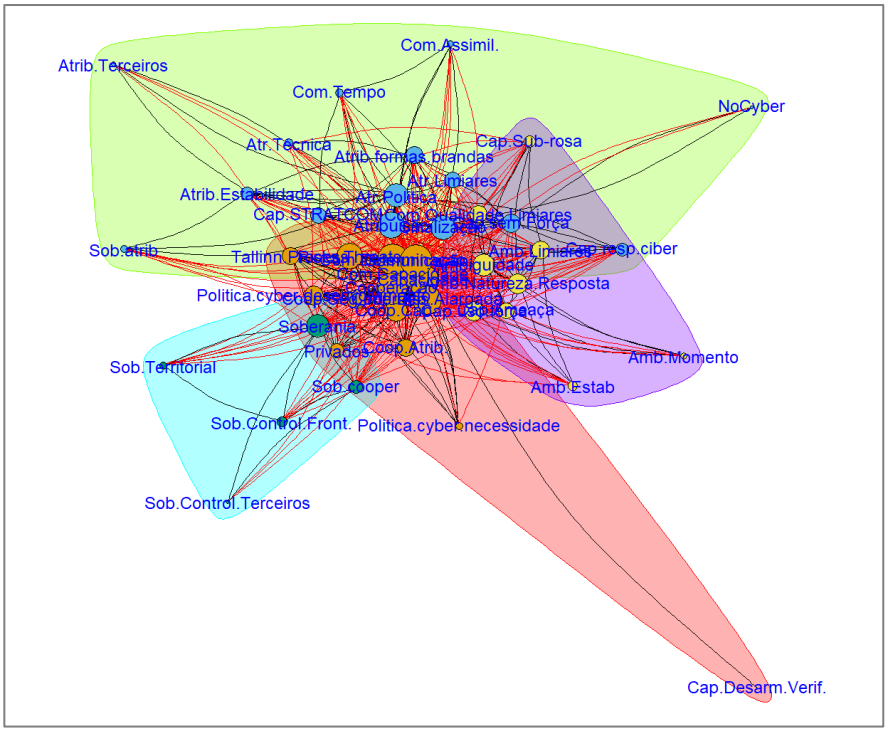


Figura 44 – Codificação Final. Comunidades de relação por solapamento (Algoritmo Greedy)

Fonte: (Autor, 2019)

Apêndice B — Dimensão teórica. Os Manuais e as dificuldades de dissuasão no ciberespaço

Ao longo deste apêndice apresenta-se o resultado do processo dedutivo e preparatório do trabalho de investigação exposto no corpo do relatório. Assim, aqui estuda-se como o TMP altera o filtro de legitimidade, na dimensão teórica, avaliando que elementos dissuasórios podem ser incluídos numa estratégia dissuasória de legitimidade credível. Em resumo, estabelecem-se os contributos teóricos dos manuais de Tallinn para a dissuasão no ciberespaço. Sobre estos contributos teóricos é que se cimentará a investigação na dimensão da praxe internacional.

A filtragem de credibilidade desde a perspetiva teórico-estratégica foi prévia, não se considerando neste trabalho opções estrategicamente não credíveis.

Embora na referenciação bibliográfica deste trabalho empregou-se o estilo *Harvard-Anglia*, tal como preconizado na NEP/ACA-018 do IUM, neste apêndice é feita uma exceção para facilitar a sua leitura e compreensão. Assim, as referências às regras e comentários do *Tallinn Manual* (Schmitt et al., 2013), e do *Tallinn Manual 2.0* (Schmitt et al., 2017), são indicadas respetivamente por TM ou TM2 seguido do número da regra, ou pelo número da regra seguida pelo número do comentário. Caso a referência seja a um parágrafo não incluído numa regra empregar-se-á o número de página[17].

B.1. Soberania

Os dois TM concluem que um Estado não pode exercer a sua soberania sobre o ciberespaço *per se* (TM 1.1 e TM2 1.7). Porém, a soberania existe no ciberespaço e, como tal, ambos os TM reconhecem aos Estados as prerrogativas da soberania sobre as infraestruturas cibernéticas localizadas no seu território soberano e sobre as atividades cibernéticas a elas associadas (TM 1.1 e TM2 1.1), ao mesmo tempo que reconhecem limitações no desenvolvimento de ciberoperações sobre ciberinfraestruturas colocadas em território de outros Estados.

O TM2 ainda aprofunda mais este assunto. O comentário constante da regra 1.4 do TM2 esclarece a aplicabilidade do princípio de soberania nas camadas física, lógica e social do ciberespaço. Para além disso, a regra 1.5 do TM2 reforça o exercício da soberania declarando que a consideração do ciberespaço como *global common* não é a mais correta,

[17] Por exemplo (TM 18), (TM 18.1), (TM2, p.45)

uma vez que assenta em infraestruturas e é utilizada por sujeitos que estão abrangidos por jurisdições e, como tal, pela soberania de um ou vários Estados. A regra 2 versa sobre a autoridade dos Estados sobre as infraestruturas, pessoas e ciberatividades, fazendo um pormenorizado estudo das questões de soberania interna nas camadas física, lógica e social, onde devemos salientar o direito estatal de proteção da infraestrutura e de salvaguarda das atividades exercidas no território (TM2 2.2),

A abordagem da questão jurisdicional na regra 2 do TM traz avanços relevantes para os problemas de dissuasão, que ainda se esclarecem mais no TM2. Assim a regra 8 do TM2 analisa os princípios gerais da jurisdição territorial e extraterritorial, sendo destacável o comentário TM2 8.2 que relembra que as operações desenvolvidas no ciberespaço estão sujeitas aos mesmos princípios gerais que qualquer outra forma de atividade. Com as Regras 2 e 9 do TM2 fica aclarado o direito exclusivo dos Estados para exercer a jurisdição e a autoridade dentro do seu território sobre as três camadas do ciberespaço. Destaca-se, contudo, a falta de acordo por parte dos autores do TM2 quanto à jurisdição sobre os dados armazenados ou transmitidos fora do território soberano (TM2 2.11).

O TM previa na regra 2 uma solução para a problemática decorrente da não coincidência das fronteiras territoriais com as fronteiras de domínio, estabelecendo a presença física ou legal de pessoas ou objetos como base principal para o exercício da jurisdição do Estado. Assim, o comentário 2.2 do TM possibilitava a jurisdição quer por nacionalidade, quer por territorialidade do espaço de operações. O comentário 2.3 do TM esclarecia a jurisdição sobre os sistemas distribuídos transfronteiriços, não sendo a multiplicidade jurisdicional impedimento para um Estado exercer a soberania no seu território. Com similar critério, a TM 2.4 resolvia a questão dos ciberataques a partir dos dispositivos móveis e ainda encontrávamos na TM 2.8 outras bases reconhecidas de jurisdição extraterritorial. A questão jurisdicional ainda se esclarecia mais abordando os Estados de Bandeira e Estados de Registo (TM 3), e a imunidade e inviolabilidade (TM 4).

O grau de detalhe do TM2 quanto à soberania (TM2 3) e jurisdição (TM2 10 e 11) extraterritorial é elevado e em geral plenamente compatível com as necessidades da dissuasão, embora estabeleça limites relevantes para o exercício desta jurisdição, muitos deles ultrapassáveis mediante a cooperação interestatal (TM2 11.b). Outras limitações, como a aplicabilidade do princípio de proteção apenas na defesa de interesses vitais do Estado (TM2 10.10 e 10.11), devem ser avaliadas positivamente porquanto contribuem para a estabilidade.

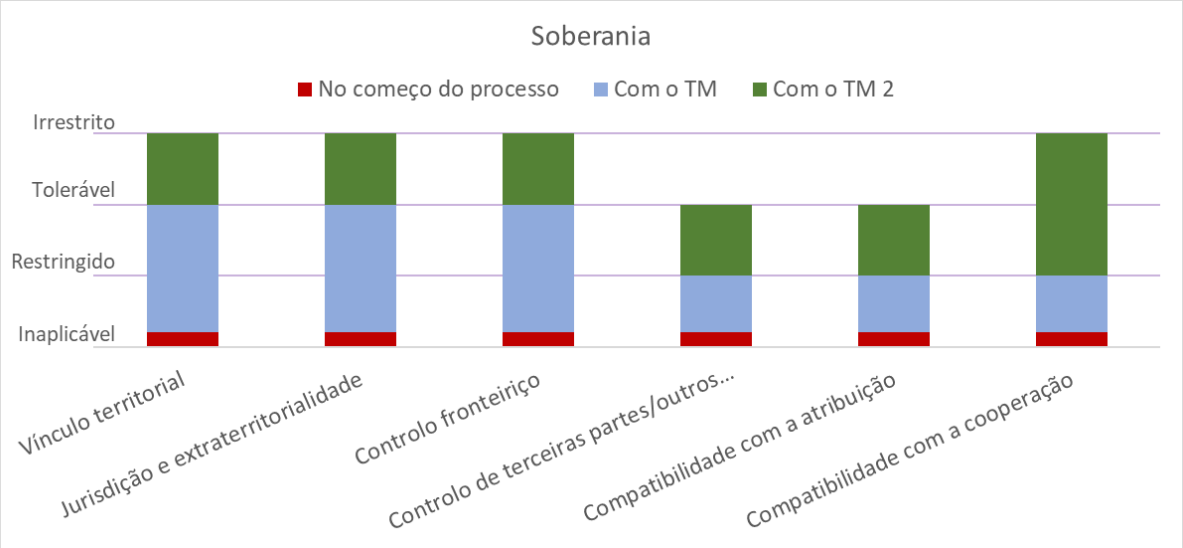


Figura 45 – Avaliação de indicadores de Soberania.

Fonte: (Autor, 2019)

Em relação às fronteiras, sendo estas os limites determinantes para o exercício da soberania territorial, adotar medidas para assegurá-las demostra a determinação nacional para exercê-la, independentemente da viabilidade técnica de o fazer. Constituem, portanto, um elemento de segurança no ciberespaço e um instrumento de comunicação (Hare, 2009) e sinalização da posição política nacional.

A autoridade dos Estados para controlar e para restringir ou proteger total ou parcialmente o acesso à Internet (TM 1.4 e 1.10, TM2 1.6, 2, 4.6 e 63.11) facilita o controlo fronteiriço efetivo, simbólico e percetual (Andreas, 2001, pp.3,4).

Deve destacar-se a irrelevância, para o exercício da soberania interna, da natureza pública ou privada de infraestruturas, atores ou atividades (TM2 2.3), sobretudo em relação à mitigação das interferências de terceiras partes nas estratégias de dissuasão.

Os contributos desta interpretação para a imputação e a mitigação dos efeitos de terceiros são positivos, mas insuficientes para ultrapassar problema. Também devemos salientar que as prerrogativas da soberania não são reconhecidas às organizações internacionais (TM2 1.10).

B.2. Imputação

Abordamos nesta secção a problemática da imputação no ciberespaço, que soma às dificuldades da imputação técnica a problemática decorrente de os artigos sobre a Responsabilidade dos Estados por Atos Internacionalmente Ilícitos (UN, 2001) não ser um

tratado, o que limita o seu caráter vinculativo ao coincidente com o Direito Internacional Consuetudinário (TM2, p. 79), embora esse instrumento vise cristalizar em texto escrito esse tal Direito Consuetudinário.

Para a dissuasão importa a possibilidade de imputar os atos ilícitos a um Estado. O TM abordou o assunto nas regras 6 a 8, e o TM2 aprofundou o tema nas regras 14 a 19. Importa destacar, a propósito da figura das cibermilícias (Ottis, 2009), a interpretação extensiva de órgãos de Estado e a equiparação a estes de pessoas ou grupos sob completa dependência de um Estado (TM 6.9; TM2 15.2-15.4). É importante também destacar a possibilidade de imputação a um Estado de ciberoperações executadas por atores não-estatais, nas condições da regra 17 do TM2: controlo efetivo ou reconhecimento da operação como própria. É de salientar que a insuficiência de provas para imputar a um Estado a responsabilidade pela ciberoperação de um ator não-estatal não impossibilita a imputação de outras responsabilidades ao Estado decorrentes dos vínculos com esse ator (TM2 17.19). Ainda podem ser atribuídos a um Estado os atos ilícitos executados por órgãos de outro Estado, desde que este esteja sob a autoridade do primeiro (TM2, 16) ou ambos atuem em conjunto em ciberoperações com impacto noutros Estados (TM2, 18).

Os TM não abordam intencionalmente a questão dos métodos de prova e de imputação técnica (TM2, p.81). Antes oferecem soluções alternativas para ultrapassar alguns dos problemas que a imputação técnica no ciberespaço apresenta para uma dissuasão eficaz.

Os TM fornecem alguns fundamentos para estabelecer a imputação política. Assim o TM2 (p.81-82) abre a porta para que um Estado possa superar a incerteza da imputação *ex ante*, permitindo-lhe atuar como um Estado razoável atuaria num caso similar, também para completar a falta de inteligência técnica com outras fontes. Quanto mais grave for o ato ilícito atribuído, mais sólidas devem ser as provas. O TM2 refere ainda (TM2, p.83) que, embora seja recomendável, não é obrigatório revelar as técnicas forenses utilizadas para chegar à imputação. Porém, isto não deve ser percebido como lassitude nos requisitos da imputação, sob pena de colocar em risco a estabilidade. Assim, a adoção de contramedidas em caso de imputação errada comporta responsabilidade para o Estado que as adote (TM2, 20.16). O incumprimento das obrigações de "diligência devida" (TM 5; TM2 6-7), como, por exemplo, no caso dos ciberataques à Estónia em 2007 (Artiles, 2010, pp.179-180), pode ser utilizado também como peça de prova política a considerar.

Os Manuais sabem compensar a margem dada para a imputação política com a exigência de verificações adicionais, para evitar que a interferência de terceiros e o alto risco de imputação errada no ciberespaço afetem a estabilidade. Assim, consideram insuficiente a apresentação de provas isoladas para a imputação de atos a um Estado. Por exemplo, o facto de os ciberataques originarem de uma determinada infraestrutura governamental (TM 7; TM2 15.12), ou o facto de a localização geográfica de atos, atores ou instrumentos do ato ilícito (TM 6.12; TM2 15.14) ou roteamento de operações se verificarem dentro de um determinado território (TM 8) devem ser avaliadas em contexto (TM2, 15.16).

Para efeitos da dissuasão, devemos pressupor a possibilidade de imputar qualquer violação de uma obrigação internacional aos Estados. A imputação de responsabilidade aos Estados pela sua atuação no ciberespaço (TM 6; TM2 14) é um passo relevante nesta direção. O facto de a imputação de um ato ilícito, a nível internacional, poder verificar-se mesmo sem dano físico ou sem que haja intenção de dano (TM2 14.8-14.9) facilita as técnicas de dissuasão. Porém, a possibilidade de estabelecer uma escala de limites consoante a gravidade do ato ilícito imputado e a contundência da resposta legitimada revela-se fulcral para articular qualquer estratégia de dissuasão.

No patamar mais alto da escala de atos ilícitos imputáveis encontramos o "ataque armado", que se apresenta como um caso agravado do "uso da força". A avaliação em termos de escala e efeitos permite determinar quando um "uso da força" se qualifica como um "ataque armado" e, portanto, legitima uma resposta que empregue a força (TM, 13 e p.55; TM2, 68,69). Importa destacar que o "uso da força" e o "ataque armado" servem fins normativos distintos: o primeiro para determinar se foi violado o Artigo 2(4) da carta das Nações Unidas; o segundo para, ainda que haja também uma violação deste Artigo, determinar a legitimidade de responder empregando a força (TM, 11; TM2, 69.11). Importa destacar a unanimidade dos autores dos TM no sentido de entenderem que todo o "ataque armado" constitui um "uso da força", mas não ao contrário (TM 13.5, TM2 71.2,71.6), embora haja Estados a considerar irrelevante a diferença entre ambos termos (TM 11.7; TM2 69.7).

Apesar da falta de jurisprudência, e da impossibilidade de fixar um limite nítido, é consensual entre os autores dos TM que quaisquer usos da força, incluindo os desenvolvidos unicamente mediante ciberoperações (TM2, 71.4), que provoquem mortos, feridos, danos graves ou destruição grave de bens, se qualificariam como "ataque armado"

(TM 11.8,13.7; TM2 69.8). A exigência de um elemento transfronteiriço seria sempre necessária num conflito entre Estados (TM 13.2; TM2 71.3).

Para dissuadir contra a possibilidade de implantar ciber-armas latentes ocultas tem especial interesse a imputação do "ataque armado" qualificado "iminente". No quadro do *jus ad bellum*, os Manuais qualificam a inserção de bombas lógicas como "ataque armado iminente", sob condição de as condições de ativação serem suscetíveis de ocorrer. Porém, se forem ciber-armas de ativação remota, apenas qualificariam o ataque "iminente" depois de o adversário ter decidido o seu emprego efetivo (TM 15.6; TM2 73.7-73.8).

Para esclarecer que ações constituem um "uso da força" abaixo do limiar de "ataque armado", é necessário avaliá-las qualitativa e quantitativamente pela semelhança em escala e efeitos com as operações nos domínios clássicos (TM 11, TM2 69,71). As regras dos TM não concretizam a definição, mas excluem dela a espionagem *per se*, outras formas de coação (económica, política, psicológica não destrutiva…), ou o apoio a ativistas (financiamento, santuário). Porém, essas regras permitem qualificar algumas combinações destas atividades como um "uso da força".

O caráter indeterminado do limiar do "uso da força" recomenda muita sensibilidade para a avaliação do que pode ser imputado à luz da comunidade internacional. Neste contexto, os Manuais têm tido um importante papel no processo de impulsão normativa. É especialmente importante a abordagem interpretativa proposta, assente na severidade do dano e numa lista, não fechada, de fatores qualitativos a avaliar: severidade, imediatismo, retidão da cadeia causal, invasão, mensurabilidade dos efeitos, caráter militar, envolvimento estatal e presunção de legalidade (TM 11.9; TM2 69.9).

Abaixo do limiar do "uso da força" ainda é atribuível responsabilidade legal internacional por "atuação ilegal" (TM 6-8, TM2 14-19). Embora o assunto seja abordado nos dois manuais, o contributo para a dissuasão do TM2 é muito mais relevante. Tal acontece porque este Manual analisa com maior profundidade a violação de preceitos gerais, como a soberania (TM 1, TM2 1-4), mas sobretudo porque a abordagem que faz na Parte II sobre a aplicabilidade dos regimes especiais do Direito Internacional no ciberespaço traz luz para considerar como ilegais ações e omissões que outras interpretações podiam considerar num limbo jurídico.

A possibilidade de imputar uma "atuação ilegal" por incumprimento do princípio geral de "diligência devida" é um importante contributo dos Manuais para a estabilidade, no domínio do ciberespaço (TM 5, TM2 6-7). Contudo, o limiar do incumprimento é um

conceito jurídico indeterminado (TM2 6.25), para cuja avaliação o TM2 oferece um leque de referências significativamente mais abrangente do que o TM. Nos dois Manuais, os autores concordam que não há obrigatoriedade estatal de regulamentar as condições de cibersegurança nos setores público e privado, mas a sua interpretação de "diligência devida" coloca sobre os Estados despreocupados o risco de responderem pelas atividades ilícitas de terceiros.

Abaixo do limiar da atuação ilegal ainda se pode imputar uma ação não amistosa, que embora isenta de relevância na perspetiva do Direito Internacional tenha relevância no domínio político e das relações internacionais.

Ainda há outras opções de imputação nos domínios do Direito Internacional Privado ou dos ordenamentos jurídicos internos dos Estados, que não são abordados nos manuais.

Contudo, e apesar da completa escala de limiares apresentada, a imputação das formas mais brandas de confrontação no ciberespaço, que consistem nas mais habituais, fica limitada, embora a possibilidade de imputação indireta pelo método empregue permita avançar no assunto. A ciberespionagem é um caso paradigmático deste problema (TM 10.8,11.9-d; TM2 32). Contudo o grande leque de normas decorrentes da aplicação ao ciberespaço dos Regimes Especiais do Direito Internacional trouxe um contributo relevante em relação à situação prévia (TM2 Parte II).

Pelo seu interesse para a dissuasão, é necessário mencionar três casos que podem afastar a ilicitude de algumas respostas dos Estados:

- A invocação do "estado de necessidade" (TM 9.10-9.12, TM2 26), que não é dependente da prática de um ato ilícito prévio por parte de outro Estado,
- A "causa de força maior" que afasta a ilicitude pela força de circunstâncias que retiram ao Estado a possibilidade de eleger outro curso de ação (TM2 19.14-19.20, 26.23).
- A emergência vital (TM2 19.18-19.20).

Embora estas três opções de resposta possam ter baixo valor na perspetiva punitiva, há pouca dúvida do elevado valor que podem atingir na perspetiva da dissuasão defensiva.

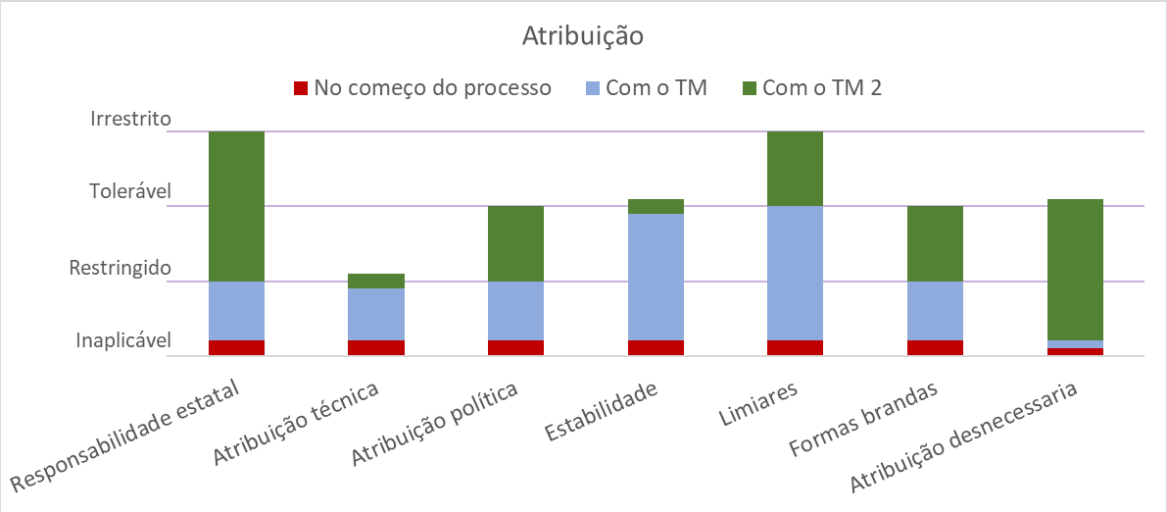


Figura 46 – Avaliação de indicadores de Imputação.

Fonte: (Autor, 2019)

B.3. Capacidade

As consequências do fracasso da dissuasão nuclear seriam catastróficas. Porém, o fracasso da dissuasão no ciberespaço não seria tão vital, exceto se os efeitos colaterais alcançassem domínios como o nuclear (Cimbala, 2016, p.57). Como a credibilidade da resposta dissuasória deve ser avaliada no contexto de a dissuasão ter falhado, no caso nuclear os limites legais para responder podem ser avaliados com maior lassitude (Brodie, 1958, pp.23-24).

Portanto, no caso ciber é imprescindível ultrapassar o paradoxo de ameaçar com o "uso da força", quando *a priori* este uso estaria vedado pelo Artigo 2(4) da Carta das Nações Unidas (CNU). Os Manuais referem que esta ameaça é possível, desde que o "uso da força" ou outras medidas que se empregassem fosse legais (TM 12.3, TM2 70.3). A aquisição de capacidades é legitimada, uma vez que não constitui uma ameaça, nos termos do artigo 2(4) da CNU (TM 12.4, TM2 70.4).

O facto de o *jus in bello* ser aplicável desde as primeiras hostilidades (Mulinen, 1987, p.7) obriga a avaliar as potenciais respostas nesta perspectiva. Consequentemente, segundo os Manuais, as armas dissuasórias devem permitir concretizar os efeitos e limitá-los a alvos claramente definidos, devendo também permitir a avaliação prévia e posterior de danos (TM 43 a 59, TM2 105-121).

A capacidade para responder legitimamente com o "uso da força" contra atividades adversárias no ciberespaço fica muito limitada pelo facto de a CNU, e a obrigação de resolver as disputas internacionais por vias pacíficas, corresponderem a um costume

internacional (TM2 65; UN, 2015b, *cit.por* TM2 65). Os conceitos "uso da força" e "legítima defesa" são também aplicáveis independentemente da arma utilizada (TM p.42; TM2 p.328). São dois os casos em que se admite o "uso da força": a "legítima defesa" (TM 13,16; TM2 71-74) e a intervenção sob mandato do Capítulo VII da CNU (TM 18; TM2 76). No segundo caso, é de salientar que apesar de o Artigo 2(7) da CNU impedir a interferência em matérias internas dos Estados, a natureza interconectada do ciberespaço pode levar a esta interferência quando haja riscos para a paz e segurança internacionais (TM2 67.2-67.4).

A resposta em legítima defesa está sujeita aos requisitos de necessidade, proporcionalidade, iminência e contiguidade (TM 13-15; TM2 72-73), bem como à determinação *ex ante* do "ataque armado" e do atacante (TM 13.21, TM2 71.23). Este posicionamento quanto à determinação *ex ante* contrasta com posicionamentos (Alexander, 2010, p.11-12) que afirmam que se podem tomar ações mesmo sem a identificação prévia do atacante, desde que se respeitem as diretrizes ou regras políticas de empenhamento (SROE). O TM2 permitiu avançar neste tema, enquadrando as respostas sem determinação *ex ante* no "estado de necessidade" (TM2 19.26). Por outro lado, se o ataque inicial desencadeasse o conflito, a resposta já seria no quadro do *jus in bello*, sendo desnecessário identificar o atacante, mas dever-se-ia delimitar e restringir o alvo a objetivos militares legítimos (TM 49-50, TM2 111-112).

O recurso aos ataques preventivos é deslegitimado nos dois Manuais (TM 15.7; TM2 73.10), o que inicialmente reforça as probabilidades de êxito da dissuasão (Knopf, 2010, p.7). Todavia, os autores dos TM aceitam a autodefesa antecipatória, adotando como legítima a modalidade da "última janela de oportunidade", que é a que melhor se adapta ao contexto temporal no ciberespaço (TM 15.4; TM2 73.4).

Para além da autodefesa antecipatória, a simples correção de vulnerabilidades permite tirar a eficácia das ciber-armas adversárias sem conflito legal algum. Ainda mais, a publicação das vulnerabilidades, ao facilitar a sua correção, contribui para um ciberespaço mais seguro, acrescentando o contributo para a estabilidade (Goldman, 2015, p. 321). A possibilidade de colocar nos sistemas adversários ciber-armas ocultas que continuem a ser efetivas depois de fixar as vulnerabilidades iniciais (Bejtlich, 2005, pp. 17 e 18) permitiria aumentar a estabilidade global mantendo a capacidade de retaliação no ciberespaço. A questão de legitimidade que se levanta é resolvida ao considerar no quadro do *jus ad bellum* que este mecanismo intrusivo não qualificaria como "ataque armado iminente",

exceto se já estivesse decidido o emprego efetivo da ciberarma. O risco político e de credibilidade reside no facto de a faculdade de avaliação residir em quem sofre a instalação (TM 15.6; TM2 73.7-73.8).

Na perspetiva técnica, para garantir uma capacidade de atuação eficaz no ciberespaço, é fulcral evitar que o adversário corrija as vulnerabilidades aproveitáveis nos seus sistemas. Neste sentido, a consideração de não ser obrigatório revelar as técnicas de imputação forense (TM2, p.83) contribui positivamente para a capacidade.

Da análise da capacidade de defesa ativa, entendida como contra ciberoperação automática sobre computadores atacantes, conclui-se que as limitações para o seu emprego são elevadas. A razão encontra-se nas dificuldades operacionais e técnicas (Libicki, 2009a, p.61) para efetivar os critérios exigíveis para a "legítima defesa" (TM 13-15; TM2 72-73), ou para os ataques no quadro do *ius in bello* (TM 49-59, TM2 111-121).

O emprego de ciber-armas de forma não automática facilita a sua licitude, mas poderá levantar dificuldades perante os tempos de resposta úteis no ciberespaço. Acrescentando a isto a dificuldade de inspeção das ciber-armas, para garantir que cumprem as regras do Direito dos Conflitos Armados (TM 48; TM2 110), concluímos que as respostas dissuasórias com ciber-armas são muito limitadas.

Nos casos em que não se verificam os elementos necessários para responder às ações ilegais do adversário no ciberespaço com o "uso da força"[18], cabe aplicar contramedidas com a finalidade única de impelir o adversário a cumprir a lei[19]. O uso de contramedidas exige o cumprimento dos seguintes princípios (TM 9; TM2 20-25), entre outros:

- Necessidade de imputar o ilícito a um Estado (TM 9; TM2 20).
- Responsabilidade estatal se o ilícito tiver sido mal atribuído (TM2 20.16).
- Falta de unanimidade sobre a não obrigatoriedade de tentar previamente respostas mais brandas (TM2 21.4)
- Não há contramedidas antecipatórias (TM2 21.5).
- Por serem medidas temporárias devem ser, na medida do possível, reversíveis (TM 9.6; TM2 21.8).
- Necessidade de notificação previa, com exceções (TM 9.4; TM2 21.10, 21.12).

[18] Há falta de unanimidade sobre a legalidade do "uso da força" debaixo do limiar do "ataque armado".

[19] A regra (TM2 20) estende a finalidade para incluir compromissos, garantias (TM2 27) e reparação de danos (TM2 28).

- Limitação nas violações do Direito Internacional admissíveis em aplicação de contramedidas (TM 9.5; TM2 22)
- Proporcionalidade em relação ao ilícito que as provoca e reciprocidade desnecessária (TM 9.7; TM2 23).
- Proibição de violar o Direito Internacional em relação a terceiras partes, mas não de as afetar incidentalmente (TM2 25).

Estas limitações são positivas para a estabilidade em termos gerais (Machado, 2013, p.650).

O emprego de capacidades ofensivas assente na invocação das figuras de "estado de necessidade", "força maior" ou "perigo/socorro" tem pouco valor dissuasório punitivo pela possível exigência de reparação posterior do dano causado (Espada, 1987, pp.131-135).

Se o adversário não tiver ultrapassado o limiar da atuação ilegal, a retorsão[20] ainda fica disponível no leque de capacidades (TM 9.13; TM2 20.4,24.5).

Adicionalmente cabem outras respostas aos ciberataques nos domínios do Direito Internacional Privado ou dos ordenamentos jurídicos internos dos Estados (TM p.4,2,13.16,14.2 TM2 8-14), que completam o leque de respostas contra as ofensas mais brandas.

O efeito multiplicador do ciberespaço na esfera da informação e a utilidade das operações de informação, sobretudo nas estratégias dissuasórias defensivas, obrigam a considerar especificamente esta capacidade para obter um balanço favorável da opinião pública internacional, incrementado assim o custo da ofensa, especialmente das formas mais brandas (Smith, 2009, pp.51-54, Libicki, 2012, pp. 14,39,46,49).

O termo "armas de informação" introduzido na proposta inicial do Código Internacional de Conduta para a Segurança da Informação (UN, 2011b, p.4) liderado pela Rússia e pela China, pode abranger aplicações para redes sociais em eventos similares às verificadas nas Primaveras Árabes (Thomas, 2017, p.8). Muitos Estados fundamentam no interesse da liberdade de expressão e de informação um posicionamento contrário a esta interpretação (Rõigas, 2015). Neste sentido, importa destacar que os Estados têm obrigações positivas, para assegurar o exercício dos direitos fundamentais, e negativas, para se autolimitar no constrangimento destes direitos. (Tikk et. al, 2010, pp.40-46).

[20] Resposta não amistosa mais legal frente a ações inamistosas legais (ou ilegais) do adversário.

O emprego de operações de informação está limitado pela possibilidade de poder ser qualificado como "intervenção ilegal", caso atinja o limiar da coerção (TM 10.10; TM2 21.5). Abaixo deste limiar, os critérios de avaliação (TM 11.9; TM2 6.27,69.9) podem ser muito úteis para construir uma mensagem efetiva para elevar os custos políticos do agressor. A propaganda, em termos gerais, não constitui violação da soberania (TM2 4.29) e pode ser impossível de perseguir extraterritorialmente (TM2 9.19,10.3).

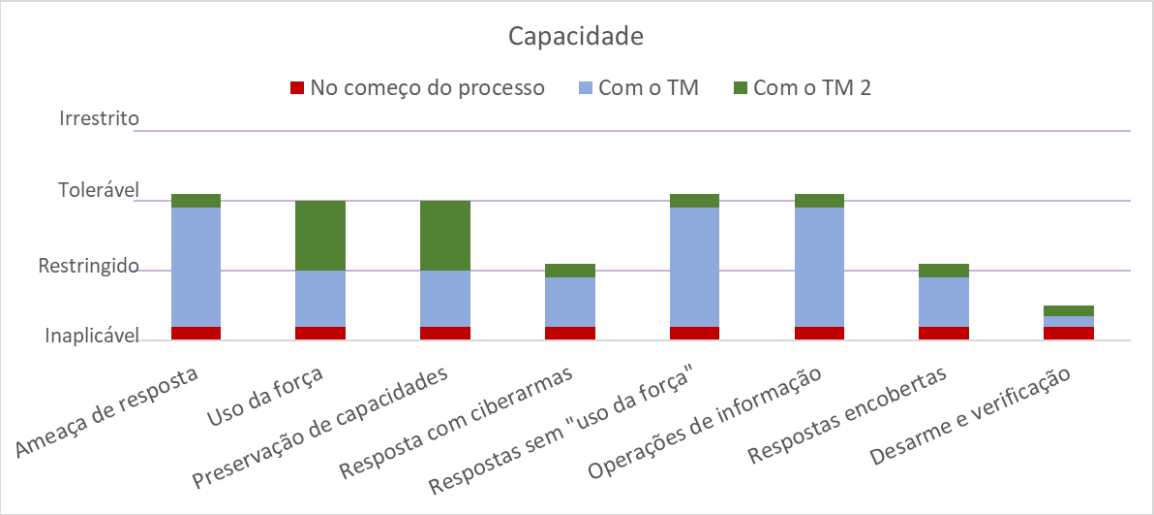


Figura 47 – Avaliação de indicadores de Capacidade.

Fonte: (Autor, 2019)

A possibilidade de empregar respostas encobertas (*sub-rosa*), quando não seja recomendável uma resposta pública (Libicki, 2009a, pp.92-102) não é fácil. No caso da legítima defesa, apesar do caráter consuetudinário deste direito, não cumprir com a obrigação de comunicação ao Conselho de Segurança constitui, para os Estados membros, uma violação do artigo 51 da CNU (TM 17; TM2 75). No caso das contramedidas (TM 9; TM2 21) os requerimentos decorrentes da finalidade destas também complicam as respostas encobertas, o que não acontece no caso da retorsão.

Por fim, os manuais não oferecem interpretações que contribuam significativamente para o desarme e a verificação de capacidades.

B.4. Ambiguidade

Nos subcapítulos dedicados à imputação e às capacidades verificou-se a disponibilidade de um leque abrangente de limiares justificantes do emprego de um leque não menos abrangente de respostas legais. O facto de os Manuais atribuírem em termos gerais uma flexibilidade interpretativa ao Estado atacado (TM 11,14.4,15.6,15.7; TM2

6.30,69,72.4,73.8) permite ajustar a nitidez dos limiares, garantindo que o ofensor deixa uma faixa de segurança abaixo do limiar, e que o atacado dispõe de uma margem de manobra acima do limiar. As necessidades de avaliação contextual estabelecidas também vão nesta direção (TM 14.5; TM2 7.16, p.81,15.9,15.13,15.16,18.5,26.2,27.7,72.5). Assim seria possível a avaliação conjunta de vários ciberataques para considerar ultrapassado um limiar que não seria ultrapassado se esses ciberataques fossem avaliados de forma independente. Por fim, o grande leque de normas decorrentes da aplicação no ciberespaço dos Regimes Especiais do Direito Internacional também acrescenta uma maior flexibilidade (TM2 Parte II).

Assim as regras interpretativas dos manuais contribuem para a dissuasão inclusivamente contra as formas mais brandas de confrontação e contra as atividades de reconhecimento, o que contribui para a estabilidade. De facto, num contexto de discordância entre Estados quanto à aplicabilidade do Direito Internacional no ciberespaço (TM p.3), os Manuais apresentam um contributo global para a estabilidade, porque apresentam um modelo interpretativo de referência para que os potenciais agressores possam fazer uma avaliação racional prévia dos custos (Deeks, 2015).

A ambiguidade em relação à natureza e intensidade da resposta em "legítima defesa" está garantida por ser desnecessário que a natureza da resposta seja a mesma que a da ofensa, e porque a quantidade de foça empregada se estabelece em relação à necessidade de efetivar a defesa e não em relação à empregada pelo atacante (TM 14.5, TM2 72.5). A situação é semelhante no caso das contramedidas (TM 9.7, TM2 23), embora o conceito de proporcionalidade seja diferente (TM2 23)

A ambiguidade em relação ao momento da resposta está limitada pelos princípios de iminência e contiguidade. O conceito de "última janela de oportunidade" (TM 15.4; TM2 73.4) permite flexibilizar o momento da resposta frente a ciberataques iminentes; também a dependência de contexto da autodefesa transfronteiriça imediata (TM2 71.26). O requisito de contiguidade também pode ser dotado de alguma ambiguidade, por exemplo enquadrando a ofensa numa "cibercampanha" (TM 15.9; TM2 73.13). Para as respostas por debaixo do limiar das contramedidas não há restrições de contiguidade.

A margem de ambiguidade na origem geográfica das respostas em "legítima defesa" em termos gerais é baixo, e está limitado ao espaço soberano dos Estados-vítima e agressor (TM 13.23-13.24; 71.25-71.26). A possibilidade de que não fique legitimada a intervenção de Estados não afetados pelo agressor reforça esta limitação, também no caso das

contramedidas (TM2 19.13). Restaria a possibilidade excecional de invocar o "estado de necessidade" (TM 9, TM2 26). Contudo, as regras de "diligência devida" induzem uma ambiguidade geográfica elevada no atacante. Porque qualquer Estado ficaria legitimado para não permitir uma ciberoperação roteada através do seu território (TM 5, TM2 6-7). Todavia, outras vias, como a autodefesa coletiva (TM 16,19; TM2 74,77), podem contribuir mais facilmente para a ambiguidade geográfica.

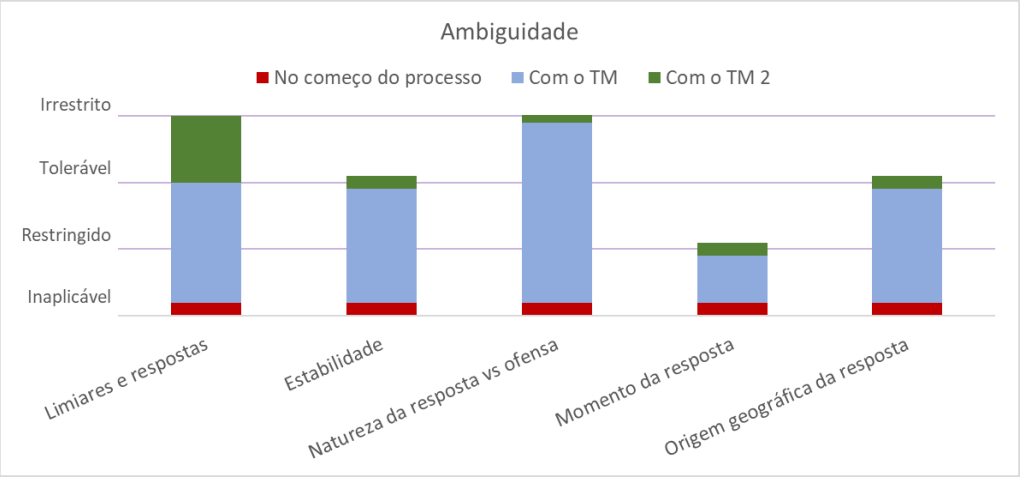


Figura 48 – Avaliação de indicadores de Ambiguidade.

Fonte: (Autor, 2019)

B.5. Cooperação

Os Manuais contribuem diretamente para a dissuasão alargada, pela sua abordagem das questões da soberania (TM 1-5; TM2 1-13), da autodefesa coletiva (TM 16; TM2 74), do papel das organizações regionais (TM 19, TM2 77) ou a tomada de contramedidas contra ilícitos que afetam vários Estados (TM 9.8; TM2 24.4-24.7, 27.2). Ainda assim, persistem limitações, por exemplo para adotar contramedidas em benefício de outro Estado (TM2, 24.5-24.9).

A contribuição de cada Estado para a cibersegurança pode influenciar outros Estados para contribuir igualmente, até delimitar uma fronteira de cibersegurança que exclui os Estados não comprometidos, expostos às suas ameaças e a ser considerados origem dos ciberataques (Hare, 2009, p.9-14). Na contribuição para esta segurança interdependente, sobressaem as regras de "diligência devida" (TM 5; TM2 6-7), de onde se destaca a possibilidade de os Estados requererem a intervenção de entidades privadas sob sua jurisdição quando for necessário (TM 5.9; TM2 7.19). Porém, é de salientar que os Estados

não estão obrigados a aceitar a cooperação de terceiros para cumprir com a "diligência devida", que é apenas exigível dentro das suas capacidades (TM2 7.26). Este facto contribui positivamente para a estabilidade em relação à preservação de capacidades.

No domínio da imputação, a cooperação entre Estados é fundamental para ultrapassar alguns dos problemas decorrentes da multiplicidade jurisdicional (TM 2; TM2 8,11) e da atuação de terceiros Estados (TM2 18).

Em consequência, as interpretações dos Manuais facilitam a cooperação para acrescentar as capacidades. Podemos destacar que:

- Um Estado atacado pode autorizar operações de outro Estado, ou de uma organização internacional, a partir do seu território (TM 1.8; TM2 4.31-4.32).
- Em infraestruturas e atividades controladas por vários Estados, a diligência devida é exigível a todos eles (TM2 6.12), o que também os legitima para atuar.
- Um Estado pode apoiar outro Estado, sem assumir responsabilidade legal internacional, agregando-lhe elementos que fiquem sob o controlo pleno do segundo (TM2 16)
- A aplicação coletiva de contramedidas é facilitada pela sua legitimação para reestabelecer obrigações devidas a um grupo de Estados ou obrigações *erga omnes* (TM 19.8; TM2 24.4-24.7, 27.2).
- Quando proceda reparar os danos por uma ação coletiva, o custo não excederá o do dano causado (TM2 28.11).
- As organizações regionais podem atuar sob autorização ou mandato do CSNU também em ciberoperações (TM 19; TM2 77).

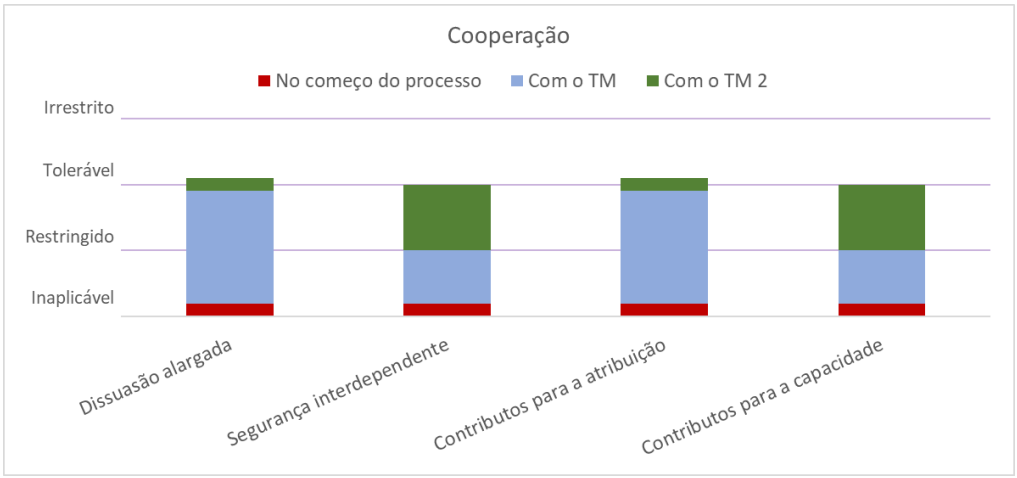


Figura 49 – Avaliação de indicadores de Cooperação.

Fonte: (Autor, 2019)

Como elementos limitadores destacam-se a possibilidade de atribuir responsabilidade legal internacional às organizações internacionais (TM2 31) e o facto de as possibilidades de cooperação fazerem menos justificável a invocação do "estado de necessidade" (TM2 26.21).

B.6. Comunicação e sinalização

As regras de interpretação constantes dos Manuais de Tallinn quanto aos limiares que devem respeitar os Estados quando atuam no ciberespaço constituem os andaimes para estabelecer um esquema de sinalização apropriado para qualquer estratégia de dissuasão no ciberespaço. Assim, permite diferenciar os patamares: ataque armado, uso da força, atuação ilegal, ação não amistosa, delito privado e, embora com diferente fundamento, estado de necessidade. Estes limiares, avaliáveis qualitativamente em termos de escala e efeitos (TM 6,11-15; TM2 14-30,69-73), são naturais e óbvios porque assentam nos princípios do Direito Internacional vigente, embora aplicado ao ciberespaço e contextualizado em termos de alcance e aplicabilidade (TM, pp.5,6). E como se discutiu em subcapítulos precedentes são discretos, distintos e finitos. Cumprem, portanto, as condições estabelecidas por Schelling (1966, p.119-138).

Em consequência, na perspetiva da assimilabilidade da mensagem, permite estabelecer uma narrativa pré-crise que estabeleça os padrões de referência legal e ética em que sustentar o discurso ao longo dos processos de gestão de crises (Libicki, 2012, p.71). Este padrão de referência de atitudes aceitáveis e não aceitáveis contribui para perceber os sinais, para comunicar a determinação de não aceitar determinados padrões comportamentais e para comunicar as capacidades de resposta que poderão ser empregues, sem risco de rejeição pela comunidade internacional.

O referido padrão de referência também permite reajustes decorrentes da sinalização empregue pelos adversários, permitindo a flexibilidade interpretativa necessária para facilitar a negociação com aqueles Estados que optem por outras abordagens ou que estejam vinculados por outros Tratados para além dos que foram considerados pelos manuais (TM, p.6). Adicionalmente, o facto de os manuais não serem considerados doutrina interpretativa vinculativa possibilita a mudança de regras e atenua o risco de bloqueios resultante de discordâncias quanto ao regime legal aplicável (TM, p.3,43; TM2, p.329).

A velocidade dos sistemas computacionais atuais pode constituir uma ameaça para a estabilidade, caso se permita que o ciclo da decisão ultrapasse a velocidade de perceção e comunicação humana. Neste sentido, a aceitação pelos autores dos TM de uma "autodefesa antecipatória" antes de lançado o ataque (TM 15.3, 73.2,73.3), e o facto de rejeitarem o critério de tempo para avaliar a legitimidade da resposta, contribuem positivamente para a sinalização e para a estabilidade. A opção interpretativa adotada, "a última janela de oportunidade" (TM 15.4; TM2 73.4,73.5), é muito apropriada para a gestão temporal da sinalização no contexto do ciberespaço.

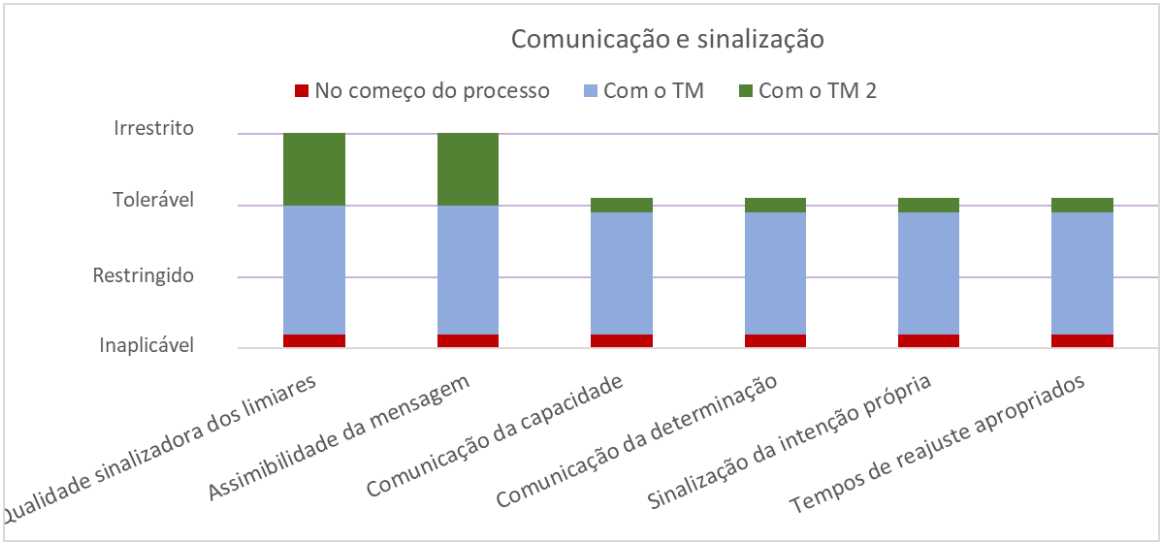


Figura 50 – Avaliação de indicadores de Comunicação e Sinalização.

Fonte: (Autor, 2019)

Por forma a consolidar a fundamentação teórica que permita desenvolver o processo dedutivo para responder à primeira pergunta derivada desde a perspetiva da praxe internacional, ao longo deste apêndice analisaram-se, na sua dimensão teórica, os contributos para a dissuasão no ciberespaço dos dois manuais de Tallinn.

O estudo permitiu verificar que os contributos dos manuais sobre as componentes do problema da dissuasão no ciberespaço (variáveis independentes) são diferenciados a nível de indicador, bem como determinar, numa escala qualitativa, a posição do filtro de legitimidade para a inclusão numa estratégia dissuasória credível de cada uma das subcomponentes correspondentes aos respetivos indicadores.

Contudo, a resposta à primeira pergunta derivada não ficará completa até que se acrescentem os resultados da análise na dimensão prática, que são abordados no Capítulo 2 deste relatório.

Apêndice C — Mapa conceitual e modelo de análise

HIPÓTESE 1 - Os efeitos do Processo do Manual de Tallinn são distintos a nível de cada dificuldade de dissuasão no ciberespaço.			
CONCEITOS	**DIMENSÕES**	**VARIÁVEIS H1**	**INDICADORES**
Dissuasão no ciberespaço	Teórica Prática das relações internacionais	Soberania	Vínculo territorial
			Jurisdição e extraterritorialidade
			Controlo fronteiriço
			Controlo de terceiras partes/outros atores
			Compatibilidade com a imputação
			Compatibilidade com a cooperação
		Imputação	Responsabilidade estatal
			Imputação técnica
			Imputação política
			Estabilidade
			Limiares
			Formas brandas
			Imputação desnecessária
		Capacidade	Ameaça de resposta
			Uso da força
			Preservação de capacidades
			Resposta com ciberarmas
			Respostas sem "uso da força"
			Operações de informação
			Respostas encobertas
			Desarme e verificação
		Ambiguidade	Limiares e respostas
			Estabilidade
			Natureza da resposta vs ofensa
			Momento da resposta
			Origem geográfica da resposta
		Cooperação	Dissuasão alargada
			Segurança interdependente
			Contributos para a imputação
			Contributos para a capacidade
		Comunicação e Sinalização	Qualidade sinalizadora dos limiares
			Assimibilidade da mensagem
			Comunicação da capacidade
			Comunicação da determinação
			Sinalização da intenção própria
			Tempos de reajuste apropriados

HIPÓTESE 2 - A compatibilidade do Processo do Manual de Tallinn com as opções de dissuasão no ciberespaço decorre do seu impacto sobre as dificuldades de dissuasão consideradas e da adoção de uma opção de dissuasão alinhada sinergicamente com os contributos que o Processo traz para ultrapassar cada dificuldade.			
CONCEITOS	**DIMENSÕES**	**VARIÁVEIS**	**INDICADORES**
Opção de dissuasão	Teórica Prática das relações internacionais	Dissuasão punitiva	Variáveis H1
		Dissuasão defensiva	Variáveis H1

Apêndice D — Código desenvolvido para a análise relacional com o pacote *igraph* para *R*

```
######### Análise relacional da codificação realizada com o RQDA

#### Cabeçalho

### Estabelecer o diretório de trabalho
setwd("E:/Militar/MASTER_CMSD/RQDA")

### Librarias

library(RQDA)
library(igraph)
windowsFonts(Arial=windowsFont("Arial"))

### Abrir o programa RQDA
RQDA()

### Declaração/inicialização de variáveis globais

## Abrir o projeto em RQDA e Conectar com Base de Dados em RQDA
# Para a codificação inicial ativar as duas linhas seguintes
openProject("TFM_TM_Dissuasao_Codif_Inicial.rqda", updateGUI = TRUE)
conRQDAgrf <- dbConnect(RSQLite::SQLite(), "TFM_TM_Dissuasao_Codif_Inicial.rqda")
# Para trabalhar com a codificação final desativar as linhas anteriores e ativar a seguintes
#openProject("TFM_TM_Dissuasao_Codif_Final.rqda", updateGUI = TRUE)
#conRQDAgrf <- dbConnect(RSQLite::SQLite(), "TFM_TM_Dissuasao_Codif_Final.rqda")

## Variábeis globais
# dataframe inicializada com tabela coding + nome codigo da BD
#dfrCoding<-dbGetQuery(conRQDAgrf, "SELECT *, freecode.name FROM coding, freecode WHERE
coding.cid=freecode.id AND (id=3 OR id=18)")
# dataframe inicializada com tabela source (arquivos) da BD
#dfrArquivos<-dbGetQuery(conRQDAgrf, "SELECT * FROM source")
# dataframe inicializada com tabela freecode (códigos) da BD
#dfrCodigos<-dbGetQuery(conRQDAgrf, "SELECT * FROM freecode")
dfrNosCodVarInd<-dbGetQuery(conRQDAgrf,
                "SELECT freecode.id, freecode.name, codecat.catid, codecat.name AS catname
                FROM freecode, codecat, treecode WHERE
                freecode.id=treecode.cid AND treecode.catid=codecat.catid AND freecode.status=1 AND
treecode.status=1
                AND (codecat.name='Variáveis_H1' OR codecat.name='Indicadores' OR
codecat.name='Indicadores_transversais')")
dfrNosCodVarInd<-dfrNosCodVarInd[with(dfrNosCodVarInd, order(dfrNosCodVarInd$name)), ]
#tblCodArq.m<-as.matrix(table(dfrCoding$fid,dfrCoding$name)) # matriz de frequencias, codes por aquivo
#tblCodArq01.m<-tblCodArq.m
#tblCodArq01.m[tblCodArq01.m>0]<-1 # matriz, caso code no aquivo ->1, se não ->0

###  Declaração de funcões
```

```
##1# Função EstruGrafo. Evalua a estrutura dum grafo. (Precisa libraria igraph). (Valdez,2016)
EstruGrafo=function(grafo){
 wtc <- cluster_walktrap(grafo)  # Análise de subgrafos e comunidades por caminhos aleatorios
 estGr<-data.frame(
   Indicadores =c("Nós","Relações", "Relações potenciais","Densidade (%
rel.pres.)","Dâimetro","Long.caminho.méd","Grau médio",
    "Modularidade","Coefic.cluster"),
   Valor=c(vcount(grafo),ecount(grafo),(vcount(grafo)*(vcount(grafo)-1))/2,round(graph.density(grafo),
2),diameter(grafo),
         round(average.path.length(grafo),2),round(mean(degree(grafo)),2),
         round(modularity(grafo,membership(wtc)),2), round(transitivity(grafo),2)
   ))
 return(estGr)
}


##2# Função AdjListCodesXArq : Lista de nodos adjacentes. Critério: Número de arquivos em que
coincidem .

AdjListCodesXArq=function(dfrCodigos){
 #  Calculo da matriz com a lista de adjacência ponderada.Colunas 1 e 2 são vertices, coluna 3 pesos.
 #  dfrCodigos é um data.frame inicializada com tabela freecode (códigos) da BD ou um filtrado da mesma
 #  Peso= número de arquivos comuns entre os dois codigos relacionados.
 numArestas=(dim(dfrCodigos)[1]^2-dim(dfrCodigos)[1])/2 # numero de arestas dum grafo = (nodos^2-
nodos)/2
 mtrCodesAdj<-matrix(0,numArestas,3) # Inicialização da matriz de adjacência
 colnames(mtrCodesAdj) <-c("from","to","weight")
 origem=dim(dfrCodigos)[1] # inicialização contador de origens de aresta
 aresta=numArestas # inicialização do contador de arestas
  while (origem>0){
  mtrCodesAdj[aresta,1]=dfrCodigos$id[origem]
  destino=origem-1 # inicializaçõ contador de destinos de aresta
  while (destino>0&aresta>0){
   # asignação de origem e destino da aresta
   mtrCodesAdj[aresta,1]=dfrCodigos$id[origem]
   mtrCodesAdj[aresta,2]=dfrCodigos$id[destino]
   # Cálculo e asignação do peso da aresta
   mtrCodesAdj[aresta,3]=dim(as.matrix(filesCodedByAnd(mtrCodesAdj[aresta,],"coding")[]))[1]
   # contadores
   destino=destino-1
   aresta=aresta-1
  }
  origem=origem-1
 }

 # resultado
 return(mtrCodesAdj)
}
##
```

```
##3# Função AdjListCodesXSolap: Lista de nodos adjacentes. Critério: Número de fragmentos comuns aos dois códigos.

AdjListCodesXSolap=function(dfrCodigos){
 #  Calculo da matriz com a lista de adjacência ponderada. Colunas 1 e 2 são vértices, coluna 3 pesos.
 #  dfrCodigos é um data.frame inicializada com tabela freecode (códigos) da BD ou um filtrado da mesma
 #  Peso= número de arquivos comuns entre os dois codigos relacionados.
 numArestas=(dim(dfrCodigos)[1]^2-dim(dfrCodigos)[1])/2 # numero de arestas dum grafo = (nodos^2-nodos)/2
 mtrCodesAdj<-matrix(0,numArestas,3) # Inicialização da matriz de adjacência
 colnames(mtrCodesAdj) <-c("from","to","weight")
 origem=dim(dfrCodigos)[1] # inicialização contador de origems de aresta
 aresta=numArestas # inicialização do contador de arestas
 while (origem>0){
  mtrCodesAdj[aresta,1]=dfrCodigos$id[origem]
  destino=origem-1 # inicializaçõ contador de destinos de aresta
  while (destino>0&aresta>0){
   # asignação de origem e destino da aresta
   mtrCodesAdj[aresta,1]=dfrCodigos$id[origem]
   mtrCodesAdj[aresta,2]=dfrCodigos$id[destino]
   # Cálculo e asignação do peso da aresta. Número de solapamentos dos códigos "origem" y "destino"
   # Emprega a função crossTwoCodes de RQDA verificando "overlap"+"inclusion"+"exact", desde que em
   # RQDA estes tipos de relação são estritos e os mais abrangentes não incluem os menos abrangentes.

mtrCodesAdj[aresta,3]=(crossTwoCodes(mtrCodesAdj[aresta,1],mtrCodesAdj[aresta,2],data=getCodingTable(), relation="overlap")
                       +crossTwoCodes(mtrCodesAdj[aresta,1],mtrCodesAdj[aresta,2],data=getCodingTable(), relation="inclusion")
                       +crossTwoCodes(mtrCodesAdj[aresta,1],mtrCodesAdj[aresta,2],data=getCodingTable(), relation="exact"))
    # contadores
    destino=destino-1
    aresta=aresta-1
  }
  origem=origem-1
 }

 # resultado, matriz de ajacencia por solapamento de códigos
 return(mtrCodesAdj)
}
##

#####################################################################

##### Corpo do script

#### Grafos

###1# Grafo "grfVarIndXArq" de relações entre códigos das Categorias Variáveis_H1, Indicadores e
```

```
Indicadores transversais
# Critério de relação: conincidência no mesmo arquivo
dfrArestasVarIndXArq<-as.data.frame(AdjListCodesXArq(dfrNosCodVarInd))
grfVarIndXArq<-graph_from_data_frame(d=dfrArestasVarIndXArq, vertices=dfrNosCodVarInd, directed =
F)
# Eliminar as arestas de peso =0
grfVarIndXArq<-delete.edges(grfVarIndXArq,E(grfVarIndXArq)[weight<=0])

## Criação dos arquivos com os grafos "grfVarIndXArq" de saída, .png
 # Cor dos vértices por categoria
 colorCateg<-matrix()
 colorCateg[1]<-"green" # cor Variáveis_H1
 colorCateg[7]<-"tomato" # cor Indicadores
 colorCateg[15]<-"gold" # cor Indicadores_transversais
 colsLeg<-c(colorCateg[1], colorCateg[7], colorCateg[15])
 V(grfVarIndXArq)$color <- colorCateg[V(grfVarIndXArq)$catid]
 # Outros parâmetros do grafo
 V(grfVarIndXArq)$size <- degree(grfVarIndXArq)/4 # Tamanho dos vértices por grau
 V(grfVarIndXArq)$label <- V(grfVarIndXArq)$name # Etiqueta dos vértices por nome de código, cor preto,
...
 V(grfVarIndXArq)$label.color <- "blue"
 V(grfVarIndXArq)$label.family <- "Arial"
 V(grfVarIndXArq)$label.cex <- 1.8 # Tamanho da fonte
 E(grfVarIndXArq)$width <- E(grfVarIndXArq)$weight/12 # Espessura das arestas por peso
 E(grfVarIndXArq)$curved <-0.2

png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Arquivo_FR.png',  width = 1600, height = 1200, units
= "px")
 lFR <- layout_with_fr(grfVarIndXArq) # Disposição com algoritmo Fruchterman-Reingold, modelo atração-
repulsão de nodos
 par(mar=c(4,1,1,1), family="Arial")
 plot(grfVarIndXArq, layout=lFR, main= "Fruchterman-Reingold", cex.main=6) # Imprimir o grafo no
arquivo de saída
 # Rotulagem
 legend(x=-1.5, y=-1, c("Variáveis_H1","Indicadores","Indicadores_transversais"), pch=21,
       col="#777777", pt.bg=colsLeg, pt.cex=3, cex=2, bty="n", ncol=1)
dev.off()

png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Arquivo_LKK.png',  width = 1600, height = 1200, units
= "px")
 lKK<- layout_with_kk(grfVarIndXArq) # Disposição com algoritmo Kamada Kawai, também minimiza a
energía do sistema elástico
 par(mar=c(4,1,1,1), family="Arial")
 plot(grfVarIndXArq, layout=lKK, main="Kamada Kawai", cex.main=6) # Imprimir o grafo no arquivo de
saída
 # Rotulagem
 legend(x=-1.5, y=-1, c("Variáveis_H1","Indicadores","Indicadores_transversais"), pch=21,
       col="#777777", pt.bg=colsLeg, pt.cex=3, cex=2, bty="n", ncol=1)
dev.off()
```

```
## Análise estrutural do grafo impressa em txt
dfrEstrgrfVarIndXArq<-EstruGrafo(grfVarIndXArq)
write.table(x=dfrEstrgrfVarIndXArq,
        file = "Saida_grafos/Grafo_Variaveis_Indicadores_por_Arquivo_Estrutura.txt",
        fileEncoding = "UTF-8", quote=F, append=F)
dfrEstrgrfVarIndXArq # Também saída por consola

## Grafo de relações representado como MAPA DE CALOR
png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Arquivo_Mapa_Calor.png',  width = 800, height =
800, units = "px")
 par(mar=c(2,1,1,2), cex=22)
 mtrMapCalor <- get.adjacency(grfVarIndXArq, attr="weight", sparse=F)
 colnames(mtrMapCalor) <- V(grfVarIndXArq)$name
 rownames(mtrMapCalor) <- V(grfVarIndXArq)$name
 palf <- colorRampPalette(c("azure", "red1"))
 heatmap(mtrMapCalor[,], revC=T, Rowv = NA, Colv = NA, col = palf(100),
     scale="none", margins=c(18,18), cexRow=1.2, cexCol=1.2, main="Adjacência entre nós")
dev.off()

## Análise de grupos, "clusters" e comunidades
grfVarIndXArq_x<-delete.edges(grfVarIndXArq,E(grfVarIndXArq)[weight<=0]) # Eliminação arestas peso X

# Análise de comunidades baseado em propagação de etiquetas. Método não jerárquico
ComGrfVarIndXArq_x<- cluster_label_prop(grfVarIndXArq_x)
 png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Arquivo_Comunidades_Propaga_Etiquetas.png',
width = 2400, height = 1200, units = "px")
 par(mfrow=c(1,2), mar=c(2,1,1,2), cex=4)
 plot(ComGrfVarIndXArq_x, grfVarIndXArq_x, vertex.label.cex=0.5 )
dev.off()

# Análise de comunidades baseado no algoritmo de modularidade de Greedy
ComGrfVarIndXArq_x<- cluster_fast_greedy(grfVarIndXArq_x)
png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Arquivo_Comunidades_Greedy.png',  width = 2400,
height = 1200, units = "px")
 par(mfrow=c(1,2), mar=c(2,1,1,2), cex=4)
 dendPlot(ComGrfVarIndXArq_x, mode="hclust", cex=.5) # Dendograma da estrutura grupal
 plot(ComGrfVarIndXArq_x, grfVarIndXArq_x, vertex.label.cex=0.5 )
dev.off()

#####################################################################

###2# Grafo "grfVarIndXSolap" de relações entre códigos das Categorias Variáveis_H1, Indicadores e
Indicadores transversais
# Critério de relação: Solapamento do texto codificado = Terem texto codificado em comum
dfrArestasVarIndXSolap<-as.data.frame(AdjListCodesXSolap(dfrNosCodVarInd))
grfVarIndXSolap<-graph_from_data_frame(d=dfrArestasVarIndXSolap, vertices=dfrNosCodVarInd,
directed = F)
# Eliminar as arestas de peso =0
grfVarIndXSolap<-delete.edges(grfVarIndXSolap,E(grfVarIndXSolap)[weight<=0])
```

```
## Criação dos arquivos com os grafos "grfVarIndXSolap" de saída, .png
# Cor dos vértices por categoria
colorCateg<-matrix()
colorCateg[1]<-"green" # cor Variáveis_H1
colorCateg[7]<-"tomato" # cor Indicadores
colorCateg[15]<-"gold" # cor Indicadores_transversais
colsLeg<-c(colorCateg[1], colorCateg[7], colorCateg[15])
V(grfVarIndXSolap)$color <- colorCateg[V(grfVarIndXSolap)$catid]
# Outros parâmetros do grafo
V(grfVarIndXSolap)$size <- degree(grfVarIndXSolap)/4 # Tamanho dos vértices por grau
V(grfVarIndXSolap)$label <- V(grfVarIndXSolap)$name # Etiqueta dos vértices por nome de código, cor
preto, ...
V(grfVarIndXSolap)$label.color <- "blue"
V(grfVarIndXSolap)$label.family <- "Arial"
V(grfVarIndXSolap)$label.cex <- 1.8 # Tamanho da fonte
E(grfVarIndXSolap)$width <- E(grfVarIndXSolap)$weight/12 # Espessura das arestas por peso
E(grfVarIndXSolap)$curved <-0.2

png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Solapamento_FR.png',  width = 1600, height = 1200,
units = "px")
lFR <- layout_with_fr(grfVarIndXSolap) # Disposição com algoritmo Fruchterman-Reingold, modelo
atração-repulsão de nodos
par(mar=c(4,1,1,1), family="Arial")
plot(grfVarIndXSolap, layout=lFR, main= "Adjacencia por Solapamento. Fruchterman-Reingold",
cex.main=6) # Imprimir o grafo no arquivo de saída
# Rotulagem
legend(x=-1.5, y=-1, c("Variáveis_H1","Indicadores","Indicadores_transversais"), pch=21,
    col="#777777", pt.bg=colsLeg, pt.cex=3, cex=2, bty="n", ncol=1)
dev.off()

png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Solapamento_LKK.png',  width = 1600, height = 1200,
units = "px")
lKK<- layout_with_kk(grfVarIndXSolap) # Disposição com algoritmo Kamada Kawai, também minimiza a
energía do sistema elástico
par(mar=c(4,1,1,1), family="Arial")
plot(grfVarIndXSolap, layout=lKK, main="Adjacencia por Solapamento. Kamada Kawai", cex.main=6) #
Imprimir o grafo no arquivo de saída
# Rotulagem
legend(x=-1.5, y=-1, c("Variáveis_H1","Indicadores","Indicadores_transversais"), pch=21,
    col="#777777", pt.bg=colsLeg, pt.cex=3, cex=2, bty="n", ncol=1)
dev.off()

## Análise estrutural do grafo impressa em txt
dfrEstrgrfVarIndXSolap<-EstruGrafo(grfVarIndXSolap)
write.table(x=dfrEstrgrfVarIndXSolap,
        file = "Saida_grafos/Grafo_Variaveis_Indicadores_por_Solapamento_Estrutura.txt",
        fileEncoding = "UTF-8", quote=F, append=F)
dfrEstrgrfVarIndXSolap # Também saída por consola

## Grafo de relações representado como MAPA DE CALOR
```

```
png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Solapamento_Mapa_Calor.png',  width = 800, height = 800, units = "px")
par(mar=c(2,1,1,2), cex=22)
mtrMapCalor <- get.adjacency(grfVarIndXSolap, attr="weight", sparse=F)
colnames(mtrMapCalor) <- V(grfVarIndXSolap)$name
rownames(mtrMapCalor) <- V(grfVarIndXSolap)$name
palf <- colorRampPalette(c("azure", "red1"))
heatmap(mtrMapCalor[,], revC=T, Rowv = NA, Colv = NA, col = palf(100),
      scale="none", margins=c(18,18), cexRow=1.2, cexCol=1.2, main="Adjacência (solapamento) entre nós")
dev.off()

## Análise de grupos, "clusters" e comunidades
grfVarIndXSolap_x<-delete.edges(grfVarIndXSolap,E(grfVarIndXSolap)[weight<=0]) # Eliminação arestas peso X

# Análise de comunidades baseado em propagação de etiquetas. Método não jerárquico
ComGrfVarIndXSolap_x<- cluster_label_prop(grfVarIndXSolap_x)
png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Solapamento_Comunidades_Propaga_Etiquetas.png',  width = 2400, height = 1200, units = "px")
par(mfrow=c(1,2), mar=c(2,1,1,2), cex=2)
plot(ComGrfVarIndXSolap_x, grfVarIndXSolap_x, vertex.label.cex=1.1, main="Agrupamentos por etiquetas. Adjacencia por Solapamento."  )
dev.off()

# Análise de comunidades baseado no algoritmo de modularidade de Greedy
ComGrfVarIndXSolap_x<- cluster_fast_greedy(grfVarIndXSolap_x)
png('Saida_grafos/Grafo_Variaveis_Indicadores_por_Solapamento_Comunidades_Greedy.png',  width = 2400, height = 1200, units = "px")
par(mfrow=c(1,2), mar=c(2,1,1,2), cex=4)
dendPlot(ComGrfVarIndXSolap_x, mode="hclust", cex=.5) # Dendograma da estrutura grupal
plot(ComGrfVarIndXSolap_x, grfVarIndXSolap_x, vertex.label.cex=0.5, main="Agrupamentos Greedy. Adjacencia por Solapamento."  )
dev.off()


#### Fechar a conexão com a BD em RQDA
dbDisconnect(conRQDAgrf)
```

Apêndice E — Código desenvolvido para mineração e análise de texto com *tm* e *R*.

```
############## MINERAÇÃO DE TEXTOS ################

#### Cabeçalho

### Estabelecer o diretório de trabalho
setwd("E:/Militar/MASTER_CMSD/RQDA")

### Librarias
library(RQDA)
library(tm)
library(wordcloud)
library(ggplot2)
windowsFonts(Arial=windowsFont("Arial"))

### Declaração de FUNçõES

## FUNÇÃO LimparCorpus. Elimina e acondiciona o texto do corpus para a análise.
LimparCorpus<-function(corpus){
 corpus<-tm_map(corpus, content_transformer(function(x) iconv(x, to='ASCII', sub='byte'))) # Conversão a ASCII
 corpus <- tm_map(corpus, tolower) # muda para minúsculas
 corpus<- tm_map(corpus,removePunctuation)# eliminar signos de pontuação
 corpus <- tm_map(corpus, removeNumbers) # eliminar números
 corpus <- tm_map(corpus, removeWords,stopwords("english")) # eliminar palavras vazias genéricas do inglês
 corpus <- tm_map(corpus, removeWords,stopwords("SMART")) # eliminar palavras vazias genéricas do inglês,
 corpus <- tm_map(corpus, stripWhitespace) # eliminar espaços em branco

 return(corpus)
}
# Fim FUNÇÃO LimparCorpus.

## FUNÇÃO NuvemPalavras. Constrói uma nuvem de palavras com os fragmentos de texto codificados "codifs"
NuvemPalavras<-function(fragmentos,titulo,vPalVacias,cores,maxPalavras,minFrec,raiz){
 # fragmentos     Datraframe: Fragmentos de texto para analisar
 # titulo         Título do gráfico impresso
 # vPalVacias     Vector: Palavras pouco significativas específicas para esta análise
 # cores          Paleta de cor para o gráfico
 # maxPalavras    Número máximo de palavras a representar no gráfico
 # minFrec        Frequência mínima duma palavra para ser representada
 # raiz           Boolean: se TRUE lematiza as palavras agrupando as de raiz comum

 # Caso o corpus esteja vazio imprimir png e terminar:
 numFragmentos<-length(fragmentos[fragmentos!=""])
 cat( numFragmentos," fragmentos de texto no corpus", "\n", "\n") # Ecrã: Número de fragmentos no
```

```
corpus
 if (numFragmentos==0){
  png(paste0("Saida_tm/Nuvem_",titulo,".png"), width = 400, height = 400, units = "px")
  layout(matrix(c(1,2), nrow=2), heights=c(4,8))
  par(mar=c(0,0,0,0))
  plot.new()
  text(x=0.5, y=0.5, paste0(titulo,"\r\n \r\n \r\n", numFragmentos," fragmentos de texto"),
     cex=1.4, font= 4, col.main= "darkgrey")
  dev.off()
  return()
 }
 # Criar o corpus de documentos em inglês:
 corpus <- Corpus(VectorSource(fragmentos), readerControl=list(language = "en"))
 # Limpar e preparar o corpus documental:
 corpus <- LimparCorpus(corpus)
 corpus <- tm_map(corpus, removeWords,vPalVacias) # eliminar as palavras contidas em vPalVacias
 if (raiz==T) {corpus <- tm_map(corpus,stemDocument)} # lematizar: agrupar flexões gramaticais da
mesma raiz.

 # Criar a nuvem de palavras e imprimi-la num ficheiro .png
 png(paste0("Saida_tm/Nuvem_",titulo,".png"), width = 400, height = 400, units = "px")
  layout(matrix(c(1,2), nrow=2), heights=c(2,16))
  par(mar=c(0,0,0,0))
  plot.new()
  text(x=0.5, y=0.5, paste0(titulo,"\r\n", numFragmentos," fragmentos de texto no corpus"),
     cex=1.5, font= 4, col.main= "darkgrey")
  wordcloud(corpus, max.words = maxPalavras, colors = cores, min.freq = minFrec, random.order = F)
 dev.off()

 # Imprimir txt com os fragmentos originais analisados:
 write.table(fragmentos[fragmentos!=""], file = paste0("Saida_tm/Textos_", titulo, ".txt"),
          sep = "\t", row.names = FALSE, fileEncoding = "UTF-8")
}
## Fim FUNÇÃO NuvemPalavras

## FUNÇÃO Comparar2nuvens compara os termos de dois corpus apresentando-os em duas nuvens de
palavras
# uma nuvem de termos divergentes e uma nuvem de termos comuns.
Comparar2nuvens<-function(frags1,frags2,titulo1,titulo2,vPalVacias,cor1,cor2,corc,maxPalavras,raiz){
 # frags1 e frags2   Datraframe: Fragmentos de texto para comparar nuvens
 # titulo1 e titulo2 Títulos dos corpus para comparar
 # vPalVacias       Vector: Palavras pouco significativas específicas para esta análise
 # cor1 e cor2      Paletas de cores para os gráficos de palavras diferentes
 # corc             Paleta de cores para o gráfico de palavras comuns
 # maxPalavras      Número máximo de palavras a representar nos gráficos
 # raiz             Boolean: se TRUE lematiza as palavras agrupando as de raiz comum

 # Caso algum corpus esteja vazio terminar
 numFrags1<-length(frags1[frags1!=""])
 cat( numFrags1," fragmentos de texto no corpus ",titulo1, "\r\n") # Ecrã: Número de fragmentos no
```

```
corpus 1
 numFrags2<-length(frags2[frags2!=""])
 cat( numFrags2," fragmentos de texto no corpus ",titulo2, "\r\n") # Ecrã: Número de fragmentos no
corpus 2
 if ((numFrags1==0) | (numFrags2==0)){
  png(paste0("Saida_tm/Compara_",titulo1,"_vs_",titulo2,".png"), width = 400, height = 400, units = "px")
  layout(matrix(c(1,2), nrow=2), heights=c(4,8))
  par(mar=c(0,0,0,0))
  plot.new()
  text(x=0.5, y=0.5, paste0(titulo1, " vs ", titulo2,"\r\n ", numFrags1," fragmentos vs ",numFrags2,"
fragmentos",
                    "\r\n \r\n COMPARAÇO IMPROPRIA"), cex=1.4, font= 4, col.main= "darkgrey")
  dev.off()
  return()
 }
 # Criar o corpus de dois documentos em inglês. Cada documento será um corpus de entrada colapsado:
 d1 <- paste(unlist(frags1), collapse =" ") # colapsar os fragmentos de texto num texto único
 d2 <- paste(unlist(frags2), collapse =" ")
 corpus <- Corpus(VectorSource(c(d1,d2)))
 # Limpar e preparar o corpus documental:
 corpus <- LimparCorpus(corpus)
 corpus <- tm_map(corpus, removeWords,vPalVacias) # eliminar as palavras contidas em vPalVacias
 if (raiz==T) {corpus <- tm_map(corpus,stemDocument)} # lematizar: agrupar flexões gramaticais da
mesma raiz.
 ## Criar as nuvens
 m <- as.matrix(TermDocumentMatrix(corpus))
 colnames(m) = c(titulo1,titulo2)
 m1<-data.frame(m[,1])
 m2<-data.frame(m[,2])
 png(paste0("Saida_tm/Compara_",titulo1,"_vs_",titulo2,".png"), width = 600, height = 450, units = "px")
  layout(matrix(c(1,1,2,3), nrow=2, byrow=T), heights=c(4,14), widths=c(25,25))
  par(mar=c(0,0,0,0))
  plot.new()
  text(x=0.5, y=0.5, paste0(titulo1, "  vs  ", titulo2,"\r\n ", "Fragmentos codificados: ", numFrags1,"  /
",numFrags2,
                    "  \r\n  "," Termos: ", length(m1[m1!=0]), "  /  ", length(m2[m2!=0]),"  \r\n \r\n ",
                    "Termos divergentes:                                    Termos comuns:"),
     font= 4, cex=1.2, col.main= "darkgrey")
  #diferencias
  comparison.cloud(m, colors=c(cor1,cor2), max.words=maxPalavras, random.order=FALSE, title.size=1.4,
scale=c(3.4,0.5))
  #coincidências
  commonality.cloud(m, color=corc, random.order=FALSE,scale=c(4,1), max.words=maxPalavras+5)
  dev.off()
}
## Fim FUNÇÃO Comparar2nuvens


## FUNÇÃO Comparar3nuvens compara os termos de três corpus apresentando-os em duas nuvens de
palavras
```

```
# uma nuvem de termos divergentes e uma nuvem de termos comuns.
Comparar3nuvens<-
function(frags1,frags2,frags3,titulo1,titulo2,titulo3,vPalVacias,cor1,cor2,cor3,corc,maxPalavras,raiz){
 # frags1,frags2 e frags3   Datraframe: Fragmentos de texto para comparar nuvens
 # titulo1,titulo2 e titulo3 Títulos dos corpus para comparar
 # vPalVacias              Vector: Palavras pouco significativas específicas para esta análise
 # cor1,cor2 e cor3        Paletas de cores para os gráfico de palavras diferentes
 # corc           Paleta de cores para o gráfico de palavras comuns
 # maxPalavras      Número máximo de palavras a representar nos gráficos
 # raiz           Boolean: se TRUE lematiza as palavras agrupando as de raiz comum

 # Caso algum corpus esteja vazio terminar
 numFrags1<-length(frags1[frags1!=""])
 cat( numFrags1," fragmentos de texto no corpus ",titulo1, "\r\n") # Ecrã: Número de fragmentos no
corpus 1
 numFrags2<-length(frags2[frags2!=""])
 cat( numFrags2," fragmentos de texto no corpus ",titulo2, "\r\n") # Ecrã: Número de fragmentos no
corpus 2
 numFrags3<-length(frags3[frags3!=""])
 cat( numFrags3," fragmentos de texto no corpus ",titulo3, "\r\n") # Ecrã: Número de fragmentos no
corpus 3
 if ((numFrags1==0) | (numFrags2==0)| (numFrags3==0)){
  png(paste0("Saida_tm/Compara_",titulo1,"_vs_",titulo2,"_vs_",titulo3,".png"),
    width = 400, height = 400, units = "px")
   layout(matrix(c(1,2), nrow=2), heights=c(4,8))
   par(mar=c(0,0,0,0))
   plot.new()
   text(x=0.5, y=0.5, paste0(titulo1, " vs ", titulo2," vs ", titulo3,"\r\n ", "Fragmentos: ",numFrags1," / ",
                numFrags2," / ",numFrags3,"\r\n \r\n COMPARAÇO IMPROPRIA"), cex=1.4, font= 4,
col.main= "darkgrey")
  dev.off()
  return()
 }
 # Criar o corpus de dois documentos em inglês. Cada documento será um corpus de entrada colapsado:
 d1 <- paste(unlist(frags1), collapse =" ") # colapsar os fragmentos de texto num texto único
 d2 <- paste(unlist(frags2), collapse =" ")
 d3 <- paste(unlist(frags3), collapse =" ")
 corpus <- Corpus(VectorSource(c(d1,d2,d3)))
 # Limpar e preparar o corpus documental:
 corpus <- LimparCorpus(corpus)
 corpus <- tm_map(corpus, removeWords,vPalVacias) # eliminar as palavras contidas em vPalVacias
 if (raiz==T) {corpus <- tm_map(corpus,stemDocument)} # lematizar: agrupar flexões gramaticais da
mesma raiz.
 ## Criar as nuvens
 m <- as.matrix(TermDocumentMatrix(corpus))
 colnames(m) = c(titulo1,titulo2,titulo3)
 m1<-data.frame(m[,1])
 m2<-data.frame(m[,2])
 m3<-data.frame(m[,3])
 png(paste0("Saida_tm/Compara_",titulo1,"_vs_",titulo2,"_vs_",titulo3,".png"),
```

```
    width = 600, height = 450, units = "px")
  layout(matrix(c(1,1,2,3), nrow=2, byrow=T), heights=c(4,14), widths=c(25,25))
  par(mar=c(0,0,0,0))
  plot.new()
  text(x=0.5, y=0.5, paste0(titulo1, " vs ", titulo2," vs ", titulo3,"\r\n ", "Fragmentos: ",numFrags1," / ",
                    numFrags2," / ",numFrags3," \r\n  ", " Termos:  ", length(m1[m1!=0]),
                   "  /  ", length(m2[m2!=0]),"  /  ", length(m3[m3!=0]), "  \r\n \r\n ",
                   "Termos divergentes:                                    Termos comuns:"),
    font= 4, cex=1.2, col.main= "darkgrey")
  #termos divergentes
  comparison.cloud(m, colors=c(cor1,cor2,cor3), max.words=maxPalavras, random.order=FALSE,
title.size=1.4, scale=c(3.4,0.5))
  #termos comuns
  commonality.cloud(m, color=corc, random.order=FALSE, scale=c(4,1),max.words=maxPalavras+10)
 dev.off()
 #return(m)
}
## Fim FUNÇÃO Comparar3nuvens

## FUNÇÃO Comparar4nuvens compara os termos de quatro corpus apresentando-os em duas nuvens de
palavras
# uma nuven de termos divergentes e uma nuvem de termos comuns.
Comparar4nuvens<-
function(frags1,frags2,frags3,frags4,titulo1,titulo2,titulo3,titulo4,vPalVacias,cor1,cor2,cor3,cor4,corc,max
Palavras,raiz){
 # frags1,... frags4   Datraframe: Fragmentos de texto para comparar nuvens
 # titulo1,...titulo4  Títulos dos corpus para comparar
 # vPalVacias        Vector: Palavras pouco significativas específicas para esta análise
 # cor1,cor2,cor3,cor4 Paletas de cores para os gráfico de palavras diferentes
 # corc              Paleta de cores para o gráfico de palavras comuns
 # maxPalavras       Número máximo de palavras a representar nos gráficos
 # raiz              Boolean: se TRUE lematiza as palavras agrupando as de raiz comum

 # Caso algum corpus esteja vazio terminar
 numFrags1<-length(frags1[frags1!=""])
 cat( numFrags1," fragmentos de texto no corpus ",titulo1, "\r\n") # Ecrã: Número de fragmentos no
corpus 1
 numFrags2<-length(frags2[frags2!=""])
 cat( numFrags2," fragmentos de texto no corpus ",titulo2, "\r\n") # Ecrã: Número de fragmentos no
corpus 2
 numFrags3<-length(frags3[frags3!=""])
 cat( numFrags3," fragmentos de texto no corpus ",titulo3, "\r\n") # Ecrã: Número de fragmentos no
corpus 3
 numFrags4<-length(frags4[frags4!=""])
 cat( numFrags4," fragmentos de texto no corpus ",titulo4, "\r\n") # Ecrã: Número de fragmentos no
corpus 4
 if ((numFrags1==0) | (numFrags2==0)| (numFrags3==0)| (numFrags4==0)){
  png(paste0("Saida_tm/Nuvem_",titulo,".png"), width = 400, height = 400, units = "px")
  layout(matrix(c(1,2), nrow=2), heights=c(4,8))
  par(mar=c(0,0,0,0))
```

```
  plot.new()
  text(x=0.5, y=0.5, paste0(titulo1, " vs ",titulo2," vs ",titulo3,"\r\n ",titulo4,"\r\n ", " Fragmentos: ",
                    numFrags1,"  / ",numFrags2," / ",numFrags3," / ",numFrags4,
                    "\r\n \r\n COMPARAÇO IMPROPRIA"), cex=1.4, font= 4, col.main= "darkgrey")
  dev.off()
  return()
 }
 # Criar o corpus de dois documentos em inglês. Cada documento será um corpus de entrada colapsado:
 d1 <- paste(unlist(frags1), collapse =" ") # colapsar os fragmentos de texto num texto único
 d2 <- paste(unlist(frags2), collapse =" ")
 d3 <- paste(unlist(frags3), collapse =" ")
 d4 <- paste(unlist(frags4), collapse =" ")
 corpus <- Corpus(VectorSource(c(d1,d2,d3,d4)))
 # Limpar e preparar o corpus documental:
 corpus <- LimparCorpus(corpus)
 corpus <- tm_map(corpus, removeWords,vPalVacias) # eliminar as palavras contidas em vPalVacias
 if (raiz==T) {corpus <- tm_map(corpus,stemDocument)} # lematizar: agrupar flexões gramaticais da
mesma raiz.
 ## Criar as nuvens
 m <- as.matrix(TermDocumentMatrix(corpus))
 colnames(m) = c(titulo1,titulo2,titulo3,titulo4)
 m1<-data.frame(m[,1])
 m2<-data.frame(m[,2])
 m3<-data.frame(m[,3])
 m4<-data.frame(m[,4])
 png(paste0("Saida_tm/Compara_",titulo1,"_vs_",titulo2,"_vs_",titulo3,"_vs_",titulo4,".png"),
    width = 800, height = 600, units = "px")
 layout(matrix(c(1,1,2,3), nrow=2, byrow=T), heights=c(4,14), widths=c(25,25))
 par(mar=c(0,0,0,0))
 plot.new()
 text(x=0.5, y=0.5, paste0(titulo1, "  vs  ", titulo2,"  vs  ",titulo3," vs ",titulo4,"\r\n ",
                    " Fragmentos codificados: ", numFrags1, "  /  ",numFrags2,"   /  ",
                    numFrags3,"  /  ",numFrags4,"\r\n  ", "Termos: ", length(m1[m1!=0]), "  /  ",
length(m2[m2!=0]),
                    "   /  ", length(m3[m3!=0]),"   /  ", length(m3[m4!=0])," \r\n \r\n ",
                    "Termos divergentes:                                    Termos comuns:"),
     font= 4, cex=1.2, col.main= "darkgrey")
 #termos divergentes
 comparison.cloud(m, colors=c(cor1,cor2,cor3,cor4), max.words=maxPalavras, random.order=FALSE,
             title.size=1.4, scale=c(3.4,0.5))
 #termos comuns
 commonality.cloud(m, color=corc, random.order=FALSE, scale=c(4,1),max.words=maxPalavras+20)
 dev.off()
 #return(m)
}
## Fim FUNÇÃO Comparar4nuvens



####    CORPO do scrip    ####
```

```
### Abrir o programa RQDA
RQDA()
### Abrir o projeto em RQDA
openProject("TFM_TM_Dissuasao_Codif_Final.rqda", updateGUI = TRUE)
###  Conetar con Base de Dados em RQDA
conRQDA <- dbConnect(RSQLite::SQLite(), "TFM_TM_Dissuasao_Codif_final.rqda")

### Inicialização de variáveis globais
vecPalvrasVacias <- c( "cyber","ignatius", "jens","david","issa", "konstantin","kosachev", "nuland",
                "victoria", "darrell", "stoltenberg", "federica", "mogherini", "rasmussen") # vector de palavras
vacias
vecPalvrasVacias_a <- c("cyber","attack", "attacks", "defence", "nato", "ignatius", "jens","david","issa",
                "konstantin","kosachev", "nuland", "victoria", "darrell", "stoltenberg", "federica" ) # vector de
palavras vacias

### Nuvens de palavras globais
 # Consulta a BD de RQDA:
 dfrFragmentosTotal<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding WHERE status=1")
 # Imprimir a nuvem de palavras num ficheiro .png
 NuvemPalavras(dfrFragmentosTotal$seltext, "Codificação Global", vecPalvrasVacias,
          cores=brewer.pal(name = "YlOrRd", n = 9), maxPalavras=50, minFrec=3, raiz=T)
 ## Nuvem de palavras global Antes TMP
 dfrFragsAntesTMP<-dbGetQuery(conRQDA,
              "SELECT DISTINCT seltext FROM coding, source, treefile, filecat WHERE coding.status=1
              AND coding.fid=source.id AND source.id=treefile.fid AND treefile.catid=filecat.catid
              AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsAntesTMP$seltext, "Dissuasão Antes do TMP", vecPalvrasVacias,
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras global desde o começo do TMP ao TM
 dfrFragsTMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat WHERE coding.status=1
                    AND coding.fid=source.id AND source.id=treefile.fid AND treefile.catid=filecat.catid
                    AND (filecat.name='FC_31dic09_07mar13')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsTMP_TM$seltext, "Codificação Global TMP-TM", vecPalvrasVacias,
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T)# Imprime nuvem
em .png
 ## Nuvem de palavras global desde o TM ao TM2
 dfrFragsTM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat WHERE coding.status=1
                    AND coding.fid=source.id AND source.id=treefile.fid AND treefile.catid=filecat.catid
                    AND (filecat.name='FD_07mar13_08feb17')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsTM_TM2$seltext, "Codificação Global TM-TM2", vecPalvrasVacias,
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T)  # Imprime nuvem
em .png
 ## Nuvem de palavras global desde o TM2 à Cimeira de Bruxelas
 dfrFragsTM2_Brux<-dbGetQuery(conRQDA,
```

```
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat WHERE coding.status=1
                AND coding.fid=source.id AND source.id=treefile.fid AND treefile.catid=filecat.catid
                AND (filecat.name='FE_08feb17_12jul18')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsTM2_Brux$seltext, "Codificação Global TM-Bruxelas", vecPalvrasVacias,
         cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T)  # Imprime
nuvem em .png
 ## Comparar 4 nuvens globais:
 Comparar4nuvens(dfrFragsAntesTMP,dfrFragsTMP_TM,dfrFragsTM_TM2,dfrFragsTM2_Brux,"Antes
TMP","cTMP-TM","TM-TM2",
          "TM2-Bruxelas" ,vecPalvrasVacias,
          "brown4","plum3","darkblue","seagreen","black",60,raiz=T)
 ## Comparar 3 nuvens globais TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsTMP_TM,dfrFragsTM_TM2,dfrFragsTM2_Brux,"cTMP-TM","TM-TM2","TM2-
Bruxelas",vecPalvrasVacias,
          "plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar nuvens globais anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsTM_TM2,dfrFragsTM2_Brux,"TM-TM2","TM2-
Bruxelas",vecPalvrasVacias,"darkblue","seagreen","black"
          ,30,raiz=T)
### nuvens de palavras de Soberania
 ## Nuvem de palavras Soberania antes do TMP
 dfrFragsSob_A_TMP<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid
                AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                AND coding.cid=freecode.id AND freecode.name='Soberania'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsSob_A_TMP$seltext, "Soberanía antes do TMP", vecPalvrasVacias,
         cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=2, raiz=F) # Imprime nuvem
em .png
 ## Nuvem de palavras Soberanía  desde o começo do TMP ao TM
 dfrFragsSob_TMP_TM<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                AND coding.cid=freecode.id AND freecode.name='Soberania'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsSob_TMP_TM$seltext, "Soberania cTMP - TM", vecPalvrasVacias,
         cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Soberanía  desde o TM ao TM2
 dfrFragsSob_TM_TM2<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                AND coding.cid=freecode.id AND freecode.name='Soberania'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsSob_TM_TM2$seltext, "Soberania TM - TM2", vecPalvrasVacias,
         cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Soberanía  desde o TM2 à Cimeira de Bruxelas
 dfrFragsSob_TM2_Brux<-dbGetQuery(conRQDA,
```

```
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                    AND coding.cid=freecode.id AND freecode.name='Soberania'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsSob_TM2_Brux$seltext, "Soberania TM2 - Bruxelas", vecPalvrasVacias,
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ## Comparar 4 nuvens Soberanía:

Comparar4nuvens(dfrFragsSob_A_TMP,dfrFragsSob_TMP_TM,dfrFragsSob_TM_TM2,dfrFragsSob_TM2_B
rux,
          "Soberanía, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas" ,vecPalvrasVacias,
          "brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens Soberanía TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsSob_TMP_TM,dfrFragsSob_TM_TM2,dfrFragsSob_TM2_Brux,"Soberanía,
cTMP-TM","TM-TM2","TM2-Bruxelas",
          vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Soberanía anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsSob_A_TMP,dfrFragsSob_TMP_TM,"Soberanía, anterior_TMP","cTMP-
TM",vecPalvrasVacias,
          "brown4","plum3","black",30,raiz=T)
 ## Comparar 2 nuvens Soberanía anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsSob_TMP_TM,dfrFragsSob_TM_TM2,"Soberanía, cTMP-TM","TM-
TM2",vecPalvrasVacias,
          "plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Soberanía anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsSob_TM_TM2,dfrFragsSob_TM2_Brux,"Soberanía, TM-TM2","TM2-
Bruxelas",vecPalvrasVacias,
          "darkblue","seagreen","black",30,raiz=T)

### nuvens de palavras de Atribuição
 ## Nuvem de palavras Atribuição antes do TMP
 dfrFragsAtr_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                    AND coding.cid=freecode.id AND freecode.name='Atribuição'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsAtr_A_TMP$seltext, "Atribuição antes do TMP", vecPalvrasVacias,
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Atribuição  desde o começo do TMP ao TM
 dfrFragsAtr_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                    AND coding.cid=freecode.id AND freecode.name='Atribuição'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsAtr_TMP_TM$seltext, "Atribuição cTMP - TM", vecPalvrasVacias,
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
```

```
em .png
 ## Nuvem de palavras Atribuição  desde o TM ao TM2
 dfrFragsAtr_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id AND freecode.name='Atribuição'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsAtr_TM_TM2$seltext, "Atribuição TM - TM2", vecPalvrasVacias,
         cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Atribuição  desde o TM2 à Cimeira de Bruxelas
 dfrFragsAtr_TM2_Brux<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                    AND coding.cid=freecode.id AND freecode.name='Atribuição'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsAtr_TM2_Brux$seltext, "Atribuição TM2 - Bruxelas", vecPalvrasVacias,
         cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ## Comparar 4 nuvens Atribuição:

Comparar4nuvens(dfrFragsAtr_A_TMP,dfrFragsAtr_TMP_TM,dfrFragsAtr_TM_TM2,dfrFragsAtr_TM2_Bru
x,
         "Atribuição, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas" ,vecPalvrasVacias,
         "brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens Atribuição TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsAtr_TMP_TM,dfrFragsAtr_TM_TM2,dfrFragsAtr_TM2_Brux,"Atribuição,
cTMP-TM","TM-TM2","TM2-Bruxelas",
         vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Atribuição anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsAtr_A_TMP,dfrFragsAtr_TMP_TM,"Atribuição, anterior_TMP","cTMP-
TM",vecPalvrasVacias,
         "brown4","plum3","black",30,raiz=T)
 ## Comparar 2 nuvens Atribuição anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsAtr_TMP_TM,dfrFragsAtr_TM_TM2,"Atribuição, cTMP-TM","TM-
TM2",vecPalvrasVacias,
         "plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Atribuição anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsAtr_TM_TM2,dfrFragsAtr_TM2_Brux,"Atribuição, TM-TM2","TM2-
Bruxelas",vecPalvrasVacias,
         "darkblue","seagreen","black",30,raiz=T)

 ### nuvens de palavras de Capacidade
 ## Nuvem de palavras Capacidade antes do TMP
 dfrFragsCap_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
```

```
                    AND coding.cid=freecode.id AND freecode.name='Capacidade'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCap_A_TMP$seltext, "Capacidade antes do TMP", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Capacidade  desde o começo do TMP ao TM
 dfrFragsCap_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                    AND coding.cid=freecode.id AND freecode.name='Capacidade'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCap_TMP_TM$seltext, "Capacidade cTMP - TM", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Capacidade  desde o TM ao TM2
 dfrFragsCap_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id AND freecode.name='Capacidade'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCap_TM_TM2$seltext, "Capacidade TM - TM2", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Capacidade  desde o TM2 à Cimeira de Bruxelas
 dfrFragsCap_TM2_Brux<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                     coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                     AND coding.cid=freecode.id AND freecode.name='Capacidade'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCap_TM2_Brux$seltext, "Capacidade TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Comparar 4 nuvens Capacidade:

Comparar4nuvens(dfrFragsCap_A_TMP,dfrFragsCap_TMP_TM,dfrFragsCap_TM_TM2,dfrFragsCap_TM2_B
rux,
          "Capacidade, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas" ,vecPalvrasVacias,
          "brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens Capacidade TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsCap_TMP_TM,dfrFragsCap_TM_TM2,dfrFragsCap_TM2_Brux,"Capacidade,
cTMP-TM","TM-TM2","TM2-Bruxelas",
          vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Capacidade anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsCap_A_TMP,dfrFragsCap_TMP_TM,"Capacidade, anterior_TMP","cTMP-
TM",vecPalvrasVacias,
          "brown4","plum3","black",30,raiz=T)
 ## Comparar 2 nuvens Capacidade anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsCap_TMP_TM,dfrFragsCap_TM_TM2,"Capacidade, cTMP-TM","TM-
TM2",vecPalvrasVacias,
          "plum3","darkblue","black",30,raiz=T)
```

```
## Comparar 2 nuvens Capacidade anterior e posterior ao TM2:
Comparar2nuvens(dfrFragsCap_TM_TM2,dfrFragsCap_TM2_Brux,"Capacidade, TM-TM2","TM2-
Bruxelas",vecPalvrasVacias,
          "darkblue","seagreen","black",30,raiz=T)

### nuvens de palavras de Ambiguidade
## Nuvem de palavras Ambiguidade antes do TMP
dfrFragsAmb_A_TMP<-dbGetQuery(conRQDA,
                  "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                  coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                  AND treefile.catid=filecat.catid
                  AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                  AND coding.cid=freecode.id AND freecode.name='Ambiguidade'") # Consulta BD RQDA
NuvemPalavras(dfrFragsAmb_A_TMP$seltext, "Ambiguidade antes do TMP", c(vecPalvrasVacias, "nato"),
        cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
## Nuvem de palavras Ambiguidade  desde o começo do TMP ao TM
dfrFragsAmb_TMP_TM<-dbGetQuery(conRQDA,
                  "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                  coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                  AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                  AND coding.cid=freecode.id AND freecode.name='Ambiguidade'") # Consulta BD RQDA
NuvemPalavras(dfrFragsAmb_TMP_TM$seltext, "Ambiguidade cTMP - TM", c(vecPalvrasVacias, "nato"),
        cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
## Nuvem de palavras Ambiguidade  desde o TM ao TM2
dfrFragsAmb_TM_TM2<-dbGetQuery(conRQDA,
                  "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                  coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                  AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                  AND coding.cid=freecode.id AND freecode.name='Ambiguidade'") # Consulta BD RQDA
NuvemPalavras(dfrFragsAmb_TM_TM2$seltext, "Ambiguidade TM - TM2", c(vecPalvrasVacias, "nato"),
        cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
## Nuvem de palavras Ambiguidade  desde o o TM2 à Cimeira de Bruxelas
dfrFragsAmb_TM2_Brux<-dbGetQuery(conRQDA,
                   "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                   coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                   AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                   AND coding.cid=freecode.id AND freecode.name='Ambiguidade'") # Consulta BD RQDA
NuvemPalavras(dfrFragsAmb_TM2_Brux$seltext, "Ambiguidade TM2 - Bruxelas", c(vecPalvrasVacias,
"nato"),
        cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
## Comparar 4 nuvens Ambiguidade:

Comparar4nuvens(dfrFragsAmb_A_TMP,dfrFragsAmb_TMP_TM,dfrFragsAmb_TM_TM2,dfrFragsAmb_TM
2_Brux,
          "Ambiguidade, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas" ,vecPalvrasVacias,
          "brown4","plum3","darkblue","seagreen","black",50,raiz=T)
```

```
 ## Comparar 3 nuvens Ambiguidade TMP-TM-TM2-Bruxelas:

Comparar3nuvens(dfrFragsAmb_TMP_TM,dfrFragsAmb_TM_TM2,dfrFragsAmb_TM2_Brux,"Ambiguidade, cTMP-TM","TM-TM2","TM2-Bruxelas",
          vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Ambiguidade anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsAmb_A_TMP,dfrFragsAmb_TMP_TM,"Ambiguidade, anterior_TMP","cTMP-TM",vecPalvrasVacias,
          "brown4","plum3","black",30,raiz=T)
 ## Comparar 2 nuvens Ambiguidade anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsAmb_TMP_TM,dfrFragsAmb_TM_TM2,"Ambiguidade, cTMP-TM","TM-TM2",vecPalvrasVacias,
          "plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Ambiguidade anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsAmb_TM_TM2,dfrFragsAmb_TM2_Brux,"Ambiguidade, TM-TM2","TM2-Bruxelas",vecPalvrasVacias,
          "darkblue","seagreen","black",30,raiz=T)

### nuvens de palavras de Cooperação
 ## Nuvem de palavras Cooperação antes do TMP
 dfrFragsCoo_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                    AND coding.cid=freecode.id AND freecode.name='Cooperação'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCoo_A_TMP$seltext, "Cooperação antes do TMP", c(vecPalvrasVacias,"nato"),
         cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem em .png
 ## Nuvem de palavras Cooperação  desde o começo do TMP ao TM
 dfrFragsCoo_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                    AND coding.cid=freecode.id AND freecode.name='Cooperação'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCoo_TMP_TM$seltext, "Cooperação cTMP - TM", c(vecPalvrasVacias,"nato"),
         cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem em .png
## Nuvem de palavras Cooperação  desde o TM ao TM2
 dfrFragsCoo_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id AND freecode.name='Cooperação'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCoo_TM_TM2$seltext, "Cooperação TM - TM2", c(vecPalvrasVacias,"nato"),
         cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem em .png
## Nuvem de palavras Cooperação  desde  o TM2 à Cimeira de Bruxelas
 dfrFragsCoo_TM2_Brux<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
```

```
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                    AND coding.cid=freecode.id AND freecode.name='Cooperação'") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCoo_TM2_Brux$seltext, "Cooperação TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Comparar 4 nuvens Cooperação:

Comparar4nuvens(dfrFragsCoo_A_TMP,dfrFragsCoo_TMP_TM,dfrFragsCoo_TM_TM2,dfrFragsCoo_TM2_
Brux,
          "Cooperação, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas" ,vecPalvrasVacias,
          "brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens Cooperação TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsCoo_TMP_TM,dfrFragsCoo_TM_TM2,dfrFragsCoo_TM2_Brux,"Cooperação,
cTMP-TM","TM-TM2","TM2-Bruxelas",
          vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Cooperação anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsCoo_A_TMP,dfrFragsCoo_TMP_TM,"Cooperação, anterior_TMP","cTMP-
TM",vecPalvrasVacias,
          "brown4","plum3", "black",30,raiz=T)
 ## Comparar 2 nuvens Cooperação anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsCoo_TMP_TM,dfrFragsCoo_TM_TM2,"Cooperação, cTMP-TM","TM-
TM2",vecPalvrasVacias,
          "plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Cooperação anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsCoo_TM_TM2,dfrFragsCoo_TM2_Brux,"Cooperação, TM-TM2","TM2-
Bruxelas",vecPalvrasVacias,
          "darkblue","seagreen","black",30,raiz=T)


### nuvens de palavras de Comunicação e Sinalização
 ## Nuvem de palavras Comunicação e Sinalização antes do TMP
 dfrFragsCS_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                    AND coding.cid=freecode.id
                    AND (freecode.name='Comunicação' OR freecode.name='Sinalização')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCS_A_TMP$seltext, "Comunicação Sinalização pre
TMP",c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação e Sinalização  desde o começo do TMP ao TM
 dfrFragsCS_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
```

```
                    AND coding.cid=freecode.id
                    AND (freecode.name='Comunicação'OR freecode.name='Sinalização')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCS_TMP_TM$seltext, "Comunicação e Sinalização cTMP - TM",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação e Sinalização desde o TM ao TM2
 dfrFragsCS_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id
                    AND (freecode.name='Comunicação'OR freecode.name='Sinalização')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCS_TM_TM2$seltext, "Comunicação e Sinalização TM - TM2",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação e Sinalização desde o TM2 à Cimeira de Bruxelas
 dfrFragsCS_TM2_Brux<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                     coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                     AND coding.cid=freecode.id
                     AND (freecode.name='Comunicação'OR freecode.name='Sinalização')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCS_TM2_Brux$seltext, "Comunicação e Sinalização TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ## Comparar 4 nuvens Comunicação e Sinalização:
 Comparar4nuvens(dfrFragsCS_A_TMP,dfrFragsCS_TMP_TM,dfrFragsCS_TM_TM2,dfrFragsCS_TM2_Brux,
           "Comunicação e Sinalização, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas",
           c(vecPalvrasVacias,"nato"),"brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens Comunicação e Sinalização TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsCS_TMP_TM,dfrFragsCS_TM_TM2,dfrFragsCS_TM2_Brux,"Comunicação e
Sinalização, cTMP-TM",
           "TM-TM2","TM2-Bruxelas", vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Comunicação e Sinalização anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsCS_A_TMP,dfrFragsCS_TMP_TM,"Comunicação e Sinalização,
anterior_TMP","cTMP-TM",
           c(vecPalvrasVacias,"nato"),"brown4","plum3", "black",30,raiz=T)
 ## Comparar 2 nuvens Comunicação e Sinalização anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsCS_TMP_TM,dfrFragsCS_TM_TM2,"Comunicação e Sinalização, cTMP-
TM","TM-TM2",
           c(vecPalvrasVacias,"nato"),"plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Comunicação e Sinalização anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsCS_TM_TM2,dfrFragsCS_TM2_Brux,"Comunicação e Sinalização, TM-
```

```
TM2","TM2-Bruxelas",
          c(vecPalvrasVacias,"nato"),"darkblue","seagreen","black",30,raiz=T)

 ### nuvens de palavras de Comunicação
 ## Nuvem de palavras Comunicação antes do TMP
 dfrFragsCS_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                    AND coding.cid=freecode.id AND (freecode.name='Comunicação')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCS_A_TMP$seltext, "Comunicação pre TMP",c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação  desde o começo do TMP ao TM
 dfrFragsCS_TMP_TM<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                     coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                     AND coding.cid=freecode.id AND (freecode.name='Comunicação')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCS_TMP_TM$seltext, "Comunicação cTMP - TM", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação desde o TM ao TM2
 dfrFragsCS_TM_TM2<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                     coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                     AND coding.cid=freecode.id AND (freecode.name='Comunicação')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCS_TM_TM2$seltext, "Comunicação TM - TM2", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação desde o TM2 à Cimeira de Bruxelas
 dfrFragsCS_TM2_Brux<-dbGetQuery(conRQDA,
                      "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                      coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                      AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                      AND coding.cid=freecode.id
                      AND (freecode.name='Comunicação')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsCS_TM2_Brux$seltext, "Comunicação TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ### nuvens de palavras de Comunicação da capacidade
 ## Nuvem de palavras Comunicação da capacidade antes do TMP
 dfrFragsCC_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
```

```
                AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                AND coding.cid=freecode.id AND (freecode.name='Com.Capacidade')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCC_A_TMP$seltext, "Comunicação da capacidade pre
TMP",c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação da capacidade  desde o começo do TMP ao TM
 dfrFragsCC_TMP_TM<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                AND coding.cid=freecode.id AND (freecode.name='Com.Capacidade')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCC_TMP_TM$seltext, "Comunicação da capacidade cTMP - TM",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação da capacidade desde o TM ao TM2
 dfrFragsCC_TM_TM2<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                AND coding.cid=freecode.id AND (freecode.name='Com.Capacidade')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCC_TM_TM2$seltext, "Comunicação da capacidade TM - TM2",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação da capacidade desde o TM2 à Cimeira de Bruxelas
 dfrFragsCC_TM2_Brux<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                AND coding.cid=freecode.id AND (freecode.name='Com.Capacidade')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCC_TM2_Brux$seltext, "Comunicação da capacidade TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ### nuvens de palavras de Comunicação da Determinação
 ## Nuvem de palavras Comunicação da Determinação antes do TMP
 dfrFragsCD_A_TMP<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid
                AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                AND coding.cid=freecode.id AND (freecode.name='Com.Determinaçao')") # Consulta BD
RQDA
```

```
 NuvemPalavras(dfrFragsCD_A_TMP$seltext, "Comunicação da Determinação pre
TMP",c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação da Determinação  desde o começo do TMP ao TM
 dfrFragsCD_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                    AND coding.cid=freecode.id AND (freecode.name='Com.Determinaçao')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCD_TMP_TM$seltext, "Comunicação da Determinação cTMP - TM",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação da Determinação desde o TM ao TM2
 dfrFragsCD_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id AND (freecode.name='Com.Determinaçao')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsCD_TM_TM2$seltext, "Comunicação da Determinação TM - TM2",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Comunicação da Determinação desde o TM2 à Cimeira de Bruxelas
 dfrFragsCD_TM2_Brux<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                     coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                     AND coding.cid=freecode.id AND (freecode.name='Com.Determinaçao')") # Consulta
BD RQDA
 NuvemPalavras(dfrFragsCD_TM2_Brux$seltext, "Comunicação da Determinação TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ### nuvens de palavras de Sinalização
 ## Nuvem de palavras Sinalização antes do TMP
 dfrFragsS_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                    AND coding.cid=freecode.id AND (freecode.name='Sinalização')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsS_A_TMP$seltext, "Sinalização pre TMP",c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=0, raiz=T) # Imprime nuvem
em .png
minFrec=3
```

```
wordcloud(dfrFragsS_A_TMP$seltext, max.words = 50, min.freq=minFrec, random.order = F)
 ## Nuvem de palavras Sinalização  desde o começo do TMP ao TM
 dfrFragsS_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                    AND coding.cid=freecode.id AND (freecode.name='Sinalização')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsS_TMP_TM$seltext, "Sinalização cTMP - TM", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ## Nuvem de palavras Sinalização desde o TM ao TM2
 dfrFragsS_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id AND (freecode.name='Sinalização')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsS_TM_TM2$seltext, "Sinalização TM - TM2", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Sinalização desde o TM2 à Cimeira de Bruxelas
 dfrFragsS_TM2_Brux<-dbGetQuery(conRQDA,
                     "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                     coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                     AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                     AND coding.cid=freecode.id
                     AND (freecode.name='Sinalização')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsS_TM2_Brux$seltext, "Sinalização TM2 - Bruxelas", c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Comparar 4 nuvens  Sinalização:
 Comparar4nuvens(dfrFragsS_A_TMP,dfrFragsS_TMP_TM,dfrFragsS_TM_TM2,dfrFragsS_TM2_Brux,
           "Sinalização, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas",
           c(vecPalvrasVacias,"nato"),"brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens  Sinalização TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsS_TMP_TM,dfrFragsS_TM_TM2,dfrFragsS_TM2_Brux,"Sinalização, cTMP-TM",
           "TM-TM2","TM2-Bruxelas", vecPalvrasVacias,"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Sinalização anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsS_A_TMP,dfrFragsS_TMP_TM,"Sinalização, anterior_TMP","cTMP-TM",
           c(vecPalvrasVacias,"nato"),"brown4","plum3", "black",30,raiz=T)
 ## Comparar 2 nuvens Sinalização anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsS_TMP_TM,dfrFragsS_TM_TM2,"Sinalização, cTMP-TM","TM-TM2",
           c(vecPalvrasVacias,"nato"),"plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Sinalização anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsS_TM_TM2,dfrFragsS_TM2_Brux,"Sinalização, TM-TM2","TM2-Bruxelas",
           c(vecPalvrasVacias,"nato"),"darkblue","seagreen","black",30,raiz=T)

### nuvens de palavras de Dissuasão Punitiva
 ## Nuvem de palavras Dissuasão Punitiva antes do TMP
 dfrFragsDP_A_TMP<-dbGetQuery(conRQDA,
```

```
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid
                AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                AND coding.cid=freecode.id AND (freecode.name='Diss.Punitiva')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsDP_A_TMP$seltext, "Dissuasão Punitiva pre TMP",c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=0, raiz=T) # Imprime nuvem
em .png

 ## Nuvem de palavras Dissuasão Punitiva  desde o começo do TMP ao TM
 dfrFragsDP_TMP_TM<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                AND coding.cid=freecode.id AND (freecode.name='Diss.Punitiva')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsDP_TMP_TM$seltext, "Dissuasão Punitiva cTMP - TM",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png

 ## Nuvem de palavras Dissuasão Punitiva desde o TM ao TM2
 dfrFragsDP_TM_TM2<-dbGetQuery(conRQDA,
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                AND coding.cid=freecode.id AND (freecode.name='Diss.Punitiva')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsDP_TM_TM2$seltext, "Dissuasão Punitiva TM - TM2",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Dissuasão Punitiva desde o TM2 à Cimeira de Bruxelas
 dfrFragsDP_TM2_Brux<-dbGetQuery(conRQDA,
                 "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                 coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                 AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                 AND coding.cid=freecode.id
                 AND (freecode.name='Diss.Punitiva')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsDP_TM2_Brux$seltext, "Dissuasão Punitiva TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Comparar 4 nuvens  Dissuasão Punitiva:

Comparar4nuvens(dfrFragsDP_A_TMP,dfrFragsDP_TMP_TM,dfrFragsDP_TM_TM2,dfrFragsDP_TM2_Brux,
          "Dissuasão Punitiva, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas",
          c(vecPalvrasVacias,"nato"),"brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens  Dissuasão Punitiva TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsDP_TMP_TM,dfrFragsDP_TM_TM2,dfrFragsDP_TM2_Brux,"Dissuasão
Punitiva, cTMP-TM",
          "TM-TM2","TM2-Bruxelas",
```

```
c(vecPalvrasVacias,"nato"),"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Dissuasão Punitiva anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsDP_A_TMP,dfrFragsDP_TMP_TM,"Dissuasão Punitiva, anterior_TMP","cTMP-
TM",
          c(vecPalvrasVacias,"nato"),"brown4","plum3", "black",30,raiz=T)
 ## Comparar 2 nuvens Dissuasão Punitiva anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsDP_TMP_TM,dfrFragsDP_TM_TM2,"Dissuasão Punitiva, cTMP-TM","TM-
TM2",
          c(vecPalvrasVacias,"nato"),"plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Dissuasão Punitiva anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsDP_TM_TM2,dfrFragsDP_TM2_Brux,"Dissuasão Punitiva, TM-TM2","TM2-
Bruxelas",
          c(vecPalvrasVacias,"nato"),"darkblue","seagreen","black",30,raiz=T)

 ### nuvens de palavras de Dissuasão Defensiva
 ## Nuvem de palavras Dissuasão Defensiva antes do TMP
 dfrFragsDD_A_TMP<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid
                    AND (filecat.name='FA_a_19may07' OR filecat.name='FB_19may07_31dic09')
                    AND coding.cid=freecode.id AND (freecode.name='Diss.Defensiva')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsDD_A_TMP$seltext, "Dissuasão Defensiva pre TMP",c(vecPalvrasVacias,"nato"),
        cores=brewer.pal(name = "YlOrBr", n = 9), maxPalavras=50, minFrec=0, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Dissuasão Defensiva  desde o começo do TMP ao TM
 dfrFragsDD_TMP_TM<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FC_31dic09_07mar13')
                    AND coding.cid=freecode.id AND (freecode.name='Diss.Defensiva')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsDD_TMP_TM$seltext, "Dissuasão Defensiva cTMP - TM",
c(vecPalvrasVacias,"nato"),
        cores=brewer.pal(name = "Purples", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Dissuasão Defensiva desde o TM ao TM2
 dfrFragsDD_TM_TM2<-dbGetQuery(conRQDA,
                    "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                    coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                    AND treefile.catid=filecat.catid AND (filecat.name='FD_07mar13_08feb17')
                    AND coding.cid=freecode.id AND (freecode.name='Diss.Defensiva')") # Consulta BD
RQDA
 NuvemPalavras(dfrFragsDD_TM_TM2$seltext, "Dissuasão Defensiva TM - TM2",
c(vecPalvrasVacias,"nato"),
        cores=brewer.pal(name = "Blues", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Nuvem de palavras Dissuasão Defensiva desde o TM2 à Cimeira de Bruxelas
 dfrFragsDD_TM2_Brux<-dbGetQuery(conRQDA,
```

```
                "SELECT DISTINCT seltext FROM coding, source, treefile, filecat, freecode WHERE
                coding.status=1 AND coding.fid=source.id AND source.id=treefile.fid
                AND treefile.catid=filecat.catid AND (filecat.name='FE_08feb17_12jul18')
                AND coding.cid=freecode.id
                AND (freecode.name='Diss.Defensiva')") # Consulta BD RQDA
 NuvemPalavras(dfrFragsDD_TM2_Brux$seltext, "Dissuasão Defensiva TM2 - Bruxelas",
c(vecPalvrasVacias,"nato"),
          cores=brewer.pal(name = "Greens", n = 9), maxPalavras=50, minFrec=3, raiz=T) # Imprime nuvem
em .png
 ## Comparar 4 nuvens  Dissuasão Defensiva:

Comparar4nuvens(dfrFragsDD_A_TMP,dfrFragsDD_TMP_TM,dfrFragsDD_TM_TM2,dfrFragsDD_TM2_Brux
,
          "Dissuasão Defensiva, anterior_TMP","cTMP-TM","TM-TM2","TM2-Bruxelas",
          c(vecPalvrasVacias,"nato"),"brown4","plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 3 nuvens  Dissuasão Defensiva TMP-TM-TM2-Bruxelas:
 Comparar3nuvens(dfrFragsDD_TMP_TM,dfrFragsDD_TM_TM2,dfrFragsDD_TM2_Brux,"Dissuasão
Defensiva, cTMP-TM",
          "TM-TM2","TM2-Bruxelas",
c(vecPalvrasVacias,"nato"),"plum3","darkblue","seagreen","black",50,raiz=T)
 ## Comparar 2 nuvens Dissuasão Defensiva anterior e posterior ao TMP:
 Comparar2nuvens(dfrFragsDD_A_TMP,dfrFragsDD_TMP_TM,"Dissuasão Defensiva,
anterior_TMP","cTMP-TM",
          c(vecPalvrasVacias,"nato"),"brown4","plum3", "black",30,raiz=T)
 ## Comparar 2 nuvens Dissuasão Defensiva anterior e posterior ao TM:
 Comparar2nuvens(dfrFragsDD_TMP_TM,dfrFragsDD_TM_TM2,"Dissuasão Defensiva, cTMP-TM","TM-
TM2",
          c(vecPalvrasVacias,"nato"),"plum3","darkblue","black",30,raiz=T)
 ## Comparar 2 nuvens Dissuasão Defensiva anterior e posterior ao TM2:
 Comparar2nuvens(dfrFragsDD_TM_TM2,dfrFragsDD_TM2_Brux,"Dissuasão Defensiva, TM-TM2","TM2-
Bruxelas",
          c(vecPalvrasVacias,"nato"),"darkblue","seagreen","black",30,raiz=T)

### Fechar a conexão com a BD em RQDA
dbDisconnect(conRQDA)
#### Fim do corpo do script
```