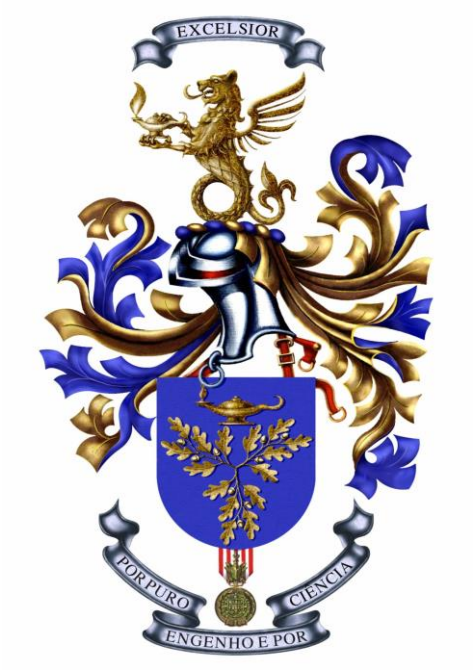
INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO PROMOÇÃO A OFICIAL SUPERIOR

2016/2017



TII

A APLICABILIDADE DO DIREITO DOS CONFLITOS ARMADOS À CIBERGUERRA. O POSICIONAMENTO DA OTAN NO MANUAL DE TALIN.

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

Bruno José de Sá Vaz

Primeiro-tenente

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A APLICABILIDADE DO DIREITO DOS CONFLITOS ARMADOS À CIBERGUERRA. O POSICIONAMENTO DA OTAN NO MANUAL DE TALIN.

1TEN M Bruno José de Sá Vaz

Trabalho de Investigação Individual do CPOS 2016/17

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A APLICABILIDADE DO DIREITO DOS CONFLITOS ARMADOS À CIBERGUERRA. O POSICIONAMENTO DA OTAN NO MANUAL DE TALIN.

1TEN M Bruno José de Sá Vaz

Trabalho de Investigação Individual do CPOS 2016/17

Orientador: Capitão-tenente TSN-JUR Ernestina Maria Santos Silva

Coorientador: Capitão-de-fragata EN-AEL Sérgio Miguel Raminhos Carrilho da Silva Pinto

Pedrouços 2017

Declaração de compromisso Anti plágio

Eu, **Bruno José de Sá Vaz**, declaro por minha honra que o documento intitulado **A APLICABILIDADE DO DIREITO DOS CONFLITOS ARMADOS À CIBERGUERRA. O POSICIONAMENTO DA OTAN NO MANUAL DE TALIN,** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **CURSO DE PROMOÇÃO A OFICIAL SUPERIOR 2016/2017** 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**, 19** de **junho** de **2017**

Bruno José de Sá Vaz

Agradecimentos

Agradeço à minha orientadora, Capitão-tenente Ernestina Silva, pela camaradagem e pela forma construtiva como orientou e acreditou no meu trabalho, ao longo do percurso da investigação.

Uma palavra de agradecimento ao Capitão-de-fragata Silva Pinto, pelo incentivo e pelo cuidado com que coorientou esta investigação, contribuindo com o seu conhecimento intrínseco da Aliança.

O meu agradecimento a todos os que contribuíram para o produto final deste trabalho, em particular ao Embaixador para a ciberdiplomacia, Luís Barreira de Sousa, ao Vice-almirante Silva Carreira, ao Capitão-tenente Câmara Assunção e à Segundo-tenente Solange Esteves. Gostaria também de agradecer a camaradagem dos oficiais discentes do Curso de Promoção a Oficial Superior da Marinha 2016-2017.

Por último não posso deixar de agradecer à minha família e aos meus amigos, que me apoiaram e incentivaram neste trajeto.

O meu agradecimento especial à Rita, que me acompanhou dedicadamente, sempre incentivando nas horas de maior dúvida.

A todos o meu muito obrigado!

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A Organização do Tratado do Atlântico Norte (OTAN) assenta a sua génese nos valores da liberdade, democracia, e do respeito pelo direito. Este fator, legítima a Aliança, como ator que influência a regulação e governo do ciberespaço.

Em 2014, na cimeira de Gales, os Chefes de Estado e de Governo (CEeG) dos 28 países pertencentes à Aliança, deram mais um passo na evolução da política de ciberdefesa, reconhecendo que o Direito Internacional (DI), incluindo o Direito dos Conflitos Armados (DCA), se aplica ao ciberespaço.

Este trabalho tem como objeto a aplicabilidade do DCA, limitando-se a investigação à análise da evolução da posição da OTAN relativamente à regulação e governação e à aplicabilidade do DCA no ciberespaço.

Como objetivo deste estudo de caso, analisou-se a evolução da posição da OTAN relativamente à aplicabilidade do DCA no ciberespaço, identificando os princípios e normas, explorando essa evolução e analisando os desafios e as razões para adoção do Manual de Talin como modelo doutrinário.

Seguindo o método hipotético-dedutivo, pretende-se demonstrar que existe pertinência em compreender esta problemática, concluindo-se que a política da Aliança é consonante com a premissa expressa no Manual de Talin, que num ciberconflito se aplicará o DCA a um ciberataque.

Palavras-chave

OTAN; Direito dos Conflitos Armados; Manual de Talin; Ciberespaço; Ciberguerra.

Abstract

NATO is based on the values of freedom, democracy, and respect for the international law. This elevation is the factor that legitimizes the Alliance in an attempt to find ways to bridge the absence of regulation and governance in cyberspace.

In September 2014, at the Wales summit, the Heads of State and Government of the 28 countries that belong to NATO, took another step towards the evolution of cyber-defense policy, recognizing that the Law of Armed Conflict (LOAC) applies to cyberspace.

The object of this paper is the applicability of the LOAC, limited to the analysis of the concepts that qualify an attack in the cyberspace as an armed attack.

The purpose of this paper is the applicability of the DCA, with research being limited to analyzing the evolution of NATO's position on regulation and governance and the applicability of DCA in cyberspace.

Following the hypothetical-deductive method, it is tried to demonstrate that there is pertinence in understanding this problematic, concluding that the policy of the Alliance is consonant with the premise expressed in the Tallin Manual, that in a cyberconflict the DCA will apply to a cyberattack.

Keywords

NATO; Law of Armed Conflicts; Tallin Manual; Cyberspace; Cyberwarfare.

Lista de abreviaturas, siglas e acrónimos

A	
AA	Ataque Armado
ABAE	Abordagem Baseada na Avaliação dos Efeitos
AC	Análise de Conteúdo
ACT	*Allied Command for Transformation*
AGONU	Assembleia Geral da Organização das Nações Unidas
ANE	Atores Não-Estaduais
C	
C2	Comando e Controlo
C3B	*Consultation Command and Control Board*
CAN	Conselho do Atlântico Norte
CC	Compromisso para a Ciberdefesa
CCD COE	*Cooperative Cyber Defense Center of Excellence*
CD	Ciberdefesa
CDMB	*Cyber Defence Management Board*
CEeG	Chefes de Estado e de Governo
CERT	*Computer Emergency Response Team*
CESEDEN	*Centro Superior de Estudios de la Defensa Nacional*
COPD	*Comprehensive Operations Planning Directive*
CNO	*Computer Network Operations*
CNU	Carta das Nações Unidas
CPAL	Cyber Prioritized Asset List
CRTI	Capacidades Relacionadas com as Tecnologias de Informação.
CSNU	Conselho de Segurança das Nações Unidas
D	
DCA	Direito dos Conflitos Armados
DDoS	*Distributed Denial of Service*
DI	Direito Internacional
E	
EALEDE	*Escuela de Altos Estudios de la Defensa*
ECDP	*Enhanced Cyber Defence Policy*
EMGFA	Estado Maior General das Forças Armadas
ECO	Estrutura de Comando da OTAN
F	
FFAA	Forças Armadas
FR	Federação Russa
G	
GPG	Grupo de Peritos Governamentais no Campo do Desenvolvimento nas Tecnologias da Informação e das Telecomunicações no Contexto da Segurança Internacional
I	
IDN	Instituto de Defesa Nacional
ISNG	Instituto Superior Naval de Guerra
J	
JISR	*Joint Intelligence, Surveillance and Reconnaissance*
L	
LD	Legítima Defesa
LOAC	*Law of armed conflicts*
M	

MISP	*Malware Information-Sharing Platform*
MNE	Ministério dos Negócios Estrangeiros
MOU	*Memorandum of Understanding*
MNCD2	*Multinational Cyber Defence Capability Development*
MN CD E&T	*Multinational Cyber Defence Education and Training*
MdT	Manual de Talin
N	
NATO	*North Atlantic Treaty Organization*
NCIA	*NATO Communications and Information Agency*
NCIRC	*NATO Computer Incident Response Crisis*
NDPP	*NATO Defence Planning Process*
NICP	*NATO Industry Cyber Partnership*
NMA	*NATO Military Authorities*
O	
OC	Operações no Ciberespaço
OI	Organização Internacional
ONU	Organização das Nações Unidas
OPC	*Operations Policy Committee*
OSCE	Organização para a Segurança e Cooperação na Europa
OTAN	Organização do Tratado do Atlântico Norte
P	
PCD	Política de Ciberdefesa
PDRRD	Prevenção, Deteção, Resiliência, Recuperação e Defesa
POP	Procedimentos de Operação Padrão
R	
ReG	Regulação e Governação
RRT	*Rapid Response Team*
S	
SCO	*Shangai Cooperation Organization*
T	
TAN	Tratado do Atlântico Norte
TIC	Tecnologias de Informação e Comunicações
TIJ	Tribunal Internacional de Justiça
TPI	Tribunal Penal Internacional
TTP	Técnicas, Táticas e Procedimentos
W	
WTC	*World Trade Center*

Introdução.

"O ciberespaço é o campo de batalha do futuro", (Leon Panetta, cit. por Ravindranath, 2014).

Esta afirmação é importante porque, conforme os dados publicados pela Organização das Nações Unidas (ONU) em 2015, 43% da população mundial tem acesso à internet, o que significa que, 3,2 mil milhões de pessoas acedem à rede global (ONU (a), 2015, p.7). A sociedade em geral e a comunidade militar em particular, estão cada vez mais dependentes de serviços e sistemas explorados em paralelo e, em igual medida, vulneráveis a ciberataques.

A ciberguerra[1] não é um conceito facilmente percetível pelo cidadão comum, mas é algo presente na liderança mundial, crescendo a consciência do risco real que esta comporta (Mesic et al., 2010, p.1). A Aliança reconheceu esta ameaça em 2010 ao rever o seu conceito estratégico (OTAN (e), 2010).

Na cimeira de Gales, a Aliança afirmou que o Direito dos Conflitos Armados (DCA) se aplica ao ciberespaço (OTAN (n), 2014, p.15) e, na cimeira de Varsóvia, reconhece o ciberespaço como um domínio operacional, no qual tem de se defender tão eficazmente como faz no ar, no mar e em terra (OTAN (c), 2016).

Este trabalho de investigação final de curso é subordinado ao tema "*A aplicabilidade do Direito dos Conflitos Armados à ciberguerra. A posição da NATO no Manual de Talin*".

Relativamente à aplicação do DCA ao ciberespaço num conflito armado, há lugar a discussão de ideias e divergência de opiniões. Vários têm sido os estudos que versam sobre o enunciado desta investigação, alguns dirigidos por autores conceituados, como o professor Michael N. Schmitt, diretor do projeto do Manual de Talin (MdT). Tão vastas têm sido as opiniões sobre esta matéria que se torna necessário delimitá-la.

Nesta investigação, não se pretende teorizar sobre a relação dos cânones do DI e o ciberespaço, mas antes, identificar os princípios e normas do DCA aplicáveis num ciberconflito, caracterizando as problemáticas da qualificação e atribuição de um ataque armado (AA) e, a relevância destas questões para uma resposta em legítima defesa (LD). Pretende-se compreender o papel da OTAN, a sua política e, analisar os desafios adjacentes à evolução da sua posição perante o ciberespaço. Este trabalho visa ainda

[1] Ver definição no Apêndice B.

explorar os moldes, em que poderá ser invocado o artigo 5.º do Tratado do Atlântico Norte (TAN) após um ciberataque.

Desta forma, considera-se que esta investigação se reveste de atualidade e pertinência, podendo constituir-se num contributo válido para a compreensão do papel da OTAN e evolução da sua posição em matéria da aplicabilidade do DI no ciberespaço e do DCA num ciberconflito. Constando-se um aumento recente de ciberataques e de ingerência no ciberespaço, torna-se relevante para a comunidade militar compreender esta evolução e suas implicações.

Assim, define-se como objeto da investigação a *aplicabilidade do DCA no ciberespaço.*

De uma forma concisa, o objetivo geral (OG) e os objetivos específicos (OE) da investigação, encontram-se descritos na Figura 1.

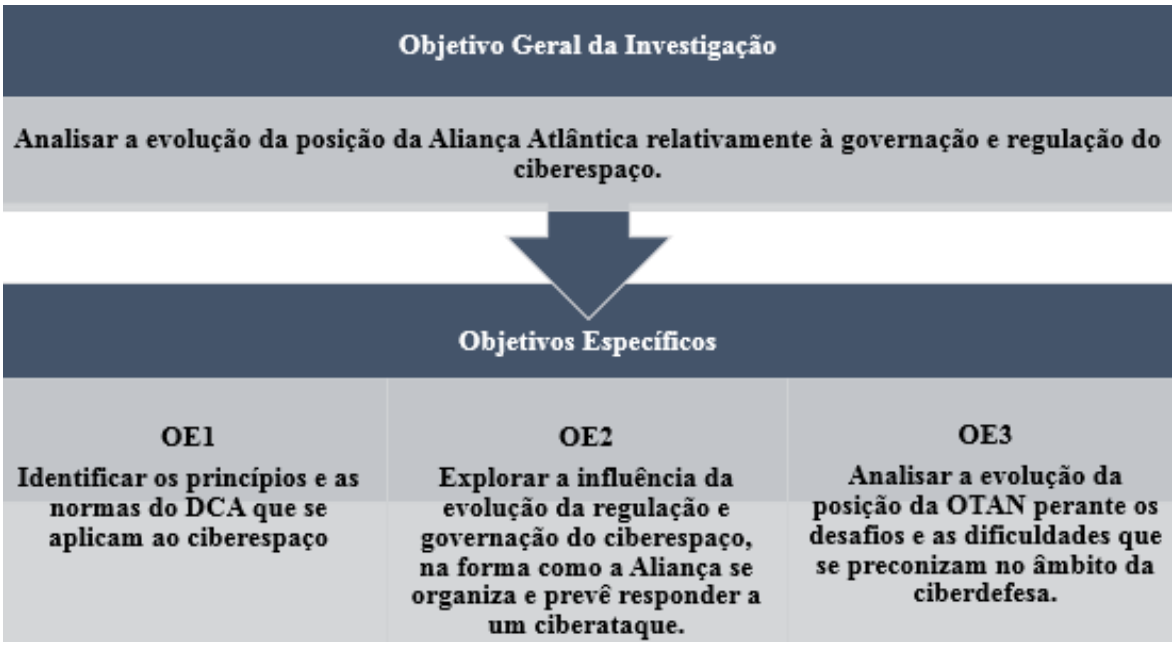


Figura 1 – Objetivo Geral e Objetivos Específicos da Investigação.

Fonte: (O autor, 2017)

Assim, para esta investigação foi definida a seguinte questão central:

Como tem evoluído a posição da Aliança Atlântica, relativamente à aplicabilidade do DCA no ciberespaço?

Considerando a questão central, o OG e os OE definidos, foram identificadas três questões derivadas (QD) às quais se pretende dar resposta com base em três hipóteses (H). Esta conceptualização está patente na Figura 2.

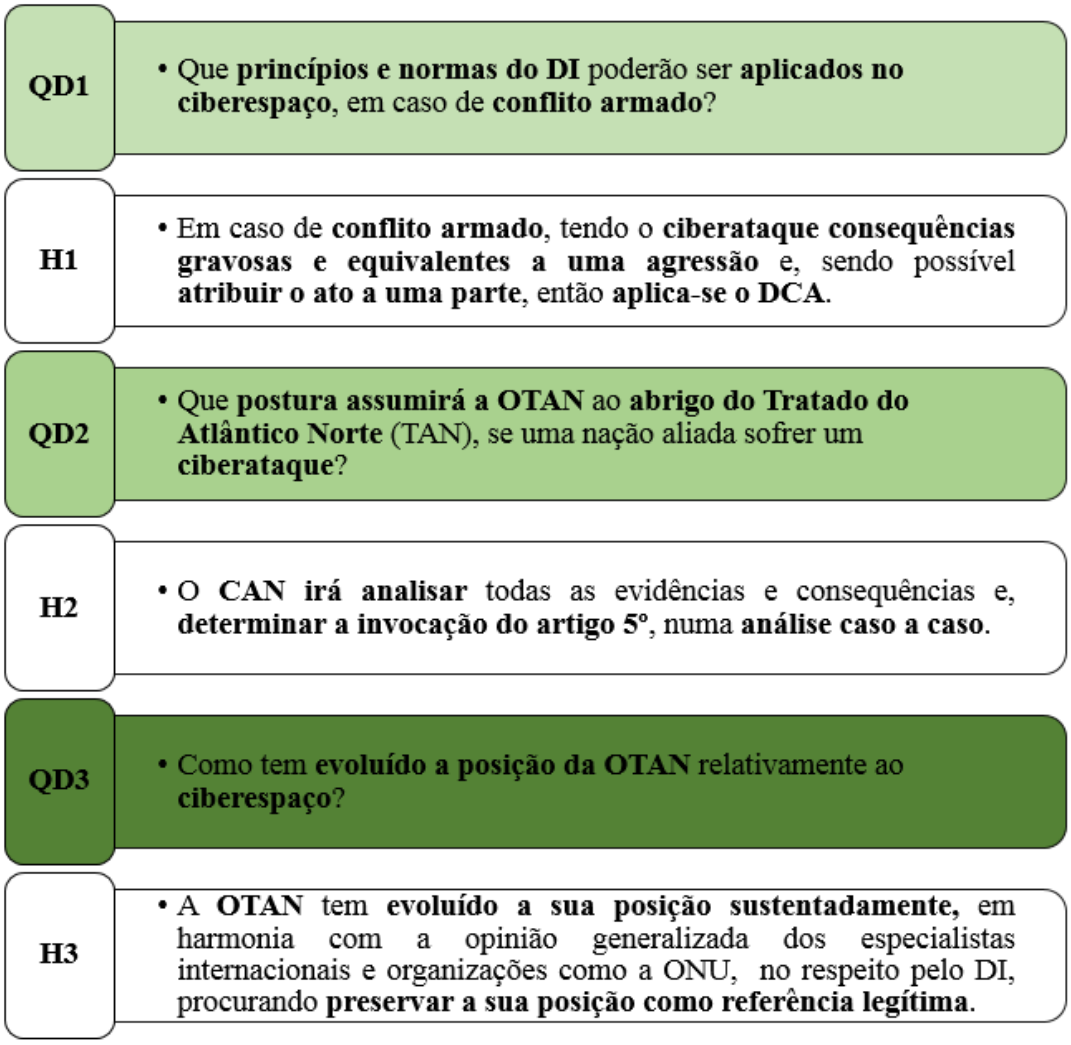


Figura 2 – Questões derivadas e hipóteses

Fonte: (O autor, 2017)

A investigação seguiu uma estratégia qualitativa, sob a forma de estudo de caso, em conformidade com as normas e procedimentos relativos aos trabalhos de investigação do IUM (2013). Neste trabalho, foi seguido o processo metodológico definido por Raymond Quivy e Luc Van Campenhoudt (2005), alicerçando a investigação no método hipotético-dedutivo. Recorreu-se à pesquisa bibliográfica de obras como o MdT, as declarações das cimeiras da OTAN, o Conceito Estratégico da OTAN (2010) e, a vários outros estudos e artigos nacionais e internacionais.

Complementou-se esta pesquisa com quatro entrevistas a detentores de cargos com responsabilidade, experiência prática na área e conhecimento teórico do objeto de estudo, conforme se pode verificar na Tabela 1.

Tabela 1 – Elementos entrevistados.

Cargo	Nome	Organização	Relevância
Embaixador Ciberdiplomacia	Luís Barreira de Sousa	MNE	Representante português e participante nas reuniões do Grupo de Peritos Governamentais no Campo do Desenvolvimento nas Tecnologias da Informação e das Telecomunicações no Contexto da Segurança Internacional (GPG) patrocinado pela Assembleia Geral da ONU (AGONU) .
VALM REF	José Manuel Silva Carreira	Instituto Superior Naval de Guerra (ISNG)	• Ex-Coordenador da Área de Ensino de Estratégia no ISNG; Ex-Docente na Faculdade de Direito de Lisboa e no ISNG; • Ex-Adjunto do Representante nacional junto do Comité Militar e Representante nacional no *Naval Board*, na OTAN, em Bruxelas; • Licenciado em Direito pela Universidade Clássica de Lisboa; • Autor de diversos artigos, entre eles o artigo "O direito humanitário, as regras de empenhamento e a condução das operações militares"
CTEN EN-AEL	Francisco Maria da Câmara Assunção	EMGFA - Direção de Comunicações e Sistemas de Informação	Membro da Estrutura Orgânica do Centro de Ciberdefesa Nacional, adjunto de Marinha para a Ciberdefesa.
Jurista MDN	Solange Patrícia Sousa Esteves	Gabinete do Secretário de Estado da Defesa Nacional	Ex-Jurista na Marinha Portuguesa, participou em vários exercícios de ciberdefesa da OTAN.

Fonte: (O autor, 2017)

Foram aplicadas as regras de apresentação em uso no IUM e foi usada a ferramenta de referenciação automática do *Microsoft Word*® 2016, adotando-se o estilo *Harvard-Anglia* (IESM, 2012).

Quanto à organização da investigação, o trabalho foi dividido em três capítulos. No primeiro capítulo, identificam-se os princípios e as normas do DCA aplicáveis ao ciberespaço, discernem-se os conceitos de *Jus ad Bellum* e de *Jus in Bellum* e, a forma como se relacionam com os conceitos de cibersegurança e ciberdefesa. Também serão abordadas, as questões da qualificação e da atribuição de um ciberataque, tentando estabelecer um modelo de análise baseado nos requisitos definidos no MdT. Por fim, identificam-se as dificuldades na obtenção de informação que permita uma resposta em LD.

No segundo capítulo, abordar-se-ão a organização e princípios da política de ciberdefesa (PCD) da OTAN, os constrangimentos do Conselho do Atlântico Norte (CAN) para proferir uma decisão quanto à invocação do artigo 5.º em caso de ciberataque, a posição de países não-OTAN, e por fim, o Compromisso para a Ciberdefesa (CC).

No terceiro capítulo, analisar-se-ão os desafios que se perspetivam no percurso da Aliança, culminando com uma abordagem ao papel que o MdT assume nos exercícios e

operações da OTAN. A Figura 3 consiste num quadro síntese do plano de trabalho, sendo possível consultar o seu Mapa Concetual no Apêndice A.

ORGANIZAÇÃO DO TRABALHO	OBJETIVOS DA INVESTIGAÇÃO		OBJETO DE ESTUDO	QUESTÃO CENTRAL	QUESTÕES DERIVADAS	HIPÓTESES
CAP 1. O DCA e o Ciberespaço. **1.1.** Princípios e normas do DCA aplicáveis ao ciberespaço. **1.2.** Jus ad Bellum, Jus In Bellum e o Ciberespaço. **1.3.** A qualificação e atribuição do ato. **1.3.1.** A qualificação. **1.3.2.** A atribuição. **1.4.** A questão da legítima defesa. **1.5.** Síntese Conclusiva. *(2598 palavras)*	OBJECTIVO GERAL O objetivo da investigação deste estudo de caso será analisar a evolução da posição da Aliança Atlântica relativamente à governação e regulação do ciberespaço.	**OE1** – Identificar os princípios e as normas do DCA que se aplicam ao ciberespaço.	A aplicabilidade do DCA no ciberespaço.	Como tem evoluído o posicionamento da Aliança Atlântica relativamente à aplicabilidade do DCA no ciberespaço?	**QD1:** Que princípios e normas do Direito Internacional poderão ser aplicados no ciberespaço, em caso de conflito armado?	**H1**: Em caso de conflito armado, tendo o ciberataque consequências gravosas e equivalentes a uma agressão e, sendo possível atribuir o ato a uma parte, então aplica-se o Direito dos Conflitos Armados.
CAP 2. A OTAN, a regulação e governação do ciberespaço. **2.1**. A Política de ciberdefesa. **2.2**. A invocação do artigo 5º do Tratado do Atlântico Norte. **2.3**. A posição de países não-alinhados com a NATO. **2.4.** O Compromisso para a Ciberdefesa. **2.5.** Síntese Conclusiva. *(2068 palavras)*		**OE2** – Caracterizar a influência da evolução da regulação e governação do ciberespaço, na forma como a Aliança se organiza e prevê responder a um ciber ataque.			**QD2.** Que postura assumirá a OTAN ao abrigo do Tratado do Atlântico Norte, se uma nação aliada sofrer um ciberataque?	**H2**: O NAC irá analisar todas as evidências e consequências e, determinar a invocação do artigo 5º, numa análise caso a caso.
CAP 3. A evolução da posição da Aliança Atlântica. **3.1**. Análise à evolução da posição da OTAN. **3.2**. Desafios identificados pela Aliança. **3.3**. O papel do Manual de Talin *(2092 palavras)*		**OE3** – Analisar a evolução da posição da OTAN perante os desafios e as dificuldades que se preconizam no âmbito da ciberdefesa.			**QD3**. Como tem evoluído a posição da OTAN relativamente ao ciberespaço?	**H3:** A OTAN tem evoluído a sua posição sustentadamente, em harmonia com a opinião generalizada dos especialistas internacionais e organizações como a ONU, no respeito pelo DI, procurando preservar a sua posição como referência legítima.

Figura 3 – Quadro síntese do plano de trabalho da Investigação.

Fonte: (O autor,2017)

1. O DCA e o ciberespaço.

A Aliança atua em conformidade com os princípios e normas do DI, no qual se incluem a Carta das Nações Unidas (CNU) e o DCA. Afinal, no artigo 1º do TAN, as partes obrigam-se a respeitar o estabelecido na CNU (OTAN (f), 1949).

Esta posição serve de mote ao grupo de especialistas reunido no *NATO Cooperative Cyber Defence Center of Excellence (CCD COE)*[2], que em 2013 publicou o MdT, e que defende que: "*Cyber Operations executed in the context of an armed conflict are subject to the law of armed conflict*" (Schmitt et al., 2013, p.75)

A aplicação do DI em geral e do DCA em particular, a atos que ocorram no ciberespaço, gera controvérsia. Alguns autores defendem que o DI aplicável ao uso da força é inadequado para enfrentar a ameaça de uma ciberguerra (Addicott, 2010). Outros afirmam que, embora exista espaço para melhoria, os princípios básicos do DCA são suficientes para resolver as questões essenciais de uma ciberguerra (Jr, 2011, p.81).

A tendência internacional aponta no sentido que as "regras do jogo" já existem e serão aquelas consagradas no DI.

Neste primeiro capítulo serão identificados os conceitos que envolvem esta questão, de forma a melhor compreender e analisar a evolução da posição da OTAN.

1.1. Princípios e normas do DCA aplicáveis ao ciberespaço.

Não existindo normas que mencionem diretamente o ciberespaço, então existirão lacunas na aplicação do DCA a um ciberconflito. Com efeito, não sendo possível prever todas as circunstâncias e condições futuras de um conflito armado, não quer dizer que o DCA convencionado e consuetudinário, não possa ser aplicado a situações que não estão expressamente previstas. Daí que seja importante compreender os princípios do DCA, e em particular abordar a cláusula de Martens.

De facto, o corpo basilar de normas passível de ser aplicado a um conflito armado no ciberespaço são as que estão previstas nas convenções que se encontram mencionadas no Anexo A.

[2] O *NATO CCD COE* é uma organização internacional sedeada em Talin, Estónia, que se encontra acreditada como um centro de excelência, pela OTAN desde 2008. A escolha deste país surge após os ataques de 2007. Este centro não pertence à estrutura de Comandos da OTAN, nem é financiado pela Aliança. No entanto pertence a uma moldura abrangente que suporta o "*NATO Command Arrangements*". São seus países patrocinadores a Estónia, a Alemanha, a Hungria, a Itália, a Letónia, a Lituânia, a Holanda, a Polónia, a Eslováquia, a Espanha e os Estados Unidos. (OTAN (d), 2017)

As normas do DCA surgem do costume internacional que rege as relações entre os Estados, ou são aquelas que as nações acordaram em tratados, visando regular juridicamente as ações que decorrem de conflitos armados (Fernandes, 2012, p.136). Estas normas encontram-se alicerçadas nos princípios básicos do DCA (Figura 4).

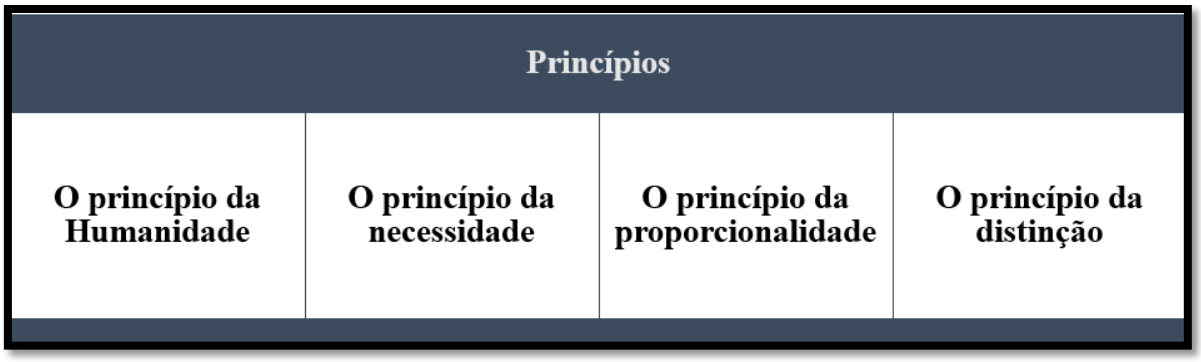


Figura 4 – Princípios de direito que consubstanciam o DCA.

Fonte: (Carreira, 2004, p.26)

À luz destes princípios, num conflito armado só poderão ser atacados alvos que permitam obter vantagem militar ou a submissão do inimigo, estando proibido o ataque a alvos não combatentes e propriedade ou sítios protegidos. No planeamento de uma ciberoperação esta *distinção* tem que ser respeitada. Por exemplo, ao empregar uma capacidade no ciberespaço, essa "arma" deverá ser dirigida a uma infraestrutura ou alvo militar, não podendo ser dirigida a civis.

Sendo o recurso à força entre Estados proibido, tal como se encontra explícito no n.º 4 do artigo 2º da CNU, há que sublinhar as situações de exceção a esta proibição, que resultam do artigo 51º da CNU e ainda do seu capítulo VII.

Se a nação A, atacar uma central de energia para afetar um centro de Comando e Controlo (C2) de uma nação B, mas ao efetuar o ciberataque à central, atinge um hospital, claramente violou os elementos que enformam o conceito de *necessidade* militar (Carreira, 2004, pp.25-35). Consideremos a análise dos quatro elementos que constituem o princípio da *necessidade* (Figura 5):

Elementos do Princípio da Necessidade	**A força usada é regulada (não arbitrária)**
	É a que permite o mais rapidamente possível alcançar a submissão total ou parcial do adversário (adequação);
	Não excede a que é exigida para atingir aquele objetivo (limitação)
	Não é proibida de qualquer outra maneira (legalidade)

Figura 5 – Elementos do Princípio da Necessidade

Fonte: (Carreira, 2004, p.26)

A *proporcionalidad*e estabelece o equilíbrio entre a *necessidade* militar e a *humanidade* (Carreira, 2004, p.32). Olhando novamente para o exemplo anterior, verifica-se claramente um ataque excessivo que provoca danos colaterais. Todo o ataque deverá ser precedido de uma análise que minimize o excesso de força. Se mais que uma opção for possível, então aquela que for menos lesiva deverá ser escolhida.

Demonstra-se assim que estes princípios se podem aplicar a um ciberataque. Se subsistirem dúvidas, veja-se a cláusula de Martens que, "*vem submeter ao Direito tudo aquilo que não esteja abrangido, tudo aquilo que esteja num vazio legal*" (Carreira, 2017).

Toda a codificação por natureza é incompleta, porque não se podem prever todas as situações num dado momento. Tornou-se então necessário conceber um instrumento que, perante novos desenvolvimentos científicos e tecnológicos dos instrumentos da guerra, garanta o princípio da *distinção*. Assim surge a cláusula de Martens[3], tornando legítimo e razoável, o preenchimento de lacunas, considerando que nem tudo o que não é expressamente proibido pelos tratados ou convenções é autorizado e, que nos casos não cobertos pelos instrumentos do DCA são aplicáveis os princípios do DI, tal como decorre do costume, dos princípios de humanidade e das exigências da consciência pública.

Por estes fatores, afigura-se plausível a afirmação no MdT de que as ciberoperações que ocorram no contexto de um conflito armado, estão sujeitas ao DCA.

[3] Ver Apêndice B.

1.2. *Jus ad Bellum, Jus In Bellum* e o Ciberespaço.

Não se pode falar em ciberataque sem nos questionarmos se estaremos perante um ato de ciberguerra ou de cibercrime "estratégico". Hoje, é possível que grupos criminosos cometam atos preparatórios ou ataques a mando de um Estado, sem que se consiga associar estas ações aos Estados que os patrocinaram.

Nestes casos, estaremos perante uma dicotomia entre o que é a cibersegurança e a ciberdefesa, entre o que é cibercriminalidade e ciberguerra, entre o que é o direito que regula a possibilidade de recurso à força por parte dos Estados[4] e, o direito que regula a condução das hostilidades, fixando os direitos e os deveres das partes quando se inicia um conflito armado[5] (Carreira, 2004, pp.18-19).

Assim, parece existir uma dicotomia entre a dimensão da segurança e a dimensão de defesa, numa mescla que hoje se designa por híbrida[6], que recorre, entre outros instrumentos, a ataques no ciberespaço (Figura 6).

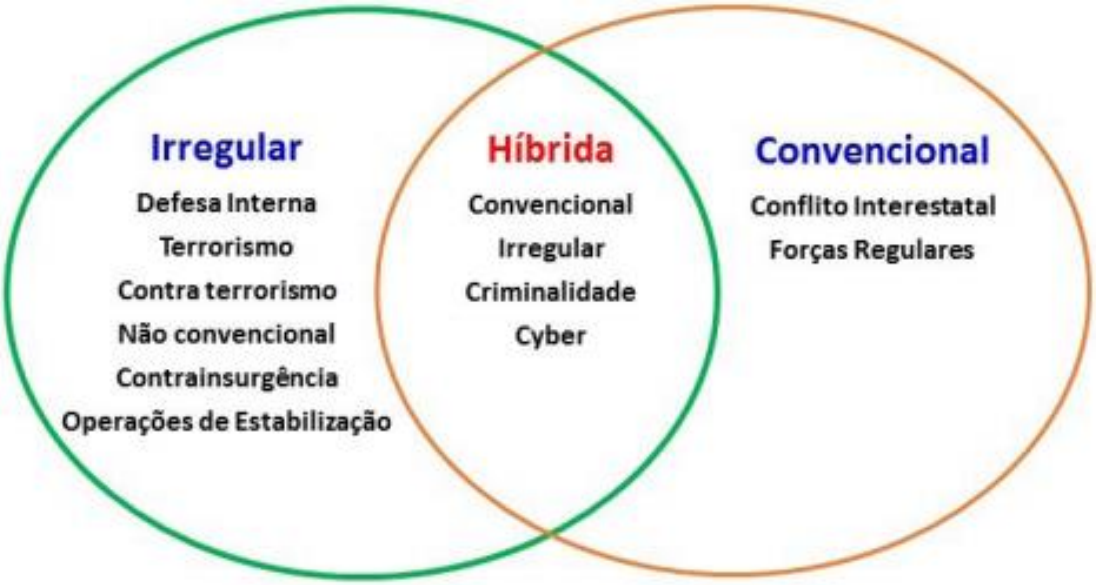


Figura 6 – Modelo Concetual de Guerra Híbrida

Fonte: (Adaptado de U.S. Government Accountability Office, 2010, p.16, cit. por Fernandes, 2016)

Estes grupos (ou indivíduos) a que os Estados recorrem, podem atuar a partir de territórios terceiros, o que agudiza a dicotomia. Compreender se estas situações são de avaliar à luz do ordenamento jurídico interno, ou do DCA, é uma questão que só poderá ser respondida com muita cooperação entre nações, incluindo os seus serviços de informações.

[4] *Jus ad Bellum.*
[5] *Jus in Bellum.*
[6] Ver o conceito no Apêndice B.

Considerando esta dicotomia, a OTAN procura responder coletivamente a estes desafios, criando cenários complexos e realistas que abranjam as várias dimensões da guerra híbrida, nomeadamente nos exercícios que são realizados, como o *NATO Cyber Coalition*[7] (Esteves, 2016). Segundo especialistas militares nacionais envolvidos nos exercícios de ciberdefesa, a OTAN não exercita as reações num cenário de ciberdefesa, mas apenas no campo da cibersegurança, até à dimensão do pré-conflito armado (Esteves, 2016).

O treino da transição de uma situação de cibercriminalidade para uma situação de conflito armado no ciberespaço é uma lacuna a que a Aliança terá de responder. Observando o espetro das dimensões (Figura 7) podemos verificar que as zonas de fronteira se esbatem, o que dificulta a caracterização da resposta correta.

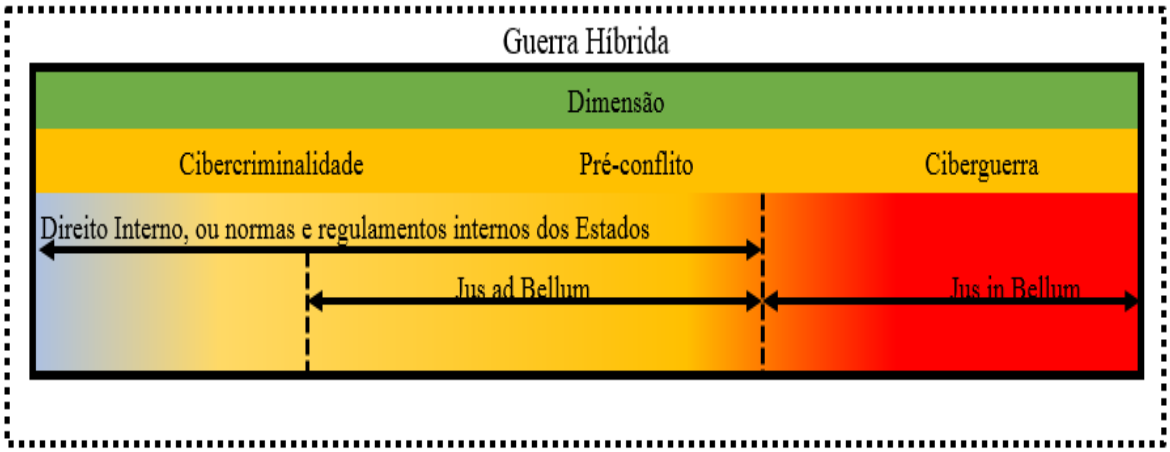


Figura 7 – Espetro da dicotomia das dimensões de Cibercriminalidade e Ciberguerra.

Fonte: (O autor, 2017)

1.3. A qualificação e a atribuição do ato.

1.3.1. A qualificação.

A inexistência de um AA inquina à partida a qualificação de um ciberataque como um ataque deste género. Para a resolução desta questão, os juristas internacionais têm recorrido a um teste assente no(s) artigo(s) 2º das quatro convenções de Genebra. Trata-se do teste do "*escopo, duração e intensidade suficiente*"[8] (Fernandes, 2012, pp.144-45). Este teste, sofre de interpretações díspares, daí que, o instrumento mais importante neste

[7] Trata-se de um exercício anual que dura três dias, e visa testar a capacidade de defesa das redes da Aliança contra ameaças no ciberespaço. Este exercício envolve mais de 600 técnicos e especialistas em cibersegurança dos vários países e parceiros da OTAN (Homesec, 2016).

[8] Este teste corresponde aos critérios do uso da força de Jean Pictet, jurista suíço que foi o principal redator técnico do texto das Convenções de Genebra de 1949 (Fernandes, 2012, p.144).

contexto, será a definição do conceito de "agressão" que decorre do artigo 1º da Resolução 3314 de 1975, da Assembleia Geral das Nações Unidas (AGONU)[9] (Fernandes, 2012, p.145).

Esta resolução permite observar alguns exemplos de atos que se podem considerar como ataques armados, mas não permite por si só responder à questão da qualificação de um ciberataque como um AA. A análise do ciberataque à luz do teste de Jean Pictet, tem sido efetuada sobre a perspetiva de três abordagens distintas[10], conforme demonstra a Figura 8.

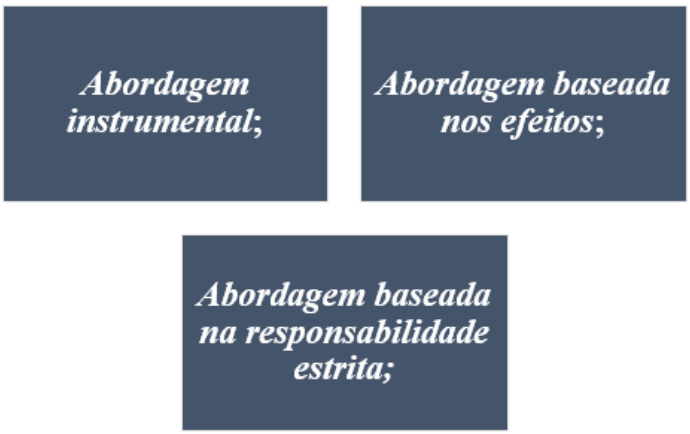


Figura 8 – Tipos de abordagem para qualificação de um ataque no ciberespaço.

Fonte: (Fernandes, 2012)

Todas estas abordagens convergem para a mesma conclusão: "*verificando-se certos requisitos os ciberataques podem constituir ataques armados*" (Fernandes, 2012, p.147).

No MdT demonstra-se[11] que a opção pela abordagem baseada na avaliação dos efeitos (ABAE), é a que permite captar os fatores quantitativos e qualitativos na análise a um ciberataque. (Schmitt et al., 2013, pp.45-46). Independentemente dos métodos, a qualificação terá natureza política. No entanto nada invalida que se criem modelos que habilitem aos Estados sustentar as suas decisões. Assim, o Manual aponta para oito requisitos[12] que ilustram a ABAE e que constam da Figura 9.

[9] Ver Apêndice B.
[10] MdT, parte 2, seção 1, regra 11 ("*Definição do uso da força*"). Ver Apêndice F.
[11] Ver Apêndice E.
[12] A definição de cada um destes requisitos encontra-se no Apêndice E.

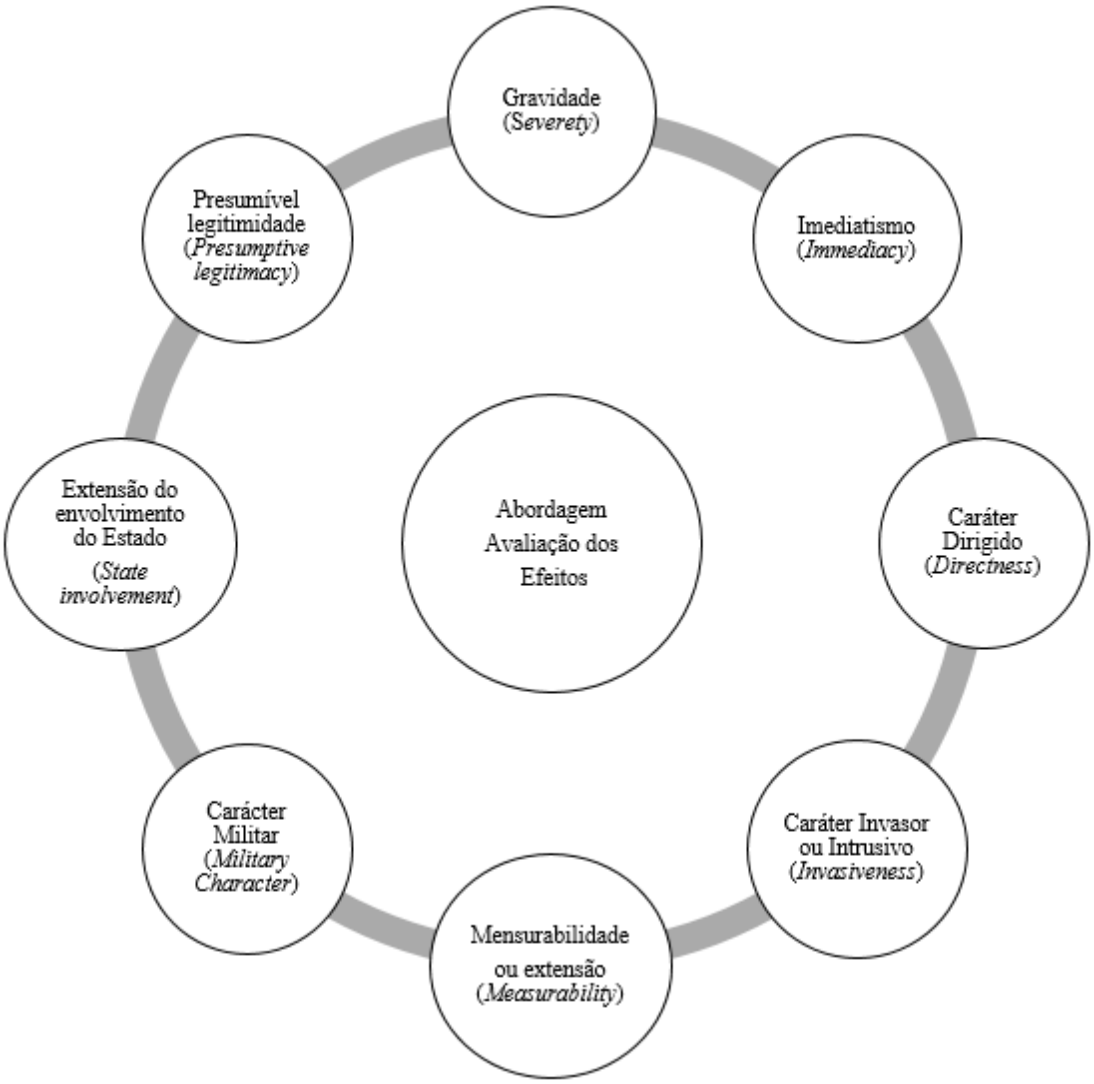


Figura 9 – Modelo da Abordagem da Avaliação dos Efeitos, e os requisitos de avaliação.

Fonte: (Schmitt et al., 2013, pp.45-52)

Não existindo doutrina da OTAN que permita qualificar um ato hostil no ciberespaço, torna-se pertinente considerar estes requisitos, construindo um modelo de análise[13] que permita qualificar um ciberataque como um AA.

1.3.2. A atribuição.

Conforme explica José Fernandes, a atribuição do ataque a uma parte é algo complexo, pois implica sobretudo uma condição tecnológica desenvolvida, que habilite à identificação da origem do ataque (2012, p.150). Identificam-se três limitações principais à capacidade de atribuir a responsabilidade de um ataque, conforme se verifica na Figura 10.

[13] Ver o exercício desenvolvido no Apêndice F.

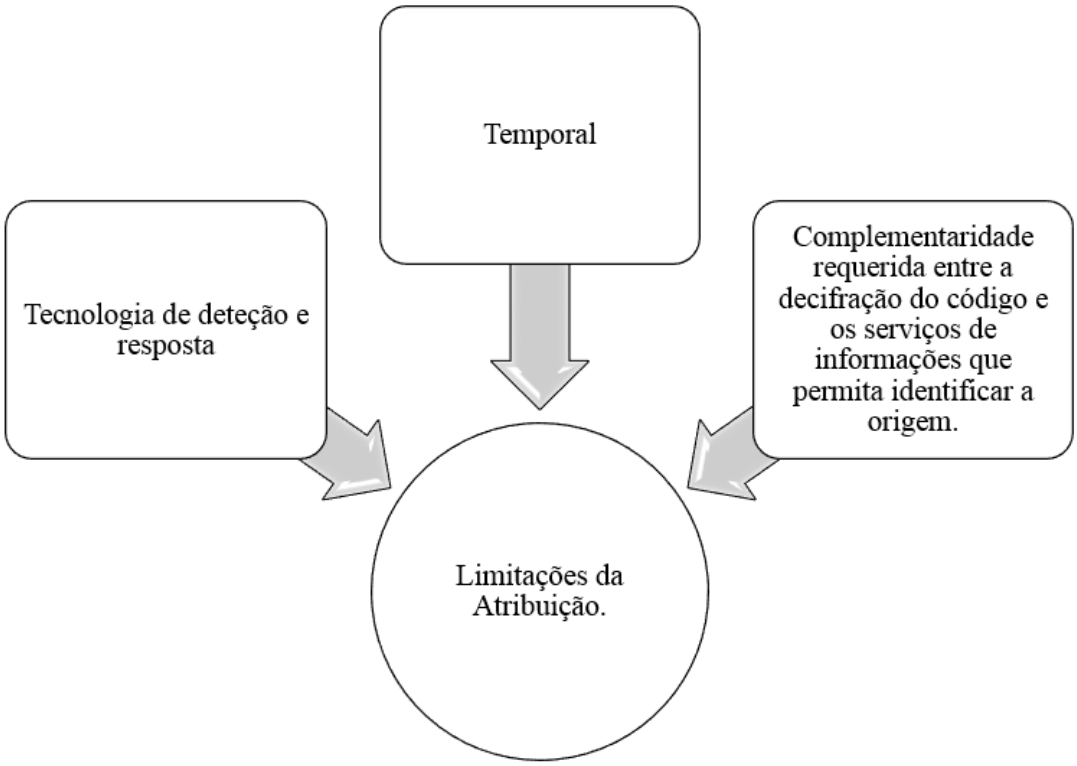


Figura 10 – As três principais limitações na atribuição de um ciberataque.

Fonte: (Fernandes, 2012)

A tecnologia possui limitações nas suas capacidades de deteção, classificação e análise dos ataques, provocando o acumular de erros na atribuição, o que naturalmente levará os decisores a duvidar da eficácia deste recurso (Fernandes, 2012, pp.150-51).

A limitação temporal, reside na necessidade de tempo para analisar o ataque após a sua ocorrência. Por outro lado, quanto maior for esse período, maior será a dificuldade em identificar a origem (Fernandes, 2012, p.168). Finalmente, torna-se complicado discernir a ocorrência, o intuito e a origem, enquanto não for descodificado o código do programa, ou verificados os registos dos dados da atividade atacante (Fernandes, 2012, p.168). Além disso todos os dados obtidos precisam de ser corroborados pelos serviços de informações, sob pena de não se conseguir comprovar os dados obtidos pela descodificação. (Assunção, 2017)

Observando os factos conhecidos do caso da Estónia[14] em 2007, verifica-se que todas estas limitações se aplicaram nesse ataque.

A problemática da atribuição aplica-se tanto a atores estatais, como não estatais (ANE). No entanto, o DCA só se aplicará de forma restrita aos ANE, se a sua atuação

[14] Ver Anexo B.

ocorrer a partir de um "Estado-santuário", que de alguma forma seja corresponsável por essas ações.

A estas limitações acresce o facto de não existir no DI uma norma que estabeleça um padrão que permita retirar conclusões quanto à origem do ciberataque (Schmitt, 2010, p.168).

Os EUA encontraram uma forma de contornar esta situação, quando notificaram o Conselho de Segurança das Nações Unidas (CSNU) de que iriam atuar em LD contra os Talibãs e a *Al-Qaeda*, fundamentando a sua atuação em informações claras e convincentes de que a *Al-Qaeda* exerceu um papel nos ataques ao *World Trade Center* (WTC). O Secretário-Geral da OTAN repete este discurso mais tarde, quando anuncia a intenção da Aliança em atuar no Afeganistão ao abrigo do Artigo 5º do TAN. (Schmitt, 2010, p.168).

Para Schmitt, informação clara e convincente constitui um argumento superior à preponderância da prova, desde que o Estado vítima demonstre que tomou medidas razoáveis para identificar o perpetrador do AA, e que, decorrente dessas medidas alcançou conclusões razoáveis. Então esse Estado vítima terá legitimidade para responder com recurso ao uso da força, independentemente de se tratar de um ciberataque ou um ataque convencional (2010, p.168).

1.4. A questão da legítima defesa.

A LD expressa no artigo 51º da CNU constitui uma exceção à proibição do uso da força[15], que constitui a expressão de um *Jus contra Bellum*, conforme explica Silva Carreira (2017, p.18).

Assim, torna-se relevante analisar a questão da LD no contexto de um conflito no ciberespaço, uma vez que estas "armas" são empregues de forma muito rápida e que o ataque, uma vez em curso, é extremamente difícil de contrariar ou conter. De facto, não se afigura verosímil, que após o início de um ciberataque, o CSNU consiga deliberar atempadamente sobre a legitimidade do uso da força.

Para a maioria das nações, as ações em LD só podem ser realizadas se o ataque estiver em curso ou iminente, nunca antes. Atacar antes de ser atacado seria em si um ato injustificado e, uma retaliação, se em sequência de uma ação consumada.

No entanto, nos EUA a LD é entendida como uma ação que permite o uso da força antes que ocorra uma ofensa real, ou seja, o uso da força em antecipação à consumação do

[15] São exceções o artigo 51º e artigos que constituem o capítulo VII da CNU. (ONU (b), 1945)

efeito do ataque é aceitável. Na perspetiva americana, desde que a resposta seja proporcional à potencial ameaça, esta resposta em LD "preventiva" é legal. A iminência será demonstrada pelo padrão de atividade e de ameaça patente nas intenções dos atores, mesmo que estas não se comprovem. Até mesmo eventos como a reunião, o planeamento, e a conspiração, podem constituir-se como ameaça concreta e, se os riscos forem severos o suficiente, justificarão atuar em LD (Jr, 2011)

As questões da qualificação, atribuição e LD são relevantes, porque a velocidade a que ocorrem os eventos no ciberespaço é elevada, tornando-se essencial o seu conhecimento e domínio, viabilizando uma defesa atempada.

1.5. Síntese conclusiva.

Neste capítulo conclui-se que os princípios e as normas que se aplicam ao ciberespaço num conflito armado são os mesmos que se aplicam aos restantes domínios operacionais. Assim, dando resposta à QD1, verifica-se totalmente a primeira hipótese, ou seja, em caso de conflito armado, aplicar-se-á o DCA a um ciberataque, sendo de referir que as maiores dificuldades advirão das considerações relativas à qualificação e à atribuição do ato e, à celeridade na obtenção de informações que permitam responder em LD a uma agressão no ciberespaço (Figura 11).

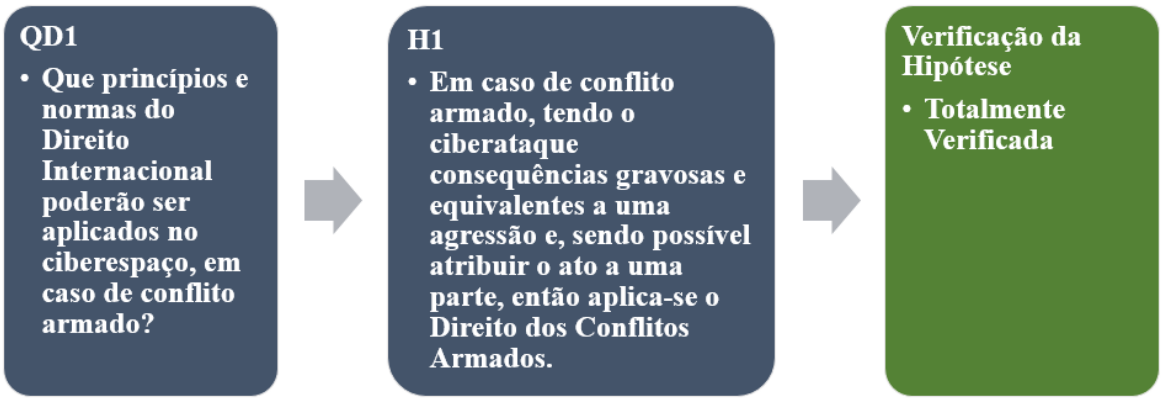


Figura 11 – Verificação da H1.

Fonte: (O autor, 2017)

Toda esta problemática importa à Aliança, pois têm implicações na sua PCD. No próximo capítulo será explorada a influência de outras Organizações Internacionais (OI), na perceção da OTAN sobre a regulação e governação (ReG) do ciberespaço.

2. A OTAN, a regulação e a governação do ciberespaço.

"*Eu declaro o espaço social global que estamos a construir naturalmente independente das tiranias que nos tentam impor. Não têm o direito moral de nos governar, nem têm métodos de coação que tenhamos verdadeira razão para temer*." (Barlow, 1996).

Este capítulo visa explorar a posição da OTAN relativamente à ReG e à aplicabilidade do DI no ciberespaço em geral e, do DCA em particular.

O respeito em absoluto pelo DI, legitima a Aliança como OI com estatuto moral elevado. Este estatuto é um objetivo estratégico vital a preservar. Assim, a Aliança acompanha a evolução nesta matéria em *fora*, como a ONU e a Organização para a Segurança e Cooperação na Europa (OSCE), tentando compreender melhor, a evolução dos desafios e das ameaças no ciberespaço.

2.1. Política de Ciberdefesa.

Quanto à governação da ciberdefesa da OTAN, esta é definida por uma política assente em três vetores, conforme se pode verificar na Figura 12:

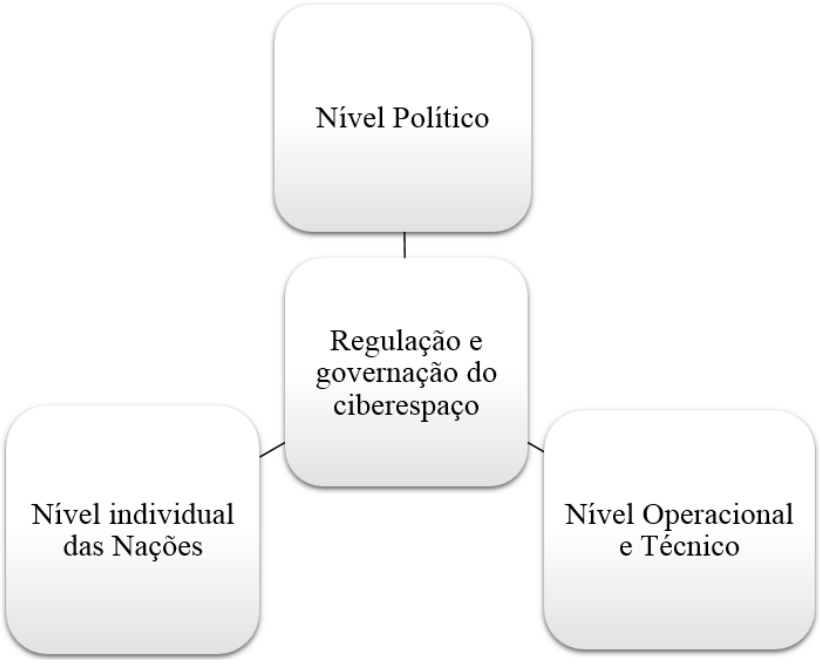


Figura 12 – Níveis de regulação e governação do ciberespaço da OTAN.

Fonte: (O autor, 2017)

Ao nível Político, o CAN é a principal autoridade na estrutura de ciberdefesa da OTAN, emanando diretivas para os comités subordinados e para as autoridades militares (NMA) (OTAN (d), 2017).

O CAN recorre ao *Cyber Defence Committee* (CDC) para fins de governação política e aos *Operations Policy Committee* (OPC) e Comité Militar (MC), para fins de governação operacional. Estes correspondem, respetivamente, aos vetores político e operacional/técnico. O primeiro apoia o CAN na definição e implementação das políticas (OTAN (n), 2016), enquanto os segundos apoiam na resposta a situações de crise no ciberespaço (OTAN (d), 2017). No Apêndice C encontra-se definido o papel de cada comité e seus órgãos e, na Figura 13, é possível verificar a estrutura da organização.

Por fim, as nações desenvolvem individualmente as suas capacidades, contribuindo para a defesa das redes nacionais ligadas às redes da Aliança. Esta poderá auxiliar na edificação (nomeadamente através da partilha de informação com as nações) ou, mediante prévia aprovação do CAN, apoiar as nações que solicitem auxílio na defesa a ciberataques (OTAN (d), 2017). As modalidades de cooperação com a NATO encontram-se estabelecidas em memorando de entendimento (MOU)[16] entre as nações e o *Cyber Defence Management Board*. São as nações, principalmente aquelas que maiores capacidades[17] têm, que mais contribuem para o desenvolvimento da PCD.

[16] Portugal assinou um NATO *Cyber Defence* MOU em junho de 2016, com o intuito de explorar essencialmente duas áreas: i) a troca de informação; ii) a reposta a incidentes através do apoio das NCIRC *Rapid Response Teams* (RRT). Atualmente assinaram MOU dezasseis nações (Albânia, Bulgária, Canada, República Checa, Dinamarca, Estónia, Alemanha, Hungria, Islândia, Holanda, Noruega, Portugal, Romania, Eslováquia, Eslovénia e Turquia).

[17] Como os EUA, Reino-Unido, França e Holanda.

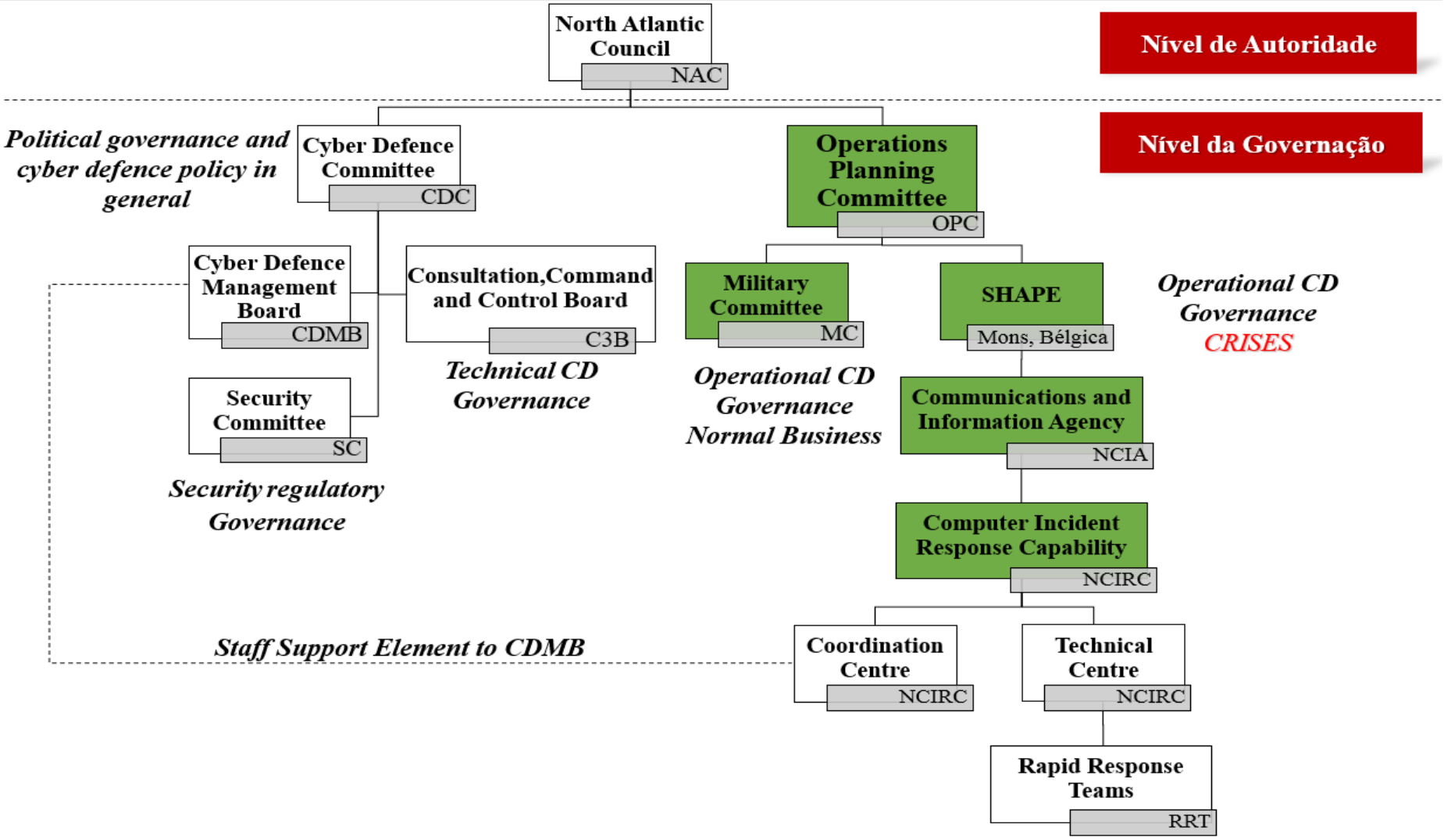


Figura 13 – Estrutura hierárquica e funcional.

Fonte:(O autor, 2017)

Em 2014, os CEeG acordaram em Gales, o reforço da PCD, aprovando a "*Enhanced Cyber Defence Policy*" (ECDP). Esta assenta em três pilares (Figura 14).

Figura 14 – Os três pilares da PCD da OTAN.

Fonte: (OTAN (d), 2017)

Para que se alcancem os objetivos desta política, a OTAN recorre a um processo de planeamento integrado, o *NATO Defence Planning Process* (NDPP)[18]. É através deste processo que a Aliança e os aliados definem e edificam[19] as suas capacidades. Estas desenvolvem-se sobretudo através de projetos *Smart Defence (*SD*)*, um conceito que representa uma forma de cooperação voluntária entre vários aliados, e que permite gerar capacidades modernas de defesa, de uma forma mais eficiente, eficaz e coerente.

[18] O NDPP é o principal meio que a Aliança e as Nações utilizam para identificar as capacidades requeridas para a sua defesa e segurança, promovendo o seu desenvolvimento e aquisição, de forma atempada e coerente.

[19] Recorrendo ao conceito DOTMLPII - (D)-Doutrina; (O) – Organização; (T) – Treino; (M) – Material; (P) – Pessoal; (L) – Liderança; (I) – Infraestruturas (I) – Interoperabilidade.

A PCD assenta em oito princípios que se encontram detalhados na Figura 15.

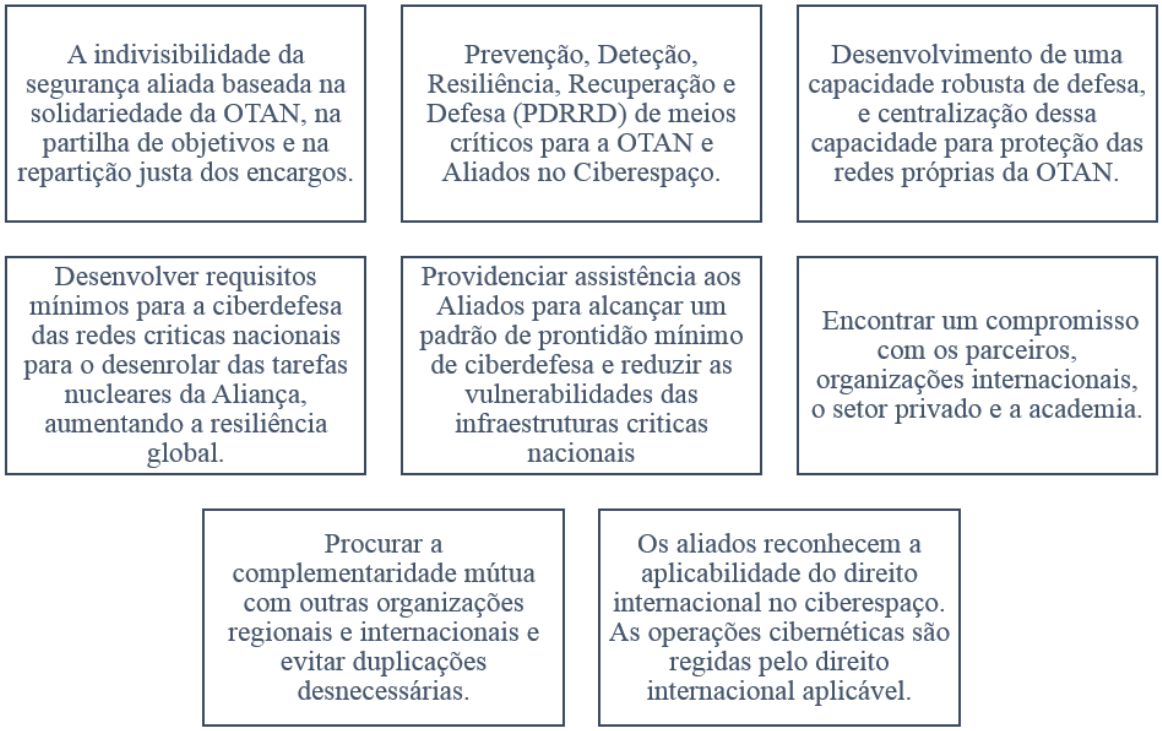


Figura 15 – Princípios da PCD da Aliança Atlântica.

Fonte: (OTAN (d), 2017)

Destes princípios realçam-se, a aplicação do DI no ciberespaço e a clara orientação para a defesa. No entanto, conforme nos explicam Sardinha Monteiro e Silva Pinto, para que a ciberdefesa seja eficaz, tem de assumir a superioridade e, esta só será alcançada se também forem exploradas as capacidades militares ofensivas no ciberespaço. Essa superioridade trará consequências, que deverão ser ponderadas nas fases de planeamento e execução das operações, à luz do DCA (Monteiro & Pinto, 2016, pp.4-5).

O desenvolvimento de "armas" trará um elemento de "*deterrence*" à ciberdefesa da Aliança, mas ao contrário da "*deterrence*"[20] nuclear, em que demonstrar que possuímos capacidade, exerce efeito sobre o oponente, nas capacidades de ciberdefesa, revelar as nossas "armas" poderá potenciar a sua neutralização imediata. Por outro lado, não desenvolver essa capacidade e não demonstrar que se está a investir neste domínio, revelará fragilidade. Conforme explica James Lewis, o secretismo em torno desta política pode ser contraproducente, levando os oponentes a acreditar que não existe risco, por incapacidade da Aliança (2015, p.2).

[20] Ver conceito no Apêndice B.

2.2. A invocação do artigo 5º do Tratado do Atlântico Norte.

O artigo 5º do TAN foi pela primeira vez invocado após o ataque ao WTC em 2001. Este artigo estabelece a garantia de apoio mútuo entre os Estados signatários (Fernandes, 2012, p.94).

Conforme foi demonstrado no primeiro capítulo, dependendo das circunstâncias, um ciberataque poderá equivaler a um AA, o que, de acordo com o artigo 51º da CNU, legitimará uma resposta em legitima defesa. Se o Estado atacado for membro da OTAN, então o CAN terá de ponderar a aplicação do artigo 5º, avaliando a situação caso a caso. (OTAN (n), 2014, p.15). Esta ponderação ocorrerá após a Parte atacada consultar as outras Partes, conforme artigo 4º do TAN[21].

O recurso ao artigo 5º possui carácter dissuasor, mas uma guerra *híbrida* com recurso a ciberataques poderá situar-se no limite inferior do limiar que justifique uma resposta baseada nesta opção (Atlantic Council, 2014, pp.6-7). Fora do limiar do conflito armado, os ciberataques contra a OTAN só poderão ser qualificados como espionagem, cibercriminalidade ou "*information war*" (Veenendaal et al., 2016, p.5). Assim, haverá benefício em manter alguma ambiguidade e flexibilidade no que concerne à tomada de posição da Aliança quanto à invocação do artigo 5º em resposta a um ciberataque.

De qualquer das formas, não possuindo capacidades ofensivas, não será possível à OTAN responder por si isoladamente, tendo que contar com as capacidades dos aliados. Em tais situações, a Aliança necessitará de demonstrar coesão e determinação para a utilização deste importante instrumento. Porventura, no futuro, este desafio constituirá o centro de gravidade estratégico da Aliança.

2.3. A posição de países não-OTAN.

Atualmente, ocorre na ONU uma verdadeira "corrida contrarrelógio", conforme relata o Embaixador Luís Barreira de Sousa (2017). De facto, o Ocidente não possui a maioria dos votos para impedir a aprovação daquilo que se veio a denominar: "*código internacional de conduta para a segurança da informação*" (Sousa, 2017).

A Federação Russa (FR) tenta aprovar este código desde 1998. (Gjelten, 2010). Para tal conta com o apoio das nações que constituem a Organização para a Cooperação de

[21] "*As partes consultar-se-ão sempre que, na opinião de qualquer delas, estiver ameaçada a integridade territorial, a independência política ou a segurança de uma das Partes*" (OTAN (f), 1949).

Shangai[22], onde se pode encontrar a China. Juntos, pretendem censurar a informação que é veiculada através do ciberespaço e que entendem como sendo contrária aos interesses dos seus regimes. Para estas nações, tratam-se de ações malévolas de ciberguerra sobre a forma de "*information war*"[23] (Gjelten, 2010).

Para os países aliados, torna-se importante contrariar este movimento, não se podendo deixar de considerar que, o surgimento do GPG e a discussão prolongada destas questões, mais não possa representar que, uma tentativa de ganhar tempo, permitindo obter votos para impedir a aprovação do "*código*" (Sousa, 2017).

Por outro lado, potências como os EUA tentam evitar um código que force a discriminação das suas capacidades, enquanto desenvolvem "armas" que lhes permitam contrariar o desenvolvimento tecnológico dos países não-OTAN. Também para este efeito, importará ganhar tempo. Estima-se que as nações mais desenvolvidas possuam as capacidades evidenciadas na Figura 16, sendo de salientar que a nação com maior pontuação não pertence à OTAN.

Estados	Capacidade ciberofensiva	Ciberdependência	Capacidade ciberdefensiva	*Score* total
EUA	8	2	1	11
Rússia	7	5	4	16
China	5	4	6	15
Irão	4	5	3	12
Coreia do Norte	2	9	7	18

Figura 16 – Estimativa de capacidades das principais potências no ciberespaço

Fonte: (Fernandes, 2012)

O GPG reúne-se periodicamente[24], tentando identificar as ameaças que surgem da utilização das Tecnologias de Informação e Comunicações (TIC) e, as ações necessárias para as combater, incluindo normas, regras, princípios e medidas para aumentar a confiança entre nações (GPG, 2015).

A OTAN demonstra inequivocamente a sua posição, ao reconhecer os esforços do GPG e da OSCE, afirmando: *"Nós acolhemos o trabalho voluntário no estudo de normas*

[22] A Organização para a Cooperação de Shangai (*SCO* em inglês), é constituída pela Federação Russa, China, Cazaquistão, Quirguistão, Tajiquistão e Uzbequistão.
[23] Ver o conceito de "*Information War*" no Apêndice B.
[24] O Grupo reuniu por 7 vezes desde a aprovação da Resolução da AGNU A/RES/58/32 de 2003.

internacionais que regulem um comportamento responsável dos Estados, e nas medidas que gerem confiança na gestão do ciberespaço."[25] (OTAN (c), 2016).

Estes esforços permitem à Aliança estar mais perto de realizar a essência da sua política, ou seja, a promoção da paz e segurança (OTAN (o), 2016).

2.4. O Compromisso para a Ciberdefesa.

Segundo Jens Stoltenberg, Secretário-Geral da OTAN, a Aliança alcançou bastante na resolução de ciberataques, mas necessita fazer mais. As ameaças não respeitam fronteiras e nenhum país é invulnerável (Stoltenberg, 2016). É por este motivo que surge o CC, assumido pelos aliados na Cimeira de Varsóvia.

O CC implica a cooperação entre nações na partilha de informação, mas também o cumprimento do exposto no artigo 3º do TAN[26], ou seja, a responsabilidade em investir e melhorar as capacidades de ciberdefesa das infraestruturas nacionais, o assegurar da compatibilidade com as redes da OTAN e, com as dos outros aliados, evitando elos fracos.

Trata-se de um instrumento vital e vinculativo para a prossecução dos objetivos de ciberdefesa coletiva, que reforça a determinação dos aliados em atribuir recursos para fortalecimento das suas defesas, sendo que foram estabelecidos prazos e métricas, para controlo e revisão das metas definidas (OTAN (a), 2016, pp.1-2). Este compromisso assenta em sete objetivos demonstrados na Figura 16:

[25] Tradução da autoria do autor.

[26] "*A fim de atingir mais eficazmente os fins deste Tratado, as Partes, tanto individualmente como em conjunto, manterão e desenvolverão, de maneira contínua e efetiva, pelos seus próprios meios e mediante mútuo auxílio, a sua capacidade individual e coletiva para resistir a um ataque armado*" (OTAN (f), 1949).

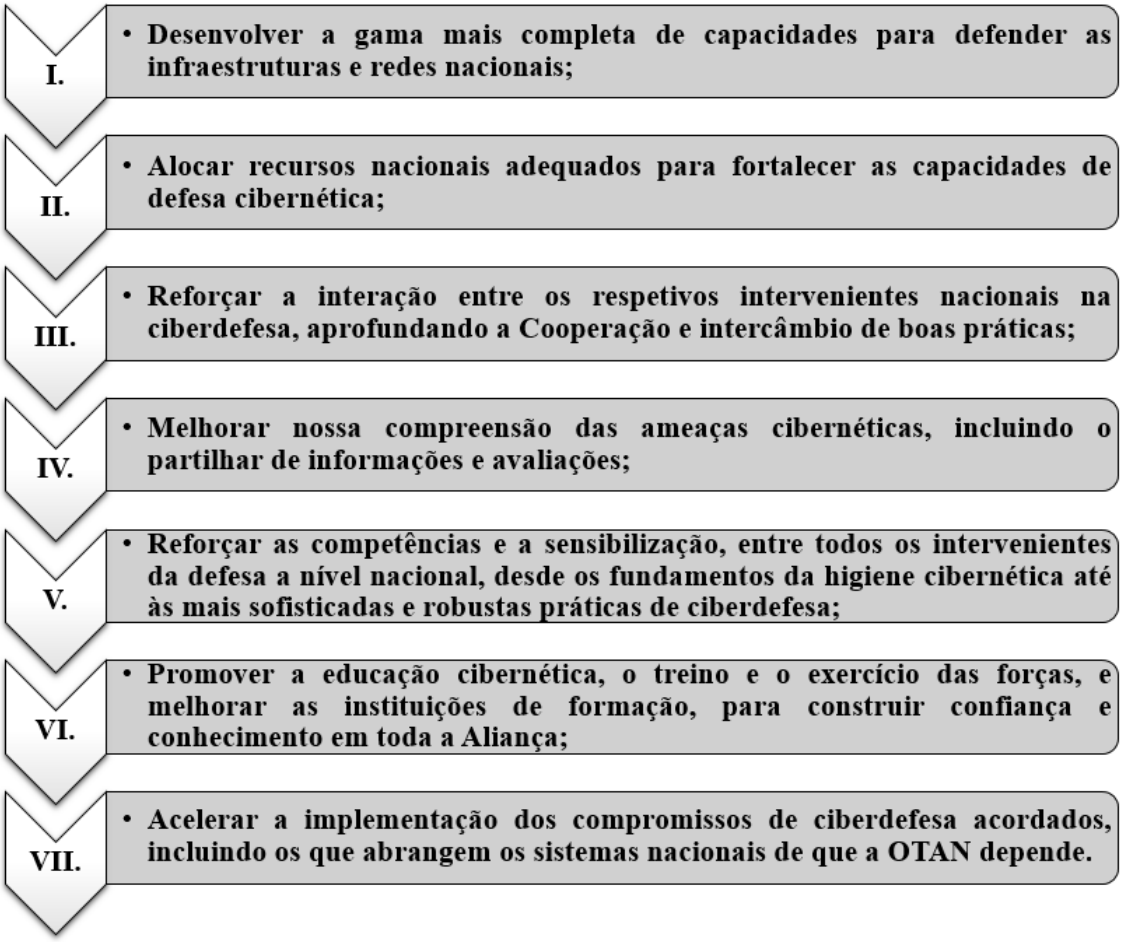


Figura 17 – Os sete objetivos chave do CC[27].

Fonte: (OTAN (a), 2016, pp.1-2)

Caberá às nações efetuar uma autoavaliação anual do estado de implementação destes objetivos.

2.5. Síntese conclusiva.

Neste capítulo conclui-se que, a OTAN se organiza em torno de uma política alicerçada em três pilares: i) A Aliança defenderá as suas redes; ii) As nações aliadas defenderão as suas infraestruturas; iii) Com base no principio da solidariedade, a Aliança poderá prestar assistência a um Aliado vítima de um ciberataque sério. Esta PCD é influenciada pelos trabalhos em torno da ReG do ciberespaço, desenvolvidos por outras OI, pois o resultado dessas deliberações permitirá melhorar a ciberdefesa da Aliança.

A OTAN, como OI que defende os princípios do DI, apresenta-se como referência moral, contrariando legitimamente a posição dos países não-OTAN.

[27] Traduzido do original.

Conclui-se ainda que, perante um ciberataque, existirá benefício em manter ambiguidade e flexibilidade relativamente à possibilidade do CAN invocar o artigo 5º do TAN. A avaliação da situação ocorrerá caso a caso, e após a solicitação de consulta pela Parte afetada. Este instrumento mantém-se relevante, providenciando dissuasão, mas poderá vir a constituir-se como o teste derradeiro à coesão e determinação da Aliança.

Por fim, o CC visa atingir sete objetivos chave, que na sua essência se resumem a: i) O investimento na edificação das capacidades de ciberdefesa nacionais, compatíveis com a OTAN e com os restantes aliados, é uma responsabilidade individual; ii) Promover a partilha da informação, do treino e da formação, reforçando as competências, sensibilização e a compreensão das ameaças cibernéticas.

Assim, conclui-se que a segunda hipótese se verifica totalmente, dando resposta à QD2 (Figura 18).

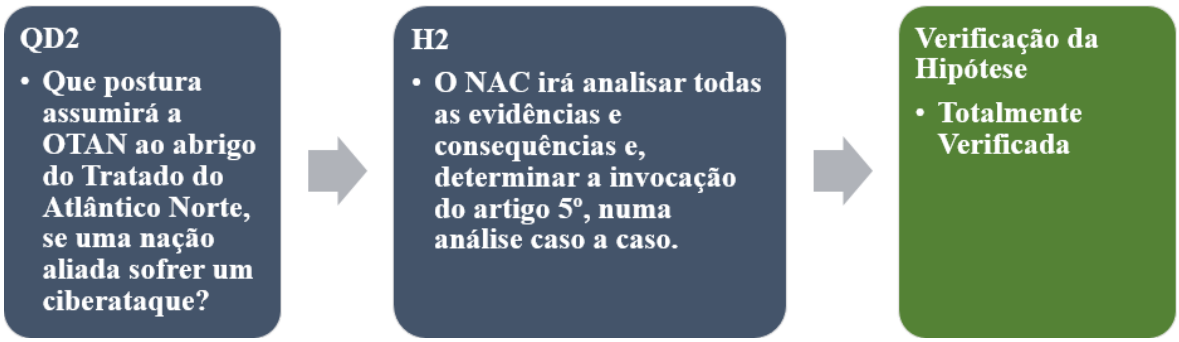


Figura 18 – Verificação da H2.

Fonte: (O autor, 2017)

No próximo capítulo, analisar-se-á a evolução da posição da Aliança perante o ciberespaço e os desafios que se perspetivam. Por último, será feita uma referência ao papel do MdT.

3. A evolução da posição da OTAN.

A sociedade assiste recorrentemente a operações no ciberespaço que visam obter informações, destabilizar sociedades e testar as capacidades de defesa das infraestruturas chave, conforme atesta a Figura 19.

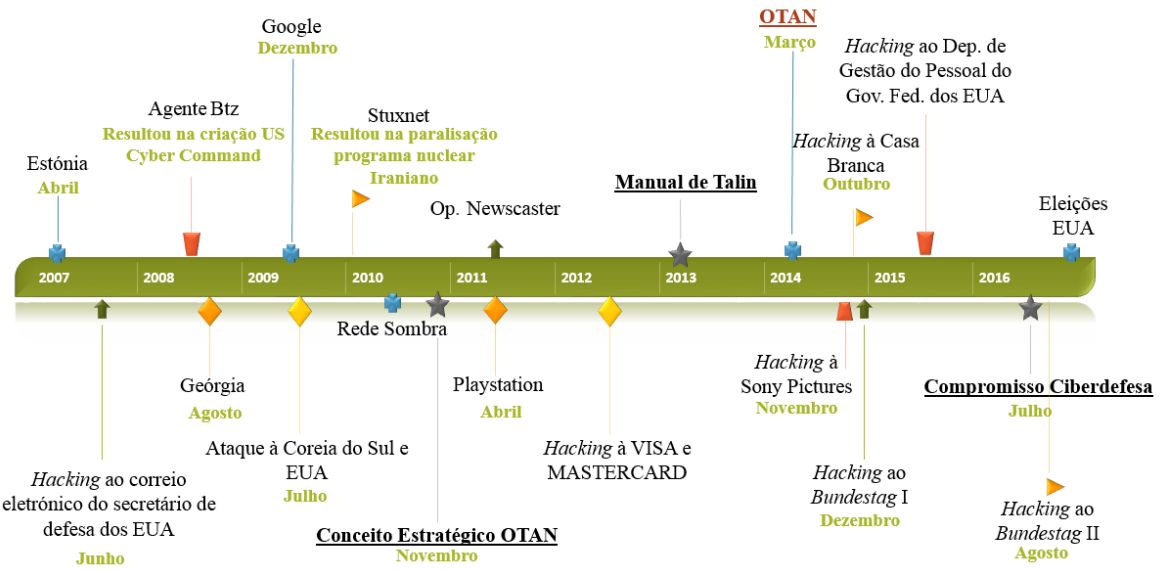


Figura 19 – Cronograma de ciberataques (2007-2016).

Fonte: (Wikipedia, 2017)

Assim, torna-se vital a defesa das redes e infraestruturas das nações aliadas e da OTAN. Todavia, as medidas adotadas não poderão implicar o atropelo de direitos, liberdades e garantias, justificando-se esse atropelo com necessidades de defesa.

Neste capítulo pretende-se analisar a evolução da posição da OTAN, considerando os desafios que enfrenta em matéria de PCD, bem como demonstrar que o MdT desempenha um papel importante nesta evolução.

3.1. Análise à evolução da posição da OTAN.

A posição da Aliança relativamente ao ciberespaço tem evoluído de forma sustentada e ponderada, alicerçada em estudos e conceitos desenvolvidos internamente e noutras organizações[28]. A OTAN preserva uma posição moralmente elevada, de organização legitimada pelo respeito pelos princípios democráticos e pelo DI e, como tal, não pode dar passos em falso.

De facto, a Aliança colocou a ciberdefesa pela primeira vez no seu radar em 2002, em Praga e, desde então, esta capacidade tem sido estudada e edificada.

[28] Como é o caso do MdT e o papel do NATO CCD COE.

Para demonstrar essa evolução, foi efetuada uma análise do conteúdo (AC) (desenvolvida no Apêndice D) das declarações finais das cimeiras da Aliança no período compreendido entre 2002 e 2016. A análise consistiu na categorização das menções e expressões utilizadas pelos CEeG e respetivo enquadramento em quatro indicadores chave, conforme se pode observar na Tabela 2.

Tabela 2 – Categorias e Indicadores da AC.

Categorias (Menções)	Indicadores
#Ciberataques; #Ciberameaças;	Ameaças (A)
#Direito Internacional; #Direito dos Conflitos Armados;	Direito (D)
#Medidas Técnicas #Medidas Operacionais #Medidas relacionadas com Treino e Exercícios #Edificação de Capacidades	Medidas (M)
#Política de Ciberdefesa #Estratégia; #Menções a OI;	Políticas (P)

Fonte: (O autor, 2017)

Posteriormente, quantificaram-se os indicadores conforme se verifica na Tabela 3, de forma a habilitar o seu tratamento estatístico.

Tabela 3 – Quantificação dos indicadores.

Documento	Quantificação						
	A	D	M	P	MED	IND	SOMA
Praga - 2002	1	0	1	0	1,0	2	2
Istambul - 2004	0	0	0	0	0,0	0	0
Riga - 2006	0	0	1	0	1,0	1	1
Bucareste - 2008	1	0	4	1	2,0	3	6
Estrasburgo/Khel – 2009	1	0	5	5	3,7	3	11
Lisboa - 2010	1	0	2	2	1,7	3	5
Chicago - 2012	1	0	4	3	2,7	3	8
Gales - 2014	1	2	7	8	4,5	4	18
Varsóvia - 2016	1	1	2	0	1,3	3	4

Fonte: (O autor, 2017)

Da análise estatística, verificou-se que o indicador com mais menções corresponde à categoria da edificação de capacidades e de medidas, logo seguida pela categoria política. Observando estes resultados (Tabela 4), constata-se que a Aliança tem tido uma posição reativa aos eventos que ocorrem no ciberespaço (Figura 19) e às deliberações de outros *fora*.

Tabela 4 – Peso dos indicadores.

Peso por Indicador	Indicadores			
	A	D	M	P
N.º de Menções	7	3	26	19

Fonte: (O autor, 2017)

Ainda relativamente ao tratamento dos indicadores, realça-se que a categoria da aplicabilidade no ciberespaço do DI, em geral, e do DCA, em particular, apresenta o menor peso, sendo mencionada apenas a partir de 2014.

Como se pode verificar na Figura 20, os indicadores demonstram uma evolução que, embora não constante, se revela gradual e suscetível a eventos como o ataque à Estónia em 2007, ou a invasão da Geórgia em 2008.

De forma a se obter uma média ponderada, recorreu-se à seguinte fórmula para o cálculo:

$$\frac{\sum(Peso\ A\ +\ Peso\ D\ +\ Peso\ M\ +\ Peso\ P)}{\sum n.º\ de\ Indicadores}$$ [29]

[29] Apenas se contabilizam os Indicadores cujo peso seja superior a zero.

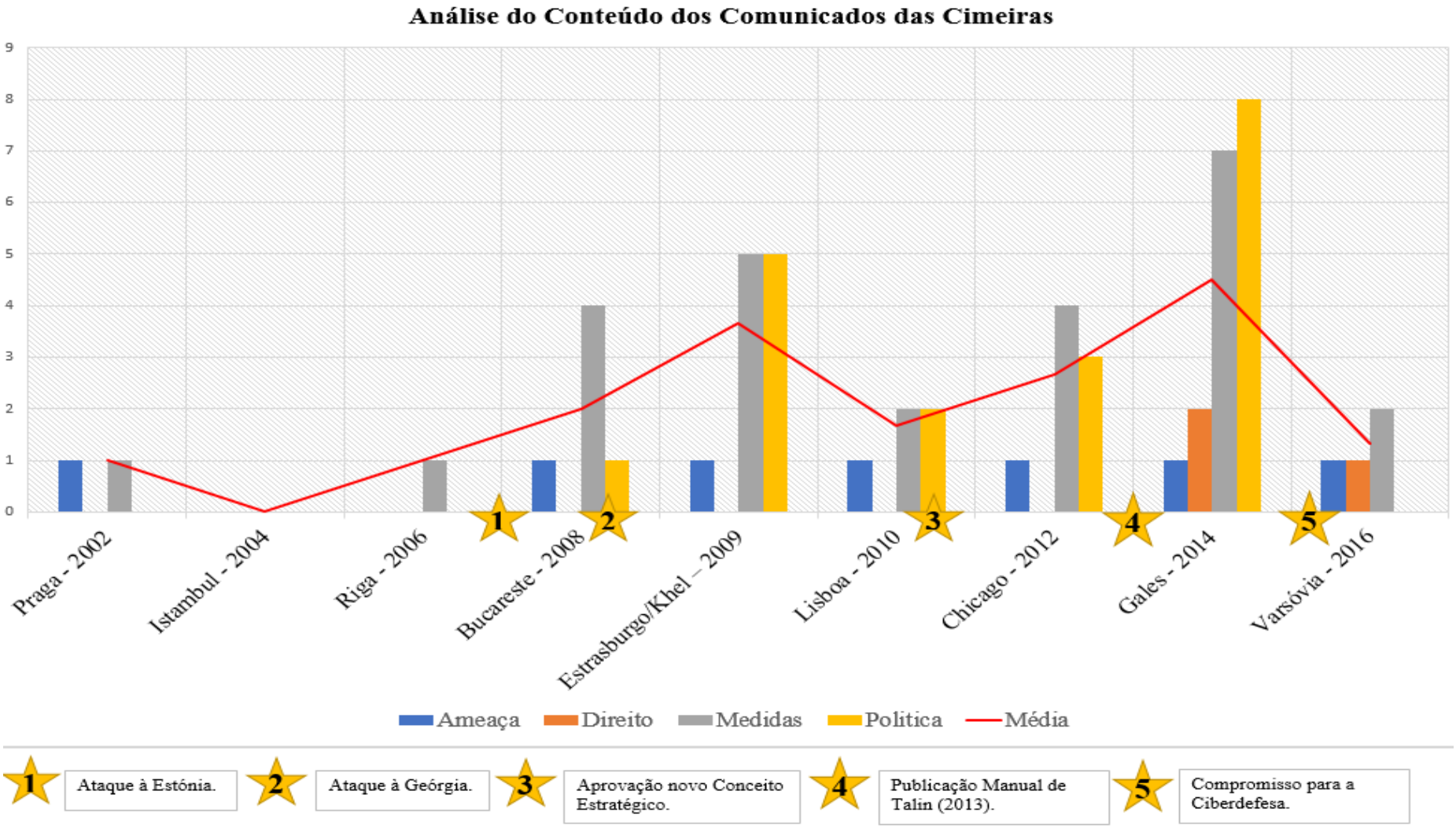


Figura 20 – Análise de Conteúdo das Cimeiras da OTAN (2002-2016).

Fonte: (O autor, 2017)

Observando em particular a categoria da aplicabilidade do DI no ciberespaço, verifica-se que existe uma relação entre a publicação do MdT (2013) e a declaração da cimeira de Gales, ilustrada na Figura 21. Em 2014, os CEeG reconhecem claramente que o DI se aplica no ciberespaço e que as operações que ocorram em resposta a um conflito armado devem obedecer ao DCA.

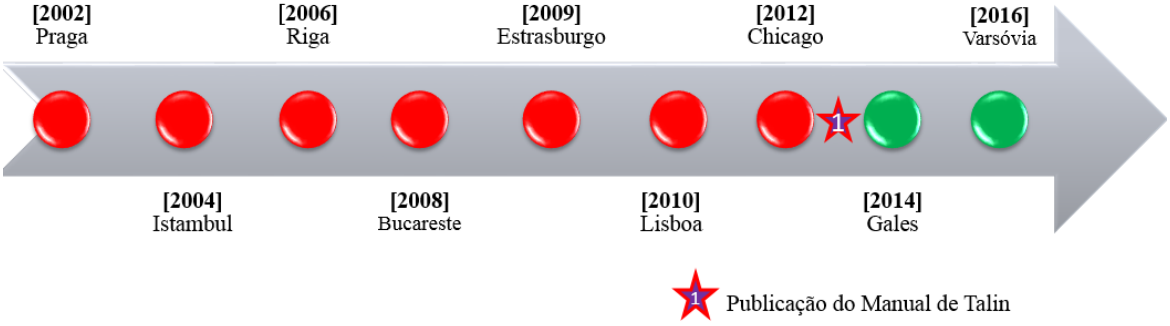


Figura 21 – Semáforo da evolução da posição da NATO relativamente à aplicabilidade do DI e do DCA no ciberespaço.

Fonte: (O autor, 2016)

3.2. Desafios identificados pela Aliança.

Ao reconhecer o ciberespaço como um domínio, a Aliança procura responder aos desafios da ciberdefesa. Estes podem ser divididos em desafios políticos, jurídicos e estratégicos-operacionais.

No tocante aos desafios políticos, os aliados têm deliberado no sentido de reforçar a PCD, conforme se verificou com a promulgação da ECDP em 2014. No entanto subsistem dúvidas quanto à forma como os países com maiores capacidades apoiarão as atividades de ciberdefesa da Aliança e dos aliados. Com efeito, a OTAN não pretenderá desenvolver uma capacidade ofensiva própria como medida de defesa coletiva, essa capacidade terá de ser providenciada por aquelas nações. Assim, afigura-se relevante disponibilizar um catálogo de capacidades, das nações e da Aliança[30] (Hutson, 2014)

Outro aspeto significativo, é a cooperação entre serviços de informações. Sendo a espionagem um dos objetivos das ciberoperações, torna-se necessário que o operacional técnico seja apoiado pelo analista "espião", que correlacione todos os pedaços de informação e aponte para conclusões (Assunção, 2017). A confiança entre os aliados é reforçada com a cooperação e partilha desta informação, tornando-se vital para que se

[30] No original "Cyber Prioritized Asset List" (CPAL).

consiga uma compilação do panorama e um aviso antecipado. Esta partilha permitirá um incremento da interoperabilidade, se as nações mais evoluídas disponibilizarem as suas informações e boas práticas às menos evoluídas. Além disso só através de uma forte ligação com a comunidade de *intelligence*, se poderá responder à questão da atribuição de um ciberataque.

Realça-se que a OTAN não possui competência para estabelecer normas do DI que regulem o ciberespaço. Todavia, sendo uma OI de 29 países cujas decisões são sempre tomadas por consenso, as posições políticas adotadas e declaradas pela Aliança poderão acabar por influenciar outras OI, como a ONU (sede onde se poderão estabelecer normas para ReG do ciberespaço).

Quanto aos desafios jurídicos, com o reconhecimento de que o DI, em geral, e o DCA, em particular, se aplicam ao ciberespaço, a dificuldade reside na criação de doutrina legal ou de regras de empenhamento (ROE) que permitam responder eficazmente a potenciais adversários.

Por fim, afigura-se relevante decompor os desafios estratégicos-operacionais nos níveis estrutural, genético e operacional (Figura 22).

Genético	Estrutural	Operacional
• A não duplicação de esforços e de recursos; • Reforçar o ênfase na formação e treino; • Introduzir uma nova forma de colaboração com as empresas que constituem o *NATO Industry Cyber Partnership* (NICP).	• Cumprir as metas do Compromisso para a Ciberdefesa; • Reforçar ligação com a UE; • A prevenção e resiliência das estruturas e sistemas.	• A partilha de informação e a segurança das infraestruturas; • A implementação, revisão e atualização de doutrina.

Figura 22 – Decomposição dos desafios nos níveis Genético, Estrutural e Operacional.

Fonte: (O autor, 2017)

A OTAN recorre ao conceito de SD, estimulando as sinergias e a cooperação entre os aliados (MDN, 2017). A SD é assumida como uma forma de evitar a duplicação de recursos, permitindo a integração das capacidades nacionais num racional de "*pooling and sharing*" que habilite uma melhor definição e coordenação de esforços entre a Aliança e as nações (MDN, 2017).

Sustentada neste racional, a OTAN desenvolve o projeto *Multinational Cyber Defence Capability Development* (MN CD2), visando a edificação das capacidades dos aliados, de forma a que estes se preparem, previnam, detetem, respondam e recuperem de ciberataques que tenham afetado a confidencialidade, integridade e disponibilidade da informação (OTAN (p), 2014).

Também de referir que a Aliança tem vindo a reforçar a sua colaboração com a União Europeia (UE)[31] visando obter sinergias que permitam usufruir das capacidades de combate à cibercriminalidade, como o Centro do Cibercrime em Haia (Robinson, 2016), mas também, com a indústria privada, onde procura obter economia de escala, eficácia, desenvolvimento tecnológico e partilha de informação (Machi, 2017).

Em cooperação com o *Allied Command for Transformation* (ACT), as nações procuram colmatar as lacunas identificadas a nível genético, com o projeto *Multinational Cyber Defence Education and Training* (MN CD E&T). A OTAN entende que a ciberdefesa é uma área de atenção permanente, pelo que importa investir na formação e treino, em complemento com o desenvolvimento tecnológico, procurando alcançar melhores técnicas, táticas e procedimentos (TTP). Na Figura 23 identificam-se as lacunas na formação.

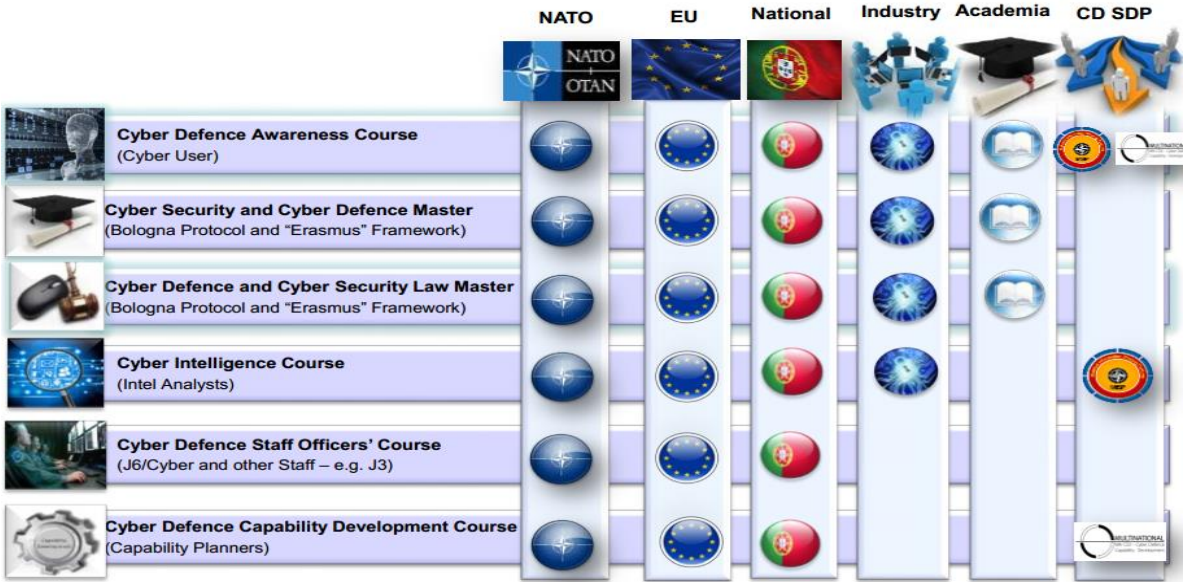


Figura 23 – Lacunas na formação, identificadas pela OTAN, UE e nações.

Fonte: (Nunes, 2016)

[31] Foi acordado um *Technical Arrangement* entre as equipas NCIRC da OTAN e as equipas *Computer Emergency Response Team of the European Union* (CERT-EU), em fevereiro de 2016, aprofundando a cooperação OTAN-UE. (OTAN (r), 2017)

Salienta-se a decisão do CAN em investir na capacidade técnica da NATO *Cyber Range* situada na Estónia. Esta infraestrutura proporciona um ambiente de simulação em tempo real, no qual os operadores podem administrar redes, treinar, e desenvolver TTP, recorrendo a tecnologia de ponta (Vill, 2017).

Ao nível operacional salienta-se o projeto *Malware Information Sharing Platform* (MISP). Este projeto visa assegurar uma deteção atempada de um ciberincidente e de *malware*[32], através da edificação de uma plataforma comum de partilha de informação, que estará acessível para que as nações possam usar essa informação nos seus Sistema de Deteção de Intrusões (OTAN (p), 2014).

Segundo Câmara Assunção esta ferramenta é essencial, pois permite a partilha de informação técnica que possibilita o aviso antecipado. A ligação aos serviços de informações é essencial permitindo corroborar esta informação com a origem dos ataques e as suas intenções (2017).

Quanto à questão de revisão de doutrina, importa abordar a publicação aliada MC 362/1 (catálogo de ROE da OTAN), revendo as diretivas existentes e se for o caso, incluir novas regras. Além disso, importará também atualizar a publicação *Comprehensive Operations Planning Directive* (COPD), permitindo integrar a ciberdefesa na fase de planeamento das operações. Por fim, não existindo doutrina concreta, importará rever e atualizar as publicações constantes na Figura 24, integrando o conceito de ciberdefesa.

[32] Ver Apêndice B.

Doutrina	
	AJP-01 (dezembro 2010) – *Allied Joint Doctrine* # Reconhece as ciber operações como um desafio à segurança da OTAN; # Reconhece as vulnerabilidades e a dependência cada vez maior da OTAN, nas suas estruturas de Comunicações e Informação; # Considera as ciber operações como um subproduto da capacidade defensiva da função conjunta de "*Information Operations*".
	AJP-6 (abril 2011) – *Allied Joint Doctrine for Communication and Information Systems.* # Não contém menções ao ciberespaço ou ciberdefesa.
	AJP-5 (junho 2013) – *Allied Joint doctrine for operational level planning.* # Refere o ciberespaço como um domínio fundamental para o planeamento a exemplo, do ar, mar e terra.
	AJP-3 (Março 2011) – *Allied Joint Doctrine for the Conduct of Operations.* # É inconsistente na integração do ciberespaço como um domínio, colocando-o sob a perspetiva do ambiente da informação.
	AJP-3.10 (novembro 2009) – *Allied Joint Doctrine for Information Operations.* #Utiliza nomenclatura desatualizada como Computer Network Operations (CNO), embora seja a publicação que melhor reflete as atividades no ciberespaço.

Figura 24 – Publicações doutrinárias da OTAN relacionadas com ciberdefesa.

Fonte: (Caton, 2016)

3.3. O papel do Manual de Talin.

Parafraseando Silva Carreira, "*o direito é conservador e anda atrás da vida*" (2017). Esta parece ser a forma como surge o MdT, como uma resposta a ações ofensivas no ciberespaço. Aliás, se nos reportarmos à situação vivida na Estónia, em 2007, podemos afirmar que esta situação terá servido de catalisador para o estudo e desenvolvimento de novos conceitos e, em última análise, do próprio MdT.

De facto, em 2009, um pequeno grupo independente de juristas internacionais encontra-se em Talin para lançar um projeto que visasse identificar as normas e princípios a aplicar a um ciberconflito. O Manual surge na sequência da reunião do grupo de especialistas do *CCD COE*, que em conjunto, e à semelhança de outras iniciativas como o Manual de San Remo[33], produziu o "*Manual de Talin sobre a aplicabilidade do Direito Internacional à ciberguerra*". Não representa as nações que patrocinam o *CCD COE*, nem o centro em si, e não pretende refletir doutrina da Aliança ou de qualquer Estado membro.

[33] No original: "*San Remo Manual on International Law applicable to armed conflicts at Sea*".

O MdT divide-se em duas partes: i) Direito Internacional sobre cibersegurança; ii) Direito sobre ciberconflitos armados. No total compreende 95 regras a "tinta negra" e respetivos comentários.

O Manual centra-se no enquadramento legal das questões que governam o ciberconflito e, em si constitui apenas uma organização e clarificação de ideias, não sendo possível considerá-lo como um primeiro passo para uma convenção sobre o ciberespaço. Assume essencialmente, um papel de aglutinação e normalização dos termos e conceitos usados, podendo nesse âmbito auxiliar a padronizar a linguagem. Como defende Silva Carreira, "*o Manual em si não traz novidade*" (2017).

No entanto, apesar de não se poder considerar um primeiro passo para uma convenção, ou como doutrina da OTAN, na verdade, o MdT constitui-se como referência usada pelos juristas militares nos treinos e exercícios de ciberdefesa, assumindo um carácter atual e relevante. (Esteves, 2016)

3.4. Síntese conclusiva.

Neste último capítulo, foi analisada a evolução da posição da OTAN relativamente ao ciberespaço, recorrendo a uma análise de conteúdo das declarações das cimeiras da Aliança, realizadas entre 2002 e 2016. Do tratamento estatístico dessa análise, foi possível inferir que a evolução tem sido sistemática e ponderada, de forma a que não se coloque em causa a legitimidade moral da Aliança. Infere-se também que a Aliança tem assumido uma postura reativa aos eventos.

São inúmeros os desafios com que se depara a OTAN na sua relação com o ciberespaço. Ao reconhecê-lo como um domínio, a Aliança procura dar resposta a esses desafios no plano político, jurídico e estratégico-operacional. Essas respostas passarão por maior cooperação entre as nações, procurando cumprir as metas acordadas no CC.

No plano político, importa continuar a aprofundar a coesão e confiança entre aliados, investindo também na sua relação com a UE, de forma a fomentar eficácia, e partilha de conhecimento e informação. No plano jurídico, a Aliança deverá resguardar a sua posição de OI de estatuto moral elevado, preservando a sua posição relativamente à aplicabilidade do DI nas operações que desenvolva no ciberespaço.

A OTAN desenvolve dois projetos importantes que contribuirão para alcançar os objetivos da estratégia genética que são o MN CD2 e o MN CD E&T.

No patamar operacional, salientam-se o desenvolvimento do projeto MISP, a necessidade de revisão de doutrina, o desenvolvimento do conhecimento situacional na ciberdefesa e o investimento na ligação com os serviços de informação.

Por último, não sendo o MdT doutrina da OTAN, serve como referência legal durante os exercícios como o *Cyber Coalition*.

Assim, conclui-se que a terceira hipótese se verifica totalmente**,** dando resposta à QD3 (Figura 25).

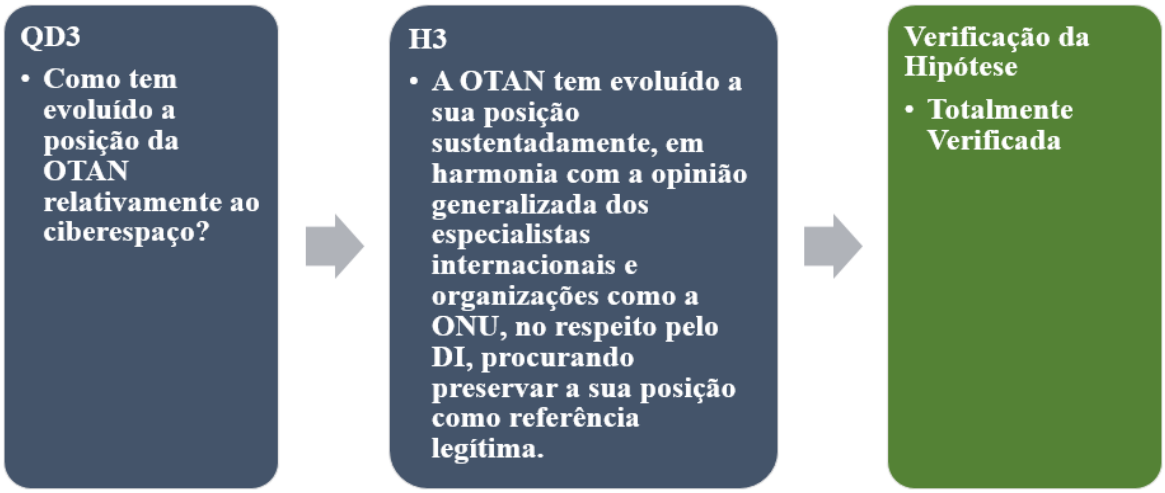


Figura 25 – Verificação da H3.

Fonte: (O autor, 2017)

Conclusões.

Esta investigação assentou numa estratégia qualitativa que permitiu desenvolver um estudo de caso, tendo por objeto, *a aplicabilidade do DCA no ciberespaço*.

O estudo desenvolveu-se em torno da seguinte questão central (QC): "*Como tem evoluído a posição da Aliança Atlântica relativamente à aplicabilidade do DCA no ciberespaço?*"

O percurso metodológico iniciou-se pela exploração bibliográfica, com o objetivo de alcançar o conhecimento do 'estado da arte', complementando-se essa exploração, com a realização de entrevistas exploratórias a peritos na matéria. Estas entrevistas permitiram cimentar conhecimentos e consolidar as respostas às QD, e consequentemente, à QC.

No primeiro capítulo concluiu-se que os princípios e as normas que se aplicam ao ciberespaço num conflito armado são os mesmos que se aplicam aos restantes domínios operacionais. Ficou também patente que existe uma dicotomia entre aquilo que será o espetro das dimensões de cibersegurança e de ciberdefesa e, consequentemente, entre o direito de fazer a guerra e o direito na guerra.

Na OTAN, a qualificação de um ciberataque como um AA, será sempre uma decisão política a tomar pelo CAN. No entanto, essa decisão poderá ser fundamentada num modelo de qualificação baseado na avaliação dos seus efeitos. Além disso foi possível identificar a complexidade na atribuição de um ataque e consequente atuação em LD. Esta complexidade poderá ser esbatida, se existir uma cooperação com os serviços de informações, que permita corroborar as conclusões alcançadas na análise forense dos indícios atinentes a um ciberataque.

Considera-se assim respondida a QD1 e validada totalmente a hipótese H1, ou seja, quando ocorra um ciberataque num contexto de conflito armado, essas ações submetem-se ao DCA.

No segundo capítulo, foi possível concluir que a OTAN tem uma PCD alicerçada nos seguintes pilares: i) A Aliança defenderá as suas redes; ii) As nações aliadas defenderão os seus próprios sistemas e infraestruturas; iii) Com base no principio da solidariedade, a Aliança poderá prestar assistência a um Aliado vítima de um ciberataque sério.

Esta política tem acompanhado os trabalhos desenvolvidos por outras OI, em particular a ONU, UE e OSCE, pois o resultado que daí advirá terá implicações na ReG do ciberespaço, e consequentemente na estratégia genética, estrutural e operacional da Aliança, na busca continuada pela edificação da capacidade de ciberdefesa. Além disso,

como OI alicerçada na defesa dos princípios do DI, apresenta-se como referência moral relativamente aos países não-OTAN, que veem no ciberespaço um veículo de transmissão de ideologia contrária à sobrevivência dos seus regimes autoritários. Esta posição tem sido contrariada pelo trabalho do GPG, que tenta ganhar tempo evitando a votação de um instrumento legal que restringirá os primados Humanista, Democrático e de Direito.

Também se demonstrou que, perante um ciberataque, existirá algum benefício em manter ambiguidade e flexibilidade no que concerne à tomada de posição da Aliança e na possibilidade do CAN invocar o artigo 5º do TAN. A avaliação da situação ocorrerá caso a caso, e após a solicitação de consulta pela Parte afetada. Este instrumento mantém-se relevante e dissuasor.

Por fim explorou-se o CC, que, alicerçado no artigo 3º do TAN, salienta que: i) O investimento na edificação das capacidades de ciberdefesa nacionais, compatíveis com a OTAN e com os restantes aliados, é uma responsabilidade individual, evitando assim, o cenário de elo mais fraco; ii) A promoção da partilha de informação, do treino e da formação, reforçando as competências, sensibilização e a compreensão das ameaças cibernéticas, é essencial para a prossecução dos objetivos da ECDP.

Assim verifica-se na totalidade a H2, respondendo à QD2, ou seja, em caso de ciberataque, o CAN irá analisar todas as evidências e consequências e determinar a invocação do artigo 5º numa análise caso a caso.

No terceiro e último capítulo, foi analisada a evolução da posição da OTAN relativamente ao ciberespaço, recorrendo a uma análise de conteúdo das declarações das cimeiras da Aliança, realizadas entre 2002 e 2016. Do tratamento estatístico dessa análise, foi possível inferir que a evolução tem sido sistemática e ponderada, de forma a não ferir a legitimidade moral da Aliança, objetivo estratégico vital a preservar. Infere-se também, que a Aliança tem assumido uma postura reativa aos eventos, observando-se picos evolutivos após ciberataques e de desenvolvimentos normativos, como é o caso da publicação do MdT em 2013.

A OTAN não se encontrava obrigada a reconhecer o ciberespaço como um domínio, no entanto, ao decidir fazê-lo, transmitiu uma mensagem estratégica, interna e externamente. A Aliança encontra-se atenta e em evolução, de forma a responder aos inúmeros desafios com que se depara nos planos político, jurídico e estratégico-operacional.

No plano político, importa continuar a aprofundar a coesão e confiança entre aliados, enquanto no plano jurídico, a Aliança deverá resguardar a sua posição, tendo por critério o respeito estrito à aplicabilidade do DI nas ciberoperações.

Conclui-se, também, que projetos como o MN CD2 e o MN CD E&T contribuirão para alcançar os objetivos da estratégia Genética e Estrutural, colmatando lacunas na edificação da capacidade de ciberdefesa e na formação e treino.

No patamar operacional, salientam-se o desenvolvimento do projeto MISP, a necessidade de revisão de doutrina, o desenvolvimento do conhecimento situacional na ciberdefesa e o investimento na ligação com os serviços de informação.

Por último, o MdT, não sendo doutrina da Aliança Atlântica, serve como referência legal para a prática dos exercícios da OTAN como o *Cyber Coalition*, bem como para apoiar o desenvolvimento da PCD da OTAN.

Assim, conclui-se que a H3 se verifica totalmente, dando resposta à QD3**,** ou seja, a OTAN tem evoluído a sua posição sustentadamente e ponderadamente, procurando preservar a sua posição como organização que respeita integralmente o DI, incluindo no domínio da ciberdefesa.

Alcançada a fase da verificação, conclui-se que as três hipóteses colocadas foram totalmente verificadas, o que permite dar resposta à questão central:

A OTAN tem evoluído de forma sustentada e ponderada a sua posição relativamente à aplicabilidade do DI em geral e do DCA, em particular, no ciberespaço. Para a Aliança, o DCA aplica-se categoricamente a um ciberataque que ocorra no contexto de um conflito armado, conforme afirmado pelos CEeG na Cimeira de Gales. Esta evolução tem sido reativa aos eventos nos últimos 14 anos, focando-se na consolidação de uma PCD comum e na edificação de capacidades que permitam uma defesa eficaz. Essa edificação sofreu um impulso com a aprovação do CC. O alcançar das metas nele definidas permitirá dar resposta aos desafios estratégicos com que a Aliança se depara.

A delimitação do objeto de estudo constituiu uma limitação à investigação. Na realidade a sinopse demonstrou ser demasiado abrangente não contribuindo para uma delimitação do problema de investigação. A extensão de literatura (sobretudo americana) sobre este assunto, não sendo uma limitação, acabou por constituir um desafio.

Desta forma consideram-se alcançados os OE e OG desta investigação, salientando como principais recomendações as seguintes:

1. Incluir um embaixador para a ciberdiplomacia junto do GPG, permitindo acompanhar o desenvolvimento dos trabalhos aí desenvolvidos;

2. Desenvolver um catálogo de capacidades, valências e perícias disponibilizadas pela OTAN aos aliados, para uso imediato em caso de ciberataque;
3. Rever o catálogo de regras de empenhamento da OTAN (MC 362/1), de forma a rever e incluir ROE que se apliquem especificamente a um ciberconflito;
4. Investir na revisão da doutrina que permita uma maior integração do conceito de ciberdefesa nos processos de planeamento e execução de operações, nomeadamente revendo a publicação COPD;
5. Definir um modelo consensual de qualificação de um ciberataque;

Por último, sugere-se que em futuras investigações sobre esta temática, se desenvolva com maior pormenor, o Modelo de Qualificação de um ciberataque, de forma a alcançar parâmetros que habilitem uma melhor tomada de decisão sobre o tipo de resposta a dar em face da gravidade do ataque.

Termina-se este estudo citando o Secretário Geral da OTAN, Jens Stoltenberg, que muito a propósito proferiu a seguinte declaração:

"*NATO is founded on the shared values of liberty, democracy, human rights and the rule of law. That is why we are determined to ensure that cyberspace remains the place for peaceful, open communication and debate that we all need it to be.*" (Stoltenberg, 2016)

Bibliografia

Addicott, J.F., 2010. Cyberterrorism: Legal Policy Issues. Em J. Moore e F. Turner, eds. *Legal Issues in the Struggle*. Durham, NC: Carolina Academic. p.550.

Assunção, C., 2017. *Entrevista ao CTEN EN-AEL Câmara Assunção* [Entrevista]. Restelo, Belém (20 janeiro).

Atlantic Council, 2014. *NATO in a era of Global Competition*. Washington, DC 20005.

Barlow, J.P., 1996. *Electronic Frontier Foundation*. [Em linha] Disponível em: https://www.eff.org/cyberspace-independence [Consult. 01 março 2017].

Carreira, J.M.S., 2004. *O Direito Humanitário, as regras de empenhamento e a condução das operações militares*. Lisboa: Comissão Cultural da Marinha.

Carreira, V.R.J.M.S., 2017. *Entrevista exploratória* [Entrevista]. Pedrouços (06 janeiro).

Caton, J.L., 2016. *NATO CYyberspace capability: a strategic and operational evolution.* Ashburn Drive, Carlisle, PA 17013-5010: U.S. Army War College Press Strategic Studies Institute.

Davis, J., 2007. Hackers take down the most wired country in Europe. *Wired*, Disponível em: https://www.wired.com/2007/08/ff-estonia/?currentPage=all [Consult. 15 janeiro 2017].

DAY, J.A., 2016. *NATO'S NEW DETERRENCE POSTURE: FROM WALES TO WARSAW*. GENERAL REPORT. NATO Parliamentary Assembly.

Deyra, M., 2001. Comissão Nacional para as Comemorações do 50.o Aniversário da Declaração Universal dos Direitos do Homem e Década das Nações Unidas para a Educação em matéria de Direitos Humanos.

Dicionário infopédia da Língua Portuguesa sem Acordo Ortográfico, 2003-2017. *www.infopedia.pt*. [Em linha] Porto: Porto Editora Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa-aao/inconveniente.

Editora, Porto, 2003-2016. *www.infopedia.pt*. [Em linha] Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/ciberespaço [Consult. 04 dezembro 2016].

Esteves, S.P., 2016. *Jurista Marinha Portuguesa* [Entrevista]. (21 dezembro).

Fernandes, J.P.T., 2012. A ciberguerra como nova dimensão dos conflitos do século XXI. *Relações Internacionais*, Março. pp.053-69.

Fernandes, H., 2016. As Novas Guerras: O Desafio da Guerra Híbrida. *Revista de Ciências Militares*, novembro. pp.13-40. Disponível em:

http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes. [Consult. 25 abril 2017].

Gjelten, T., 2010. *World Affairs*. [Em linha] Disponível em: http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament [Consult. 01 março 2017].

GPG, 2015. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Nova Iorque.

Graça, P.J.B., 2013. *O Ciberataque como Guerra de Guerrilha. O Caso dos Ataques DoS/DDoS à Estónia, Geórgia e ao Google - China*. Lisboa: Universidade de Lisboa - ISCSP.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Nova Iorque: Assembleia Geral das Nações Unidas.

Guerra, I.C., 2006. *Pesquisa Qualitativa e Análise do Conteúdo - Sentidos e formas de uso*. 1ª ed. Cascais: Principía Editora, Lda.

Healey, J. e Jordan, K.T., 2014. *NATO's Cyber Capabilities: Yesterday,Today, and Tomorrow.* Issue Brief. Brent Scowcroft Center on International Security.

Herzog, S., 2011. *Journal of Strategic Security*. [Em linha] Disponível em: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss [Consult. 22 março 2017].

HM Government, 2015. *www.gov.uk*. [Em linha] Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf [Consult. 04 dezembro 2016].

Homesec, 2016. *NATO's largest cyber defence exercise, Cyber Coalition 2016*. [Em linha] Disponível em: http://www.homsec.es/natos-largest-cyber-defence-exercise-cyber-coalition-2016-wrapped-up-in-estonia-on-friday-2-december-2016/ [Consult. 12 fevereiro 2017].

Hutson, P., 2014. Cyber Defence in operations. *The Three Swords Magazine*, pp.35-39. Disponível em: http://www.jwc.nato.int/images/stories/threeswords/cyber_def_review.pdf [Consult. 22 janeiro 2017].

IESM, 2012. *NEP / ACA - 018 - Regras de apresentação e referenciação para os trabalhos escritos a realizar no IESM*. Pedrouços: IESM.

IESM, 2013. *NEP / ACA - 010 - TRABALHOS DE INVESTIGAÇÃO*. Pedrouços: IESM.

Jr, C.J.D., 2011. Perspectives for Cyber Strategists on Law of Cyberwarfare. *Strategic Studies Quarterly*, pp.81-99.

Kolb, R. e Hyde, R., 2008. *An introduction to the International Law of Armed Conflicts*. Oxford-Portlland: Hart Publishing.

Lewis, J.A., 2015. *The Role of Offensive Cyber Operations in NATO's Collective Defence*. THE TALLINN PAPERS. Talin: CCDCOE.

Lifländer, C.-M., 2017. *Conferência Ciberdefesa: O desafio do século XXI*. Lisboa: Comissão de Defesa Nacional.

Machi, V., 2017. Private Sector Plays Bigger Role in NATO Cyber Strategy. *National Defense*, fevereiro. pp.30-31.

McCoubrey, H. e White, N.D., 1992. *International Law and Armed Conflict*. Aldershot: Darmouth Publishing Company Limited.

MDN, 2017. Cyber Pooling & Sharing and Smart Defence Academia, Industry and EU-NATO Cooperation. Em *3rd NATO Cyber Defence Smart Defence Projects' (CD SDP) Conference*. Lisboa, 2017.

Melo, P.J.P.d., 2011. *A Ciberguerra. Estrutura Nacional para enfrentar as vulnerabilidades – uma capacidade militar autónoma ou partilhada*. Pedrouços, Portugal: IESM.

Mesic et al., 2010. *Air Force Cyber Command (Provisional) Decision Support*. Santa Monica, Califórnia: RAND Corporation.

Microsoft, s.d. *Microsoft - Central de Proteção e Segurança*. [Em linha] Disponível em: https://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx [Consult. 14 fevereiro 2017].

Monteiro, L.S. e Pinto, S.S., 2016. Strategia nº 21 - Ciberespaço. *Revista da Armada*, abril. pp.4-5.

Moreira, J.M.D., 2012. O impacto do ciberespaço como nova dimensão nos conflitos. *Boletim Ensino - Instituto Universitário Militar*, novembro. pp.27-50.

NCIA, s.d. *Multinational MN CD2 - Cyber Defence Capability Development*.

Neves, P.J.B.d., 2015. *Capacidade de resposta a incidentes de segurança da informação no ciberespaço. Uma abordagem DOTMLPI-I*. Lisboa.

NIST, 2013. *Security and Privacy Controls for Federal Information Systems and Organizations.* Reports on Computer Systems Technology. Nova Iorque: U.S. Department of Commerce.

NSA, 2012. *AAP-06 NATO Glossary of Terms and Definitions*. 2ª ed. Bruxelas: NSA.

Nunes, P.V., 2016. NATO MultiNational Smart Defence Project on Cyber Defence Education & Training. Em *2nd CD SDP Conference*. Lisboa, 2016.

ONU (a), 2015. *Relatório sobre os Objetivos*. Nova Iorque: ONU.

ONU (b), 1945. *UNITED NATIONS*. [Em linha] Disponível em: http://www.un.org/en/sections/un-charter/chapter-i/index.html [Consult. 30 janeiro 2017].

ONU (c), 1975. *Resolução 3314 da Assembleia Geral sobre a Definição de Agressão*. Nova Iorque.

OTAN (a), 2016. *Cyber Defence Pledge*. [Em linha] Bruxelas Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133177.htm [Consult. 13 dezembro 2016].

OTAN (b), 2011. *Defending the networks - The NATO Policy on Cyber Defence*. Bruxelas, Bélgica: Nato Graphics & Priting.

OTAN (c), 2016. *Warsaw Summit Communiqué*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en [Consult. 04 dezembro 2016].

OTAN (d), 2017. *NATO - Cyber Defence*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/topics_78170.htm# [Consult. 29 abril 2017].

OTAN (e), 2010. *Strategic Concept - for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Lisboa.

OTAN (f), 1949. *Tratado do Atlântico Norte*. Washington.

OTAN (g), 2002. *Prague Summit Declaration*. [Em linha] Disponível em: http://www.nato.int/docu/pr/2002/p02127e.htm [Consult. 11 dezembro 2016].

OTAN (h), 2004. *Istanbul Summit Communiqué*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_21023.htm [Consult. 23 janeiro 2017].

OTAN (i), 2006. *Riga Summit Declaration*. [Em linha] Disponível em: http://www.nato.int/docu/pr/2006/p06-150e.htm [Consult. 15 janeiro 2017].

OTAN (j), 2008. *Bucharest Summit Declaration*. [Em linha] Disponível em: http://www.nato.int/cps/en/natolive/official_texts_8443.htm [Consult. 12 dezembro 2016].

OTAN (k), 2009. *Strasbourg / Kehl Summit Declaration*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/news_52837.htm?mode=pressrelease [Consult. 06 março 2017].

OTAN (l), 2010. *Lisbon Summit Declaration*. [Em linha] Disponível em: http://www.nato.int/cps/en/natolive/official_texts_68828.htm [Consult. 06 dezembro 2016].

OTAN (m), 2012. *Chicago Summit Declaration*. [Em linha] Chicago: NATO Disponível em: http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en [Consult. 12 fevereiro 2017].

OTAN (n), 2014. *Wales Summit Declaration*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_112964.htm [Consult. 28 dezembro 2016].

OTAN (n), 2016. *Operations Policy Committee*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/topics_69312.htm [Consult. 10 janeiro 2017].

OTAN (o), 2016. *Warsaw Summit Communiqué*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en [Consult. 28 dezembro 2016].

OTAN (p), 2014. *Multinational Projects*. Bruxelas.

OTAN (q), 2011. *NATO Countering the Hybrid Threat*. Norfolk: ACT.

OTAN (r), 2017. *NATO Multimedia Library*. [Em linha] OTAN Disponível em: http://www.natolibguides.info/cybersecurity [Consult. 20 maio 2017].

Quivy, R. e Campenhoudt, L.V., 2005. *Manual de investigação em Ciências Sociais*. 4ª ed. Lisboa: Gradiva.

Ranger, S., 2014. *NATO updates cyber defence policy as digital attacks become a standard part of conflict*. [Em linha] Disponível em: http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/ [Consult. 29 abril 2017].

Ravindranath, M., 2014. Panetta: Cyberspace is "battlefield of the future". *The Washington Post*, 12 março.

Robinson, N., 2016. NATO: changing gear on cyber defence. *Nato Review Magazine*.

Schmitt, M.N., 2010. Cyber Operations in International Law:The Use of Force, Collective Security,Self-Defense, and Armed Conflicts. Em Policy, C.o.D.C.I.S.a.D.O.f.U.S. *Proceedings of a Workshop on deterring cyberattacks*. Washington, DC 20001, EUA: National Academy of Sciences. pp.151-78.

Schmitt, M.N., 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, United States: Cambridge University Press.

Schmitt, M.N. et al., 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, United States: Cambridge University Press.

Sklerov, M.J., 2009. Solving the Dilemma of State Response to Cyberattacks: A Justification. *Military Law Review*, pp.1-85. Disponível em: https://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/201-fall-2009.pdf [Consult. 2017 abril 12].

Sousa, L.B.d., 2017. *Entrevista ao Embaixador para a Ciberdiplomacia* [Entrevista]. (15 fevereiro).

Stoltenberg, J., 2016. *NATO and Cyber: Time to Raise our Game*.

Stoltenberg, J., 2016. *NATO and Cyber: Time to Raise our Game*. [Em linha] Disponível em: http://www.defensenews.com [Consult. 14 junho 2017].

The White House, 2015. *www.whitehouse.gov*. [Em linha] The White House Disponível em: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf [Consult. 04 dezembro 2016].

TIJ, 1986. *Case concerning military and paramilitary activities in and against Nicaragua.* Reports of Judgments. Advisory opinions and orders. Tribunal Internacional de Justiça.

TPI, 1998. *Rome Statute of the International Criminal Court*. Roma.

Traynor, I., 2007. Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, Disponível em: https://www.theguardian.com/world/2007/may/17/topstories3.russia [Consult. 15 janeiro 2017].

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

Vill, M., 2017. *Guardtime. Blogs and News.* [Em linha] Disponível em: https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range [Consult. 27 março 2017].

Wikipedia, 2017. *List of cyberattacks*. [Em linha] Disponível em: https://en.wikipedia.org/wiki/List_of_cyberattacks [Consult. 03 junho 2017].

Wingfield, T., 2009. International law and information operations. Em *Cyberpower and national security*. pp.525-42.

Anexo A — Lista de fontes do Direito dos Conflitos Armados.

Tabela 5 – Fontes do DCA

Fonte	Título	Data	N.º de Artigos
Convenção de Genebra	Melhoria das condições dos feridos no campo de Batalha.	1864	10
II Conferência de Haia	Leis e Costumes da Guerra em Terra.	1899	60 (55 em anexo)
IV Conferência de Haia	Leis e Costumes da Guerra em Terra.	1907	64 (56 em anexo)
I Convenção de Genebra	Para Melhoria das Condições dos Feridos e Doentes das Forças Armadas no Terreno	1864 [revista em 1949]	77 (13 em anexo)
II Convenção de Genebra	Para Melhoria das Condições dos Feridos, Doentes e Náufragos das Forças Armadas no Mar	1949	63
III Convenção de Genebra	Relativa ao Tratamento dos Prisioneiros de Guerra	1929 [revista em 1949]	143
IV Convenção de Genebra	Relativa à Proteção de Civis em Tempo de Guerra	1949	180 (21 em anexo)
Protocolo I	Relativa à Proteção das Vítimas de Conflitos Armados Internacionais (amplia a definição dos mesmos às guerras de libertação nacional)	1977	102
Protocolo II	Relativa à Proteção das Vítimas de Conflitos Armados Não Internacionais (completa o artigo 3 comum às quatro convenções de genebra)	1977	28
Protocolo III	Relativa à Adoção de um Emblema Adicional Distintivo	2005	17

Fonte: (Fernandes, 2012)

Anexo B — O caso da Estónia.

Em 2007, o Governo da Estónia decide remover uma estátua de bronze (Figura 26), erigida em 1947 pelos soviéticos para comemorar os seus mortos em combate depois de terem expulsado as tropas alemãs no final da Segunda Guerra Mundial. Para os Estónios, esta estátua representava a ocupação soviética (Graça, 2013, pp.29-32).

Figura 26 – Estátua soviética.

Fonte: (Traynor, 2007)

Esta remoção serviu de catalisador para uma série de ataques que paralisaram a Estónia durante três semanas (Traynor, 2007). Os ataques começaram no dia 7 de abril e afetaram sites de variadas instituições e organizações estónias, tais como: o Parlamento estónio, Ministérios, redações de jornais, os principais bancos comerciais, empresas de telecomunicações e servidores de DNS, paralisando a quase totalidade dos serviços via internet (Graça, 2013, pp.29-32).

Em 2007, 49% da população lia diariamente o jornal online e, mais de 90% das transações bancárias eram feitas pela internet na Estónia, ao ponto de esta ser alcunhada de e-Stonia (Graça, 2013, pp.29-32).

Alguns dos ataques foram de *Distributed Denial of Service* (DDoS), com recurso a centenas máquinas comprometidas, situadas na FR, EUA, Europa ocidental e, Irão, o que impossibilitou a atribuição do ataque. Como alguns dos ataques partiram da FR, o Ministro dos Negócios Estrangeiros estónio acusou a administração russa. No entanto, a FR negou que estivesse por detrás dos ataques (Graça, 2013, pp.29-32).

A 6 de setembro de 2007 o ministro da Defesa estónio admitiu que não tinha provas que ligassem os ataques às autoridades russas (Graça, 2013, pp.29-32).

Apêndice A — Mapa Concetual da Investigação

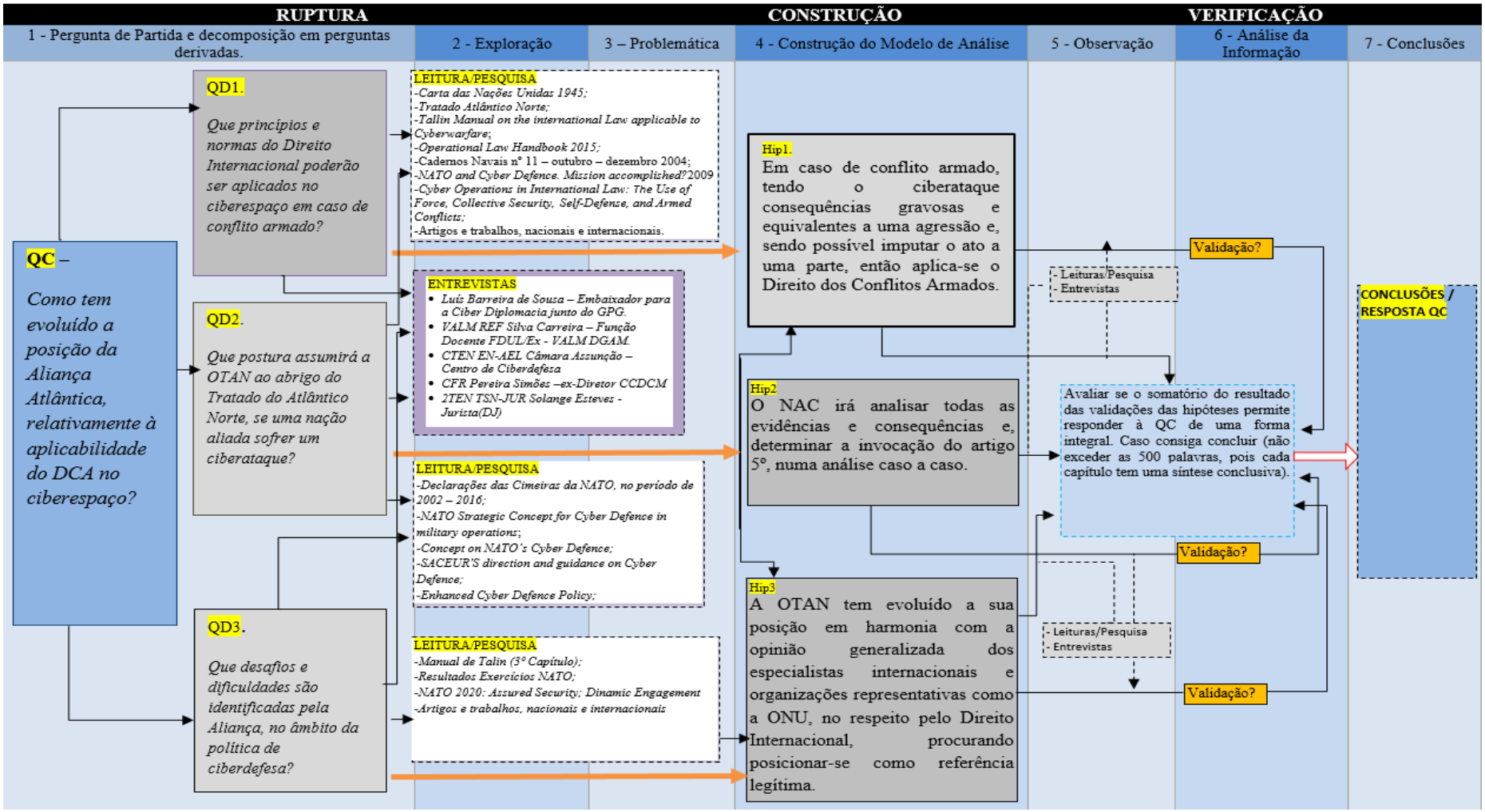


Figura 27 – Mapa Concetual da Investigação.

Fonte: (O autor, 2017)

Apêndice B — Corpo de conceitos

Agressão	Para o efeito de referência neste trabalho a definição de agressão é a que consta no artigo 1º, da Resolução da Assembleia Geral das Nações Unidas de 1975, e que se transcreve: "*A agressão é o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, ou de qualquer forma incompatível com a Carta das Nações Unidas, tal como decorre da presente definição*." (ONU (c), 1975)
Ataque Armado	Para o efeito de referência neste trabalho, um ataque armado consiste "*num ato, com grande amplitude, gravidade e escala, praticado utilizando quaisquer instrumentos ou dispositivos que tenha consequências e provoque efeitos violentos no adversário, ainda que os instrumentos ou dispositivos usados não tenham normalmente essa finalidade*." (Moreira, 2012, p.39)
Ciberataque	Um ciberataque é uma operação ofensiva ou defensiva no ciberespaço, da qual é razoável esperar que provoque ferimentos ou morte a pessoas e/ou, danos ou destruição a objetos (Schmitt et al., 2013, p.106).
Ciberdefesa	Os meios para alcançar e executar medidas defensivas para reagir contra ciberataques e mitigar os seus efeitos, preservando e restaurando a segurança das comunicações, da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas (Neves, 2015).
Ciberespaço	De acordo com o manual de Talin, trata-se do ambiente formado por componentes físicos e não físicos, caracterizado pelo uso de computadores e do espectro eletromagnético, para armazenar, modificar e trocar dados usando redes de computadores (Schmitt et al., 2013).
Ciberguerra	Ciberguerra é a palavra que é "*formada pelas palavras (ciber+guerra), sendo que a primeira é oriunda do grego, cibernética, ("kybernetiké, a arte de governar). Atualmente existe um desvio do significado original da palavra grega, e podemos inferir que a ciberguerra é a guerra no ciberespaço*." (Melo, 2011, p.1);
Cibersegurança	Estratégia, política e normas com vista à segurança das operações no ciberespaço, abrangendo missões de redução da ameaça, de vulnerabilidades, de compromisso internacional, de resposta a incidentes, resiliência, e políticas de recuperação, incluído operações em rede, garantia da informação, ações judiciais, diplomáticas, militares e de inteligência relacionadas com a segurança e estabilidade da infraestrutura global de informação e Comunicações (Neves, 2015).
Cláusula de Martens	"*Em virtude de qualquer codificação ser por natureza incompleta – por não ser possível prever todas as situações num determinado momento – apresenta uma dupla vantagem, já que: rejeita primeiramente a ideia de que tudo o que não é expressamente proibido pelos tratados aplicáveis é autorizado e em segundo lugar torna aplicáveis os princípios proclamados, independentemente da ulterior evolução das situações."* (Deyra, 2001, pp.23-24)
Deterrence	Convencer um potencial agressor de que as consequências da coerção ou do conflito armado, superam os ganhos potenciais. Isto exige a manutenção de uma capacidade e estratégia militar credíveis, consonantes com a clara vontade política de agir (NSA, 2012).

Guerra Hibrida	Não existindo uma definição concreta, para efeitos desta investigação considere-se a seguinte*: as ameaças híbridas são usadas pelos adversários, que possuam a capacidade de empregar simultaneamente meios convencionais e não convencionais, de forma adaptativa na busca de seus objetivos* (OTAN (q), 2011)
Information War	*Confrontação entre dois ou mais estados no espaço da informação, com o propósito de subverter politicamente, economicamente e socialmente os povos, através de psicologia de massas, ou através de lavagem cerebral, de forma a destabilizar a sociedade e os estados. A disseminação de informação prejudicial às esferas espiritual, cultural e moral de outras nações, é uma ameaça à estabilidade desses países*. (Gjelten, 2010)
Legítima Defesa	Para o efeito de referência neste trabalho a definição de legítima defesa é aquela que é conforme à alínea c), do n.º 1, do artigo 31º, do Estatuto do Tribunal Penal Internacional: "*The person acts reasonably to defend himself or herself or another person or, in the case of war crimes, property which is essential for the survival of the person or another person or property which is essential for accomplishing a military mission, against an imminent and unlawful use of force in a manner proportionate to the degree of danger to the person or the other person or property protected. The fact that the person was involved in a defensive operation conducted by forces shall not in itself constitute a ground for excluding criminal responsibility under this subparagraph*;" (TPI, 1998)
Malware	*Software* ou *firmware* que se destina a executar processos não autorizados que terão um impacto adverso na confidencialidade, integridade, ou disponibilidade num Sistema de Informação. Um vírus, um *worm*, ou outra estrutura de código que infete uma máquina. *Spyware* e algumas formas de *adware* são exemplos de código malicioso (NIST, 2013)

Apêndice C — Estrutura de Cibergovernação da OTAN.

O CDC é o principal órgão subordinado ao NAC para a definição da politica de ciberdefesa. Além disso, o comité providencia supervisão e aconselhamento às nações aliadas, nos seus esforços para edificar um nível de perícia que se coadune com a política definida (OTAN (d), 2017).

Ao nível de implementação da política e da organização da Aliança, surge o *Cyber Defence Management Board* (CDMB), que é o órgão responsável por coordenar a ciberdefesa através das estruturas civis e militares da Aliança. Este órgão compreende os responsáveis políticos, militares, operacionais e técnicos dos órgãos internos da OTAN com responsabilidades na ciberdefesa (OTAN (d), 2017).

O *NATO Consultation, Command and Control Board* (C3B) é o principal órgão de consultoria técnica e de implementação das diretivas técnicas, tácitas e de procedimentos(TTP) para a ciberdefesa (OTAN (d), 2017).

O OPC é o comité responsável por liderar a operacionalização da política de ciberdefesa no decurso de uma crise e pelo planeamento da gestão da crise. (OTAN (n), 2016)

Quanto às responsabilidades específicas para a identificação dos requisitos operacionais, para a aquisição, implementação e operacionalização das capacidades de ciberdefesa, estas são repartidas entre as *NATO Military Authorities* (NMA) e a *NATO Communications and Information Agency* (NCIA) (OTAN (d), 2017).

A NCIA é responsável pela prestação dos serviços técnicos de ciberdefesa em toda a estrutura da Aliança. Este papel é delegado no *Technical Centre* da *NATO Computer Incident Response Capability* (NCIRC). Este centro tem um papel fundamental em responder a uma agressão contra a Aliança. Além de responder a incidentes, o centro produz relatórios e dissemina essa informação para os administradores, gestores e utilizadores das redes (OTAN (d), 2017).

Por outro lado, dentro do NCIRC, existe um *Coordination Centre* que atua como um elemento de estado-maior, responsável por coordenar as atividades de ciberdefesa internamente, e em conjunto com as nações. Este elemento atua em apoio ao CDMB. (OTAN (d), 2017)

Ao nível do planeamento de exercícios e consequente recolha de lições aprendidas, o *Allied Command Transformation* (ACT) é o responsável por planear e conduzir anualmente, o exercício *Cyber Coalition*. (OTAN (d), 2017)

Apêndice D — Análise de Conteúdo da evolução da posição da OTAN no ciberespaço.

Tabela 6 – Análise do conteúdo das Cimeiras da NATO.

Documento	Referência	Indicadores (ADMP)	Quantificação			
			A	**D**	**M**	**P**
Comunicado da Cimeira da OTAN em Praga — 2002	(OTAN (g), 2002) Parágrafo 4 Alínea F.	**Ameaça:** "*Cyber-attacks"* **Direito**: — **Medidas**: "*Strengthen Cyber Defense Capabilities"* **Política: -**	1	0	1	0
Comunicado da Cimeira da OTAN em Istambul — 2004	(OTAN (h), 2004)	**Ameaça:** — **Direito:** — **Medidas:** — **Política:** —	0	0	0	0
Comunicado da Cimeira da OTAN em Riga — 2006	(OTAN (i), 2006) Parágrafo 24	**Ameaça:** — **Direito:** — **Medidas:** "*work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber-attack*" **Política:** —	0	0	1	0
Comunicado da Cimeira da OTAN em Bucareste — 2008	(OTAN (j), 2008, p.11) Parágrafo 47	**Ameaça:** "*Cyber-attacks"* **Direito:** — **Medidas**: "*Strengthening Alliance information systems;* • *protect key information systems in accordance with ally's respective responsibilities;* • *Share best practices;* • *provide a capability to assist Allied nations, upon request, to counter a cyber-attack"* **Política:** *Policy on Cyber Defence; Linkage between NATO and national authorities*	1	0	4	1

Comunicado da Cimeira de Estrasburgo/Khel — 2009	(OTAN (k), 2009) Parágrafo 49	**Ameaça:** "*state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems;*" **Direito: —** **Medidas:** "*strengthening communication and information systems that are of critical importance to the Alliance against cyber-attacks;* • *improved the existing Computer Incident Response Capability* • *activated the **Cooperative Cyber Defence Centre of Excellence*** • *accelerate our cyber defence capabilities* • *Cyber defence is being made an integral part of NATO exercises*" **Política:** "*Policy on Cyber Defence;* • *NATO Cyber Defence Management Authority* • *strengthening the linkages between NATO and Partner countries* • *framework for cooperation on cyber defence between NATO and Partner countries* • *acknowledge the need to cooperate with international organisations, as appropriate*"	**A** 1	**D** 0	**M** 5	**P** 5
Comunicado da Cimeira da OTAN em Lisboa — 2010	(OTAN (l), 2010) Parágrafo 2 Parágrafo 40	**Ameaça:** "*Cyber threats are rapidly increasing and evolving in sophistication.*" **Direito: —** **Medidas:** "*enhance our cyber defence capabilities* • *improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber-attack*" **Política:** "*take into account the cyber dimension of modern conflicts in NATO's doctrine* *we will work closely with other actors, such as the UN and the EU, as agreed*"	**A** 1	**D** 0	**M** 2	**P** 2
Comunicado da Cimeira da OTAN em Chicago — 2012	(OTAN (m), 2012, p.12) Parágrafo 49	**Ameaça:** "*Cyber-attacks continue to increase significantly in number and evolve in sophistication and complexity*" **Direito: —** **Medidas:** "*critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC)* • *NATO bodies under centralised cyber protection* • *further integrate cyber defence measures into Alliance structures and procedures* • *identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability*" **Política:** "*adopted a Cyber Defence Concept, Policy, and Action Plan* • *we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation.* • *full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia*"	**A** 1	**D** 0	**M** 4	**P** 3

Comunicado da Cimeira da OTAN em Gales — 2014	(OTAN (n), 2014, p.15) Parágrafo 72	**<u>Ameaça</u>:** "*As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging*" **<u>Direito</u>:** "*international law, including international humanitarian law and the UN Charter, applies in cyberspace.* • *impact could be as harmful to modern societies as a conventional attack*" **<u>Medidas</u>:** "*committed to developing further our national cyber defence capabilities* • *enhance the cyber security of national networks upon which NATO depends for its core tasks* • *continue to integrate cyber defence into NATO operations and operational and contingency planning* • *enhance information sharing and situational awareness among Allies* • *intensify our cooperation with industry through a NATO Industry Cyber Partnership* • *improve the level of NATO's cyber defence education, training, and exercise activities* • *develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability*" **<u>Política</u>:** "*we have endorsed an Enhanced Cyber Defence Policy* • *principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence* • *responsibility of NATO is to defend its own networks* • *assistance to Allies should be addressed in accordance with the spirit of solidarity* • *emphasizing the responsibility of Allies to develop the relevant capabilities* • *We affirm therefore that cyber defence is part of NATO's core task of collective defence* • *A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis* • *engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU*"	**A** 1	**D** 2	**M** 7	**P** 8

Comunicado da Cimeira da OTAN em Varsóvia — 2016	(OTAN (o), 2016, p.15) Parágrafo 70	**Ameaça:** "*Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack*" **Direito:** "*We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable*" **Medidas:** "*cyberdefence will continue to be integrated into operational planning and Alliance operations and missions* • *continue to implement NATO's Enhanced Policy on Cyber Defence and strengthen NATO's cyber defence capabilities*" **Política:** "*cyber defence is part of NATO's core task of collective defence* • *we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea* • *We will continue to follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace* • *welcome the work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace*"	**A**	**D**	**M**	**P**
			1	1	2	

Fonte: (O autor, 2017)

Apêndice E — Modelos de Qualificação de um ciberataque como um ataque armado.

Conforme referido no subcapítulo 1.3.1.1, existem várias abordagens para a definição de uma operação no ciberespaço como um ataque armado. No entanto, decorrente do estudo dos especialistas envolvidos na publicação do manual de Talin, a abordagem baseada nos efeitos é aquela que maior razoabilidade tem. Esta posição é sustentada na observação das considerações tecidas após ataques perpetrados com meios cinético, e também nas conclusões do Tribunal Internacional de Justiça (TIJ) retiradas da decisão do caso da Nicarágua vs EUA.

Sucintamente, o TIJ considerou que o apoio financeiro dos EUA ao grupo guerrilheiro *Contra's* (envolvido em atos subversivos na Nicarágua), não constituiu ação suficiente, no que aos efeitos produzidos diz respeito, que habilitasse afirmar, que essa ação particular se tivesse constituído como um ataque armado, pelo que não alcançou o padrão de uso da força[34] que caracteriza uma agressão. (TIJ, 1986, p.108)

Ora se o apoio financeiro a um grupo guerrilheiro não corresponde ao uso da força em conformidade com o TIJ, a mesma interpretação poderá ser feita para o financiamento de um grupo de *hacktivistas*, que conduza operações no ciberespaço durante uma sublevação, ou uma insurgência. Por outro lado, se o Estado armar, treinar e suportar uma guerrilha envolvida numa hostilidade contra outro Estado, então essas ações qualificam-se como uso de força. (TIJ, 1986)

Assim, ceder a um grupo organizado capacidades ofensivas no ciberespaço (*Malware*[35] por exemplo) e, providenciar treino para o uso dessas capacidades, de forma a que habilitem à realização de ciberataques contra uma parte terceira, qualifica-se como uso de força.

Então de que forma se poderá avaliar se as ações resultam num uso indevido da força? Michael N. Schmitt parte destas conclusões do TIJ e da abordagem delas retirada, de avaliar os atos com base nos efeitos alcançados. A sua abordagem caracteriza o padrão de danos infligidos e alguns elementos qualitativos do grau de intensidade das ciberoperações.

Em complemento a esta tese, defende o grupo de especialistas envolvidos no manual de Talin (do qual faz parte Schmitt), que os atos que provoquem ferimentos ou a morte a indivíduos e, a destruição de propriedade, se constituem inquestionavelmente como atos de uso da força. (Schmitt et al., 2013)

Assim, independentemente da avaliação política que será feita pelos Estados, ao se efetuar uma avaliação baseada em efeitos, a tendência será para colocar maior importância nos fatores definidos pelo grupo de especialistas no manual de Talin, e que importam abordar neste trabalho:

Abordagem baseada nos efeitos[36] – Modelo conhecido por ser baseado nas consequências. O critério assenta no efeito global provocado pelo ciberataque, no(s) Estado(s) vítima(s). Por exemplo, a manipulação informática de dados de instituições bancárias e financeiras, afetando um determinado país, pode ser vista como um ataque informático. Embora esta ação não tenha semelhança com um ataque cinético, o resultado global que a manipulação de informação irá causar ao bem-estar económico do Estado vítima, justificará a sua equiparação a um ataque armado (Fernandes, 2012, p.146).

Esta abordagem assenta em oito requisitos definidos no manual de Talin:

[34] Decisão do caso da Nicarágua, paragrafo 228.
[35] *Malware* é o nome abreviado para *software* malicioso e trata-se de qualquer tipo de *software* indesejado, instalado sem o devido consentimento. (Microsoft, s.d.)
[36] "*Effects-based approach*" no original.

- **Gravidade** – Os atos que ameacem a integridade física de indivíduos ou a destruição da propriedade numa extensão muito maior que outras formas de coerção, representarão em si atos de uso de força. Aqueles que provoquem apenas inconveniência e incómodo não serão dessa forma considerados. Entre estes dois extremos opostos, os atos ocorridos no ciberespaço e que maior impacto tenham nos interesses nacionais vitais, terão maior probabilidade de serem considerados como uso de força (Schmitt et al., 2013, p.48).

  Ainda de acordo com Schmitt, este fator pode ser avaliado categorizando-o de acordo com os critérios de: *i) pessoas mortas, graves danos em infraestruturas; ii) pessoas feridas, danos moderados em infraestruturas; iii) sem pessoas afetadas, sem danos percetíveis em infraestruturas.* No fundo, trata de perceber-se quantas pessoas faleceram, qual a dimensão da área atacada (escopo), qual a extensão dos danos na área afetada (intensidade) e duração dos mesmos (2010). A Gravidade é o fator preponderante desta abordagem.
- **Imediatismo–** Defende Schmitt que as consequências da coerção armada, ou da ameaça do uso da coerção armada geralmente ocorre com grande imediatismo, enquanto que outras formas de coerção se desenvolvem mais lentamente. Em situações mais dilatadas no tempo, o estado visado, ou a comunidade internacional, tem oportunidade de encontrar uma solução pacifica para o caso, oportunidade essa que, num ciberataque, manifestamente não existe (2013, p.49).
- **Caráter Dirigido** – As consequências da coerção armada têm maior ligação direta ao *actus reus* (ato de culpabilidade) do que em outras formas de coerção, que geralmente dependem de numerosos fatores contributivos. Quanto mais atenuada for a ligação entre o ato inicial e as suas consequências, menor será a probabilidade de os Estados conseguirem imputar o ato ao ator responsável pela violação da proibição do uso da força. As operações no ciberespaço em que o nexo causa efeito seja claramente identificado, será mais fácil de caracterizar como um ataque armado (Schmitt et al., 2013, p.49).
- **Caráter Intrusivo** – Este fator caracteriza o nível de intrusão no Estado alvo ou nos seus sistemas. Por exemplo, a intrusão numa infraestrutura militar com capacidade de ciberdefesa certificada caracterizar-se-á como um ato mais intrusivo, que um ato dirigido a um sítio no ciberespaço pertencente a uma faculdade. Da mesma forma a intrusão num sítio alojado no domínio www.governo.pt, terá um grau de extensão da invasão superior a uma invasão a uma página no domínio ".com" (Schmitt et al., 2013, p.49).
- **Mensurabilidade ou Extensão** – Este fator está associado à maior capacidade de os Estados caracterizarem ações no ciberespaço como ataques armados, fundamentando essa caracterização com a observação dos factos. Quanto melhor se quantificar e identificar um conjunto de consequências, maior facilidade haverá em se qualificar a situação (Schmitt et al., 2013, p.50).
- **Carácter Militar** – Uma ligação entre as operações no ciberespaço e operações militares em curso, aumenta a probabilidade de caracterização dessas ações como uso de força (Schmitt et al., 2013, p.50).
- **Envolvimento do Estado** – Representa a extensão do envolvimento do Estado numa operação que abrange desde a atuação direta ao envolvimento periférico. Quanto mais claro for o nexo

de casualidade entre uma operação no ciberespaço e um Estado, maior será a probabilidade de os restantes Estados caracterizarem essa operação como uso da força (Schmitt et al., 2013, p.51).

- **Presunção da Legitimidade** – na maioria dos casos, o uso da força, seja sob o prisma ou da lei doméstica ou da lei internacional, é ilegal, exceto se estivermos perante uma exceção que a permita (Fernandes, 2012, pp.148-49), como é o caso da legítima-defesa. O principio assenta no facto de que os atos que não são proibidos são permitidos. Na ausência de uma convenção, tratado internacional, ou de uma proibição assente no costume comummente aceite, um ato no ciberespaço é presumivelmente legal. Por exemplo, propaganda, operações psicológicas, espionagem, ou pressão económica, não são ações proibidas. Assim, há menor probabilidade destes atos serem considerados pelos Estados como uso da força.

Por outro lado, importa também compreender sucintamente as outras abordagens:

Abordagem Instrumental[37]– Modelo em que a avaliação será efetuada com o intuito de saber se o dano provocado por um ciberataque poderia, previamente, ser apenas causado por um ataque cinético. Por exemplo, usando este modelo, um ciberataque conduzido com o objetivo de colocar fora de funcionamento uma rede elétrica seria considerado um ataque armado. (A razão dessa qualificação tem a ver com o facto de antes do desenvolvimento de cibercapacidades, a destruição de uma rede elétrica ter, tipicamente, requerido o bombardeamento desta, ou o uso de algum tipo de força cinética para obter esse resultado) (Fernandes, 2012, p.146).

Abordagem baseada na responsabilidade estrita[38] –Este modelo assenta numa abordagem baseada na responsabilidade estrita. Segundo esta abordagem um ciberataque contra qualquer infraestrutura nacional critica seria, de forma automática, considerado equiparável a um ataque armado. Tal qualificação seria justificada pelas potenciais consequências severas que podem resultar de um qualquer ataque a tais sistemas de infraestruturas críticas nacionais (Fernandes, 2012, p.147).

[37] "*Instrument-based approach*" no original.
[38] "*Strict liability approach*" no original.

Apêndice F — Diagrama de Análise dos Requisitos de Schmitt.

Compreender os requisitos de Schmitt, permite compreender os fatores que qualificam um ataque armado no ciberespaço. Pretende-se, com este Apêndice, realizar um exercício, que permita tentar estabelecer um modelo que habilite uma resposta às perguntas identificadas no Manual de Talin (Figura 28):

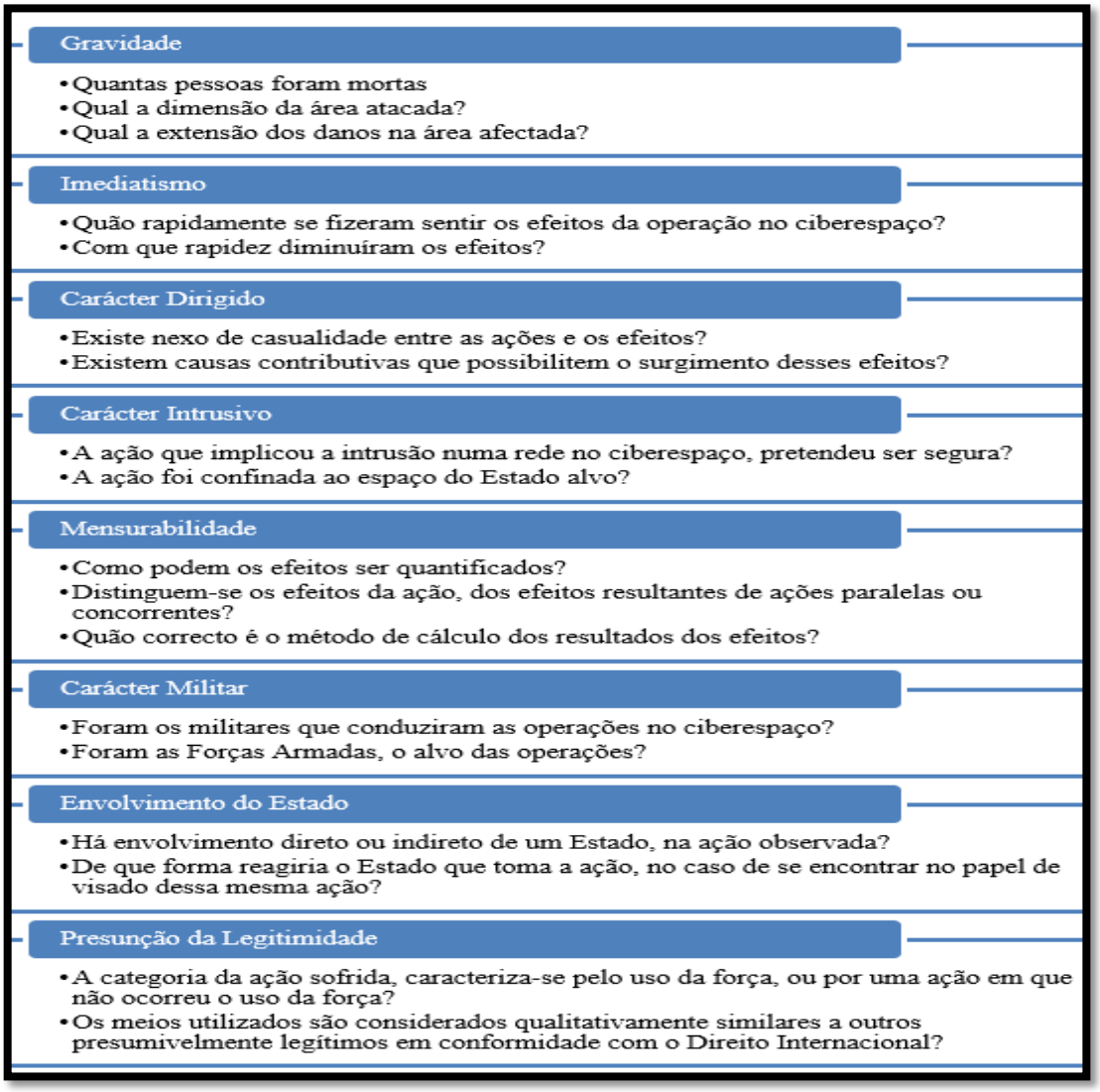


Figura 28 – As questões que identificam critérios para a análise.

Fonte: (Schmitt et al., 2013, p.51)

Da análise destas questões e dos requisitos definidos no Manual, definiram-se critérios para quantificação que ao serem ponderados permitem definir padrões. Esses padrões ao se verificarem, permitirão uma melhor justificação do que se considera ser um ataque armado, perante a comunidade internacional.

Assim, definiram-se os seguintes princípios quantitativos associados aos critérios do Grau da Importância[39] e do Grau de Aplicabilidade[40], (Tabela 7):

[39] O Grau de Importância corresponde ao significado que uma ação tem à luz de cada requisito.
[40] O Grau de Aplicabilidade corresponde ao enquadramento de uma agressão como um ato que constitua um ciberataque.

Tabela 7 – Princípios Quantitativos.

Grau	Importância (Ip)	Aplicabilidade (A)
1	Irrelevante	Não aplicável
2	Pouco significativo	Aplica-se raramente
3	Significativo	Aplica-se
4	Relevante	Aplica-se recorrentemente
5	Extremamente relevante	Consistentemente aplicável

Fonte: (O autor,2017)

Recorrendo a uma análise multicritério, quantificam-se os requisitos e ponderam-se pesos para cada um (Tabela 8). Definindo-se politicamente o grau 4 como aquele a partir do qual se considera que se estará perante um ciberataque grave, abaixo desse grau será considerado um ataque negligenciável, obtendo-se os padrões da Figura 29.

Tabela 8 – Exemplo da quantificação de um ciberataque.

Requisitos	Pesos	Grave				Negligenciável			
		Ip	A	Med Ip	Med A	Ip	A	Med Ip	Med A
Gravidade	30%	5	5	1,5	1,5	3	3	0,9	0,9
Imediatismo	10%	5	5	0,5	0,5	4	5	0,4	0,5
Caráter Dirigido	10%	3	2	0,3	0,2	3	2	0,3	0,2
Caráter Intrusivo	10%	4	3	0,4	0,3	3	3	0,3	0,3
Mensurabilidade ou Extensão	10%	3	3	0,3	0,3	2	2	0,2	0,2
Carácter Militar	10%	5	3	0,5	0,4	4	5	0,4	0,5
Extensão do envolvimento do Estado	10%	4	3	0,4	0,4	1	1	0,1	0,1
Presunção de Legitimidade	10%	5	5	0,5	0,5	1	1	0,1	0,1
	100%			**4,4**	**4,1**			**2,7**	**2,8**

Fonte: (O autor, 2017)

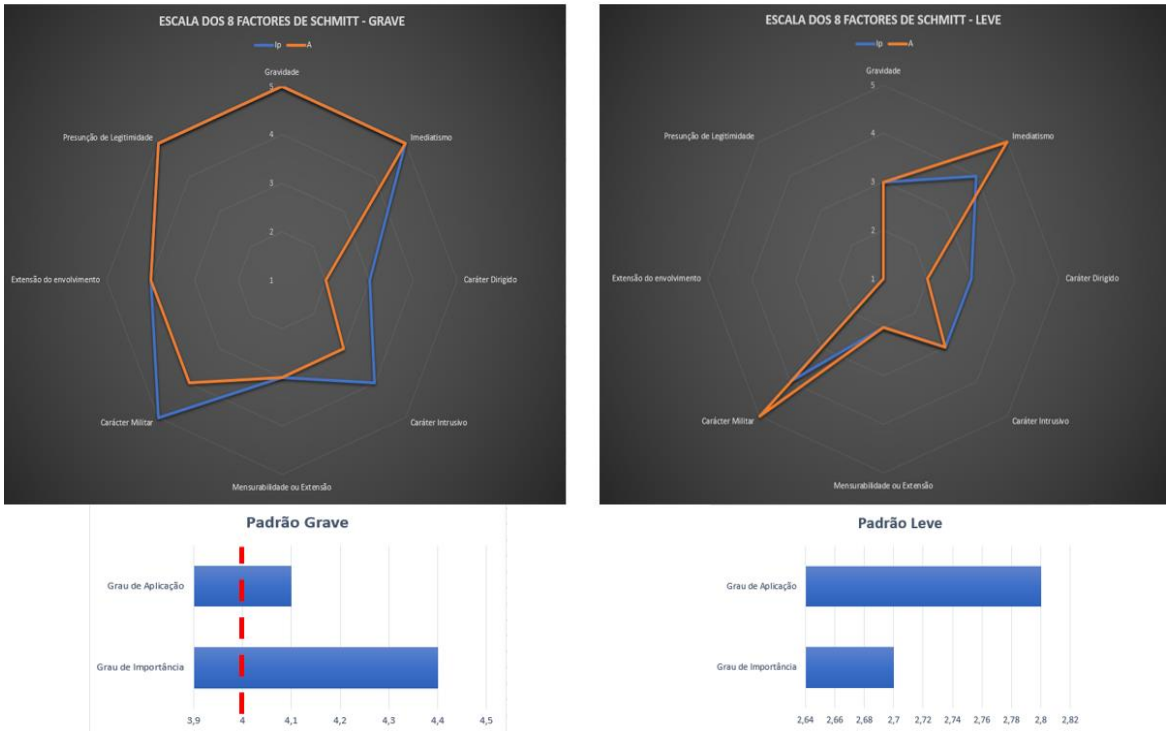


Figura 29 – Diagrama de Análise

Fonte: (O autor, 2017)