INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE ESTADO-MAIOR CONJUNTO
2016/2017

TII - TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

COMPATIBILIDADE DAS REGRAS CONTIDAS NO MANUAL DE TALLINN COM UMA ESTRATÉGIA EFICAZ DE DISSUASÃO NO CIBERESPAÇO.

Rubén Vega Bustelo
COMANDANTE DE INFANTERÍA DEM, ESPAÑA

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

COMPATIBILIDADE DAS REGRAS CONTIDAS NO MANUAL DE TALLINN COM UMA ESTRATÉGIA EFICAZ DE DISSUASÃO NO CIBERESPAÇO.

CTE INF DEM ESP, Rubén Vega Bustelo.

Trabalho de Investigação Individual do CEM-C

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

COMPATIBILIDADE DAS REGRAS CONTIDAS NO MANUAL DE TALLINN COM UMA ESTRATÉGIA EFICAZ DE DISSUASÃO NO CIBERESPAÇO.

CTE INF DEM ESP, Rubén Vega Bustelo.

Trabalho de Investigação Individual do CEM-C

Orientador: MAJ PILAV Nuno André Barros Monteiro da Silva.

Pedrouços 2017

Declaração de compromisso Anti Plágio

Eu, **Rubén Vega Bustelo** declaro por minha honra que o documento intitulado **"Compatibilidade das regras contidas no Manual de Tallinn com uma estratégia eficaz de dissuasão no ciberespaço"** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **CEMC 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, 16 de junho de 2017

Rubén Vega Bustelo

Comandante de Infantería (ESP)

Agradecimentos

A todos os que fizeram possível a realização deste trabalho.

Em especial:

Ao meu orientador, MAJ PILAV Nuno André Barros Monteiro da Silva, pelas suas apartações e conselhos desde o início do projeto e pela sua ajuda na correção do trabalho, bem como pelas suas indicações e sugestões no desenvolvimento do mesmo, especialmente nos momentos de maior dificuldade e incerteza.

À minha mulher Mari Paz, pela sua compreensão e apoio incondicional, pela tranquilidade que sempre me deu para que eu pudesse trabalhar.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

Na Cimeira de Gales da OTAN de 2016, acordou-se que a ciberdefesa faz parte nuclear do esquema de segurança coletiva e declarou-se a aplicabilidade do direito internacional no ciberespaço. Posteriormente, na Cimeira de Varsóvia de 2016, a OTAN reafirmou o seu mandato coletivo em relação à ciberdefesa, assim como o reconhecimento do ciberespaço como um domínio mais das operações. Adicionalmente, reafirmou o seu compromisso para atuar de acordo com legalidade internacional neste domínio. A OTAN considera que com estas medidas melhorará a sua capacidade de dissuasão e defesa.

Por outro lado, desde 2009 o *NATO Cooperative Cyber Defence Centre of Excellence* esta a promover o *Tallinn Manual Process* orientado à investigação e formação relativa à aplicabilidade do direito internacional no ciberespaço. Este processo atingiu o primeiro grande objetivo em 2013 com a publicação do *Tallinn Manual*, publicação sob a responsabilidade exclusiva de seus autores, sem reconhecimento oficial pela OTAN.

Através duma estratégia de investigação qualitativa de raciocínio hipotético-dedutivo avalia-se a compatibilidade das regras contidas no *Tallinn Manual* com a eficácia das estratégias de dissuasão no ciberespaço para terminar avançando na proposta de estratégias mais eficazes e de novas linhas de investigação.

Palavras-chave

Tallinn Manual Process, dissuasão, direito internacional, atribuição, ciberespaço.

Abstract

At the NATO Wales Summit 2016, it was agreed that cyber defence is part of NATO's core task of collective defence and that international law applies in cyberspace. Later, at the Warsaw Summit in 2016, NATO reaffirmed its defensive mandate in relation to cyber defence, and recognised cyberspace as another domain of operations. NATO commitment to act in accordance with international law in this field was also reaffirmed. All these measures are believed to support NATO's broader deterrence and defence.

On the other hand, since 2009 the NATO Cooperative Cyber Defence Centre of Excellence has promoted the Tallinn Manual Process, oriented to research and training concerning the applicability of international law in cyberspace. This process reached its first major goal in 2013 with the publication of the Tallinn Manual, under the sole responsibility of their authors, without official recognition by NATO.

Through a qualitative research strategy of hypothetical-deductive reasoning, it´s assessed the compatibility of the Tallinn Manual rules with the effectiveness of deterrence strategies in cyberspace, to finish advancing the proposal for more effective strategies and new lines of investigation.

Keywords

Tallinn Manual Process, deterrence, international law, attribution, cyberspace.

Lista de abreviaturas, siglas e acrônimos.

CCDCOE	*NATO Cooperative Cyber Defence Centre of Excellence*.
CNA	*Computer Network Attack.*
CND	*Computer Network Defense.*
CNE	*Computer Network Exploitation.*
CNU	Carta das Nações Unidas
CSNU	Conselho de Segurança das Nações Unidas
EUA	Estados Unidos de América.
GIG	*Gobal Information Grid.*
IPv6	*Internet Protocol version 6*
NATO	*North Atlantic Treaty Organisation.*
NCSS	*National Cybersecurty Strategies.* Estratégias Nacionais de Cibersegurança.
MCCD	*Mando Conjunto de Ciberdefensa* (Espanha).
OTAN	Organização do Tratado do Atlântico Norte.
ONU	Organização das Nações Unidas.
SROE	*Standing Rules of Engagement*
TIC	Tecnologias da Informação e as Comunicações.
TM	*Tallin Mannual*
UE	União Europeia

Introdução

"Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them."

(Brodie, 1946)

O presente Trabalho de Investigação Individual (TII) do Curso de Estado-Maior Conjunto está enquadrado no âmbito da aplicabilidade do direito dos conflitos armados à ciberguerra, e subordina-se ao tema: "Compatibilidade das regras contidas no Manual de Tallinn com uma estratégia eficaz de dissuasão no ciberespaço".

Este tema insere-se no âmbito dos estudos de Estratégia, mais especificamente na factibilidade de incluir as regras de interpretação jurídica decorrentes do *Tallinn Manual Process*[1] na doutrina da NATO.

Neste âmbito, em 2013 publicou-se o *Tallinn Manual on The International Law Applicable to Cyber Warfare* (Schmitt, et al., 2013), que é o primeiro manual de um processo mais ambicioso. Trata-se de um documento publicado sob a responsabilidade de seus autores, não vinculante para nenhuma nação ou organização, relativo à aplicação à ciberguerra da legislação existente (Schmitt et al., 2013; CCDCOE, s.d.b, p. Research).

O tema abordado é de grande relevância e atualidade. Na Cimeira de Gales da OTAN em 2014, acordou-se que a ciberdefesa faz parte nuclear do esquema de segurança coletiva e declarou-se a aplicabilidade do direito internacional no ciberespaço, incluindo o Direito Internacional Humanitário e a Carta das Nações Unidas (NATO, 2014b). Posteriormente, no comunicado conjunto da Cimeira da NATO em Varsóvia de 2016, a OTAN reafirmou o seu mandato coletivo em relação à ciberdefesa, assim como o reconhecimento do ciberespaço como mais um domínio das operações, que deve ser defendido com a mesma efetividade que o terrestre, o marítimo e o aéreo. A OTAN considera que assim melhorará a sua habilidade para proteger e para conduzir operações nestes domínios, também para manter a liberdade de ação e de decisão em todas as circunstâncias, sustentado deste modo a sua capacidade de dissuasão[2] e defesa. Assim também, a OTAN reafirmou o seu compromisso para atuar de

[1] Trata-se dum processo iniciado em 2009 pelo *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) que assenta em dois pilares, a investigação sobre as questões legais pertinentes às ciberoperações e o treino projetado para operacionalizar os resultados das investigações. (CCDCOE, s.d.a.; CCDCOE, s.d.b.; CCDCOE, s.d.a., Schmitt et al., 2013, pp.1-4)

[2] "*NATO's broader deterrence and defence*".

acordo com legalidade internacional neste domínio (NATO, 2016). Portanto, a OTAN evidencia dois elementos que devem concorrer para atingir os seus objetivos: manter a capacidade de dissuasão alargada e atuar de acordo com a legalidade internacional, resultando que o posicionamento pormenorizado em relação ao segundo condicionará as capacidades disponíveis para o primeiro.

Fora do âmbito da defesa coletiva, se nos circunscrevermos ao âmbito de cada Estado, a manual referência do CCDCOE para a definição de estratégias nacionais de cibersegurança (Klimburg, 2012, pp. 81-86) avalia as estratégias ofensivas e defensivas a combinar para um Estado fazer o seu ciberespaço mais seguro, nomeadamente a dissuasão versus a resiliência[3]. Para determinar o modo de combinar estas estratégias, importa avaliar qual é o grau de compatibilidade das regras do *Tallinn Manual* com ambas as possibilidades.

Por outro lado, na altura do início do *Tallinn Manual Process*, assim como agora, poucas leis ou normas internacionais definem explicitamente os comportamentos aceitáveis e inaceitáveis no ciberespaço, o que dificulta o processo de garantir a segurança dos Estados, ao terem poucas garantias de que não serão alvo de ataques cibernéticos caso se abstiverem de atacar os seus adversários (Goodman, 2010, p.120). O facto de quatro nações da Organização para a Cooperação de Shangai, incluindo a China e a Rússia, terem apresentado em 2011 na Assembleia General das Nações Unidas uma proposta de Código Internacional de Conduta para a Segurança da Informação (ONU, 2011a), seguida duma revisão da mesma em 2015 (ONU, 2015), partindo de uma abordagem jurídica significativamente diferente à feita no âmbito da OTAN, confirma as dificuldades de assegurar o ciberespaço.

Além disso, a ambiguidade é um elemento relevante da dissuasão assente em represálias, desde que fornece a quem dissuade flexibilidade situacional (Schelling, 1966 cit. por Solomon, 2011, p.3) e está estreitamente ligado a outros elementos fulcrais como a credibilidade. Segue-se assim a necessidade de conhecer ate que ponto o posicionamento exato em relação à interpretação do direito internacional no ciberespaço pode limitar a capacidade de dissuasão.

Consequentemente, considera-se do maior interesse para a OTAN e para os seus Estados conhecer os efeitos das regras do *Tallinn Manual* (TM) sobre a dissuasão, assim como os da possível aceitação oficial desta interpretação jurídica. Com este trabalho

[3] Ver definição no Apêndice A e comentários na secção 1.4.1.

pretende-se incrementar o conhecimento neste campo contribuindo para o esclarecimento destas questões.

A amplitude do âmbito em que nos desenvolvemos exige uma delimitação apropriada do objeto de investigação. Assim, consideram-se como objeto de estudo desta investigação a dissuasão no ciberespaço e o TM exclusivamente nos aspetos que afetam a dissuasão no ciberespaço. Embora seja amplamente aceite que os efeitos das atividades dos atores não estatais continuarão a ter efeitos muito relevantes no ciberespaço, apresentando um dos maiores riscos para a dissuasão efetiva e para a segurança transnacional no ciberespaço (Jensen, 2012, pp.781,782), neste estudo só se abordará a dimensão interestatal da dissuasão, em linha com o âmbito do TM.

Em relação ao TM só será objeto de estudo o volume publicado em 2013, não se estudando o *Tallinn Manual 2.0*, cuja recente publicação não permitiu enquadrá-lo no cronograma estabelecido para o desenvolvimento deste trabalho.

O objetivo geral deste trabalho é compreender como as regras de interpretação do direito internacional contidas no TM afetam a dissuasão no ciberespaço, e como a afetariam caso fossem assumidas oficialmente pela NATO ou pelos seus membros.

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

OE1 - Determinar em que medida o *Tallinn Manual* contribui para superar as dificuldades específicas do meio cibernético relativas à aplicação de doutrinas de dissuasão no ciberespaço.

OE2 - Determinar em que medida é compatível o posicionamento do *Tallinn Manual* com as opções de dissuasão no ciberespaço.

Para atingirmos o nosso objetivo geral, identificamos a seguinte pergunta de partida (Bryman, 2012, p.384):

"Em que medida as regras contidas no Tallinn Manual e o posicionamento oficial em relação a elas são compatíveis com uma estratégia eficaz de dissuasão no ciberespaço?"

Esta pergunta de partida leva duas perguntas derivadas:

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

PD2 - *Em que medida é compatível o posicionamento do Tallinn Manual com as opções de dissuasão no ciberespaço?*

Durante esta investigação o autor procurou romper com qualquer ideia preconcebida. Indispensável à construção do modelo teórico que foi o ponto de partida para o processo

dedutivo, formularam-se as hipóteses que se seguem e cujo processo de validação orientou a construção de explicações que permitiu avaliar a solução do problema da investigação.

HIP1 - *As regras do Tallinn Manual têm efeitos diferenciados sobre cada dimensão do problema da dissuasão no ciberespaço, que por sua vez poderão variar dependendo da existência de posicionamento oficial no que respeita a estas regras.*

HIP2 - *A compatibilidade do Tallinn Manual com as opções de dissuasão no ciberespaço está relacionada com o impacto das suas regras sobre as dimensões da dissuasão consideradas e às estratégias adotadas, o que permitirá delinear estratégias mais eficazes.*

Quanto à metodologia de investigação, na fase exploratória, para além de algumas entrevistas orientadoras, conduziu-se uma profunda revisão documental que revelou a linha de investigação e a metodologia assente numa estratégia científica de investigação qualitativa segundo o raciocínio hipotético-dedutivo, assente no modelo de analise que se apresenta no Mapa Conceitual do Apêndice C e no Corpo de Conceitos do Capítulo 1 e do Apêndice A. A fundamentação teórica do modelo de análise inclui-se no Apêndice C.

O trabalho está estruturado em três capítulos. O primeiro capítulo abrange a parte descritiva do relatório, sustentada na análise documental, fornecendo a base concetual e concretizando a problemática da situação atual.

A parte analítica inclui-se nos dois capítulos seguintes, dedicados respetivamente à análise do impacto do TM para a solução dos problemas de dissuasão no ciberespaço e à análise da compatibilidade das regras do TM com as opções para a dissuasão.

Na parte conclusiva, o estudo resume, compara e salienta os principais contributos do TM neste âmbito, finalmente apontando para novas linhas de investigação.

Na referenciação bibliográfica empregou-se o estilo *Harvard-Anglia*, tal como preconizado na NEP/ACA-018 do IUM, com exceção das referências às regras e comentários do *Tallinn Manual* (Schmitt, et al., 2013), que, para facilitar a compreensão do texto são referenciadas pela palavra "Regra" seguida do número da regra ou do comentário à regra em questão.

1. Conceitos, estado do arte e metodologia

1.1. Caracterização do Ciberespaço

O ciberespaço é domínio das operações militares mais recentemente incorporado e o mais diferente. Não ocupa um espaço natural nem geográfico e é totalmente artificial, o que envolve maior vulnerabilidade (Gómez de Ágreda, 2012,p.171), porque a estrutura que o sustenta é intrinsecamente mais débil e modificável que os domínios terrestre, marítimo, aéreo e espacial.

Há diversas definições de ciberespaço e a maioria delas estruturam-no em camadas, que variam em função das questões a abordar (Even e Siman-Tov, 2012, p.10-13).

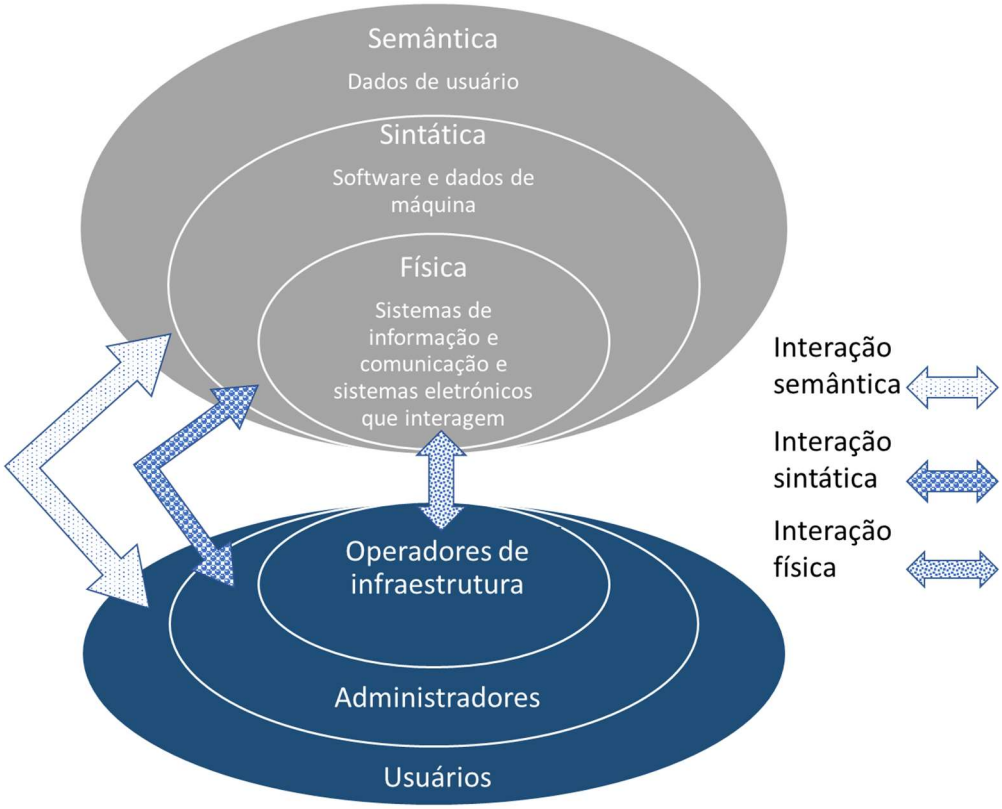

Figura 1 – Estrutura de camadas do ciberespaço e interação humana

Fonte: (Autor, 2017)

Na taxonomia da OTAN, define-se o ciberespaço como o domínio global formado pelos sistemas de informação e de telecomunicações e outros sistemas eletrônicos, sua interação e os dados que são armazenados, processados ou transmitidos por esses sistemas (NATO, 2014a).

Para facilitar a compreensão, neste trabalho empregaremos a estrutura da figura 1, que subdivide os dados em dois níveis: uma camada semântica que inclui a informação e uma

camada sintática que inclui o software e os dados destinados a ser usados pelos computadores (Libicki, 2009a, p.12).

Quanto aos limites do ciberespaço, à semelhança do que se passa com os domínios aéreos e espacial, obedecem a diferentes interpretações, sendo o problema mais conceptual do que prático. O relevante é que o ciberespaço existe fisicamente em cada um dos outros domínios, conectando-os e fortalecendo-os, enquanto que as atividades neles realizadas se podem expressar no domínio do ciberespaço (Even e Siman-Tov, 2012, p.10).

Importa salientar duas diferenças fulcrais do ciberespaço em respeito aos domínios tradicionais. A sua vinculação geográfica é baixa, limitando-se ao traçado das redes de comunicação e à localização dos dispositivos e servidores, que são geralmente propriedade de companhias privadas, o que altera o significado tradicional das fronteiras (Hare, 2009). Adicionalmente, produz uma aproximação virtual de contendores longe demais para uma batalha convencional (Sánchez, 2012, p.142). A outra grande diferença é a escala temporal que emprega, própria dos computadores e na ordem dos microssegundos.

Estas diferenças quanto à natureza, estrutura, geografia e escala temporal moldam as dimensões do problema da dissuasão no ciberespaço.

1.2. Conceitos relativos à dissuasão

Para Cabral Couto (Couto, 1988, p.59) "*A dissuasão, em sentido lato, visa impedir uma potência adversa de, numa situação dada, recorrer a determinados meios de coação em virtude da existência de um conjunto de meios e de disposições capazes de constituírem uma ameaça suficientemente desencorajadora.*

A dissuasão é, essencialmente, um resultado de natureza psicológica: traduz-se por uma inibição ou paralisia perante uma ameaça que se receia e que é de concretização possível e plausível. Deriva de um cálculo desfavorável entre as potenciais vantagens ou benefícios que se podem colher no caso de se levar a efeito uma determinada ação e os riscos ou custos inerentes a essa ação, dadas as possibilidades do adversário. " Sendo uma ameaça "*qualquer acontecimento ou ação (em curso, ou previsível), de variada natureza e proveniente de uma vontade consciente que contraia a consecução de um objetivo...* " O que Couto (1988, p.329) sumariza como "*o produto de uma possibilidade por uma intenção*".

Vemos, portanto, que se trata duma forma de coação, que se orienta a manter um status-quo impedindo a ação do outro, a diferença doutras formas mais assertivas e arriscadas, que perseguem mudar o comportamento que o adversário já está desenvolvendo (Pape, 1996 cit. por Cimbala, 1998).

O termo português dissuasão abrange dois conceitos diferenciados na terminologia anglo-saxónica: *dissuasion* e *deterrence*. O primeiro é o mais abrangente podendo incluir só a simples ação diplomática, enquanto o segundo envolve necessariamente capacidades e intenções militares como integrantes da estratégia (Codner, 2009, p.4-5; Gray, 2003, p.14). Para a finalidade deste estudo, empregar-se-á o termo na segunda acepção:

Dissuasão (em terminologia anglo-saxónica: ***deterrence***): A prevenção da ação pelo medo das consequências. A dissuasão é um estado de espírito provocado pela existência de uma ameaça credível de ação contrária de consequências inaceitáveis. (US DoD, 2001)

No que concerne à abrangência da cobertura dissuasória, consideramos duas modalidades diferenciadas de dissuasão, mas estreitamente relacionadas (Snyder 1961 cit. por Quackenbush, 2011, p.4):

Dissuasão central ou fundamental: quando o objetivo é dissuadir um ataque direto contra o defensor, normalmente sobre o seu território nacional. (Gray, 2003, p.13 e Quackenbush, 2011, p.4)

Dissuasão estendida ou alargada: quando o objetivo se alarga para defender aos aliados e amigos. (Gray, 2003, p.13)

Por fim, se considerarmos a vontade real dos oponentes para empregar a força (Haffa, 1992,p.8; Morgan, 1977,pp.28-29), diferenciamos:

Dissuasão imediata ou pura: quando o dissuasor, ciente da ameaça, desencadeia uma contra ameaça para dissuadir a um potencial atacante que já considera ativamente o emprego da força.

Dissuasão geral: quando está presente a possibilidade de um conflito armado, mas o potencial atacante não está a considerar ativamente o emprego da força para ameaçar os interesses do dissuasor.

Embora seja mais abundante a literatura empírica sobre a dissuasão imediata, a dissuasão general é muito mais abrangente e precede necessariamente à imediata. Assim, se a dissuasão general sempre tivesse sucesso não ocorreriam crises nem guerras e não seria necessária a dissuasão imediata. Iniciada a crise, a dissuasão imediata visa controlar a escalada (Quackenbush, 2011, p.4-5).

Este trabalho orientar-se-á mais para a dissuasão general.

Já no domínio do ciberespaço, e restrito à finalidade deste trabalho, devemos diferenciar (Autor, 2016):

Dissuasão no ciberespaço: a dissuasão exercida aplicando quaisquer opções de dissuasão para a prevenção de ações adversárias não desejadas no ciberespaço.

Ciberdissuasão: a dissuasão no ciberespaço empregando meios e opções do ciberespaço.

Ficam fora de ambas definições o emprego de ciberarmas ou de recursos do ciberespaço contra outros tipos de ataques.

1.3. Requisitos para a dissuasão:

Embora aparentemente sejam muitas as teorias da dissuasão, para Morgan (2003, p.8) pode haver diferentes estratégias de dissuasão, mas todas as abordagens teóricas fazem parte duma única teoria, que procura explicar a dissuasão mediante alguns elementos chave.

Para atingir os objetivos deste trabalho vamos focar-nos nas seguintes dimensões:

1.3.1. Ambiguidade

A ambiguidade necessária para a dissuasão consiste em induzir no adversário uma incerteza que lhe dificulte a valoração do risco em relação ao potencial benefício de ofender o defensor. Pretende-se, portanto, garantir uma faixa de segurança entre o limiar do espaço de manobra do dissuadido e o limiar em que o dissuasor está disposto para iniciar as represálias.

A dissuasão é mais uma questão de induzir incerteza ao adversário do que de induzir a certeza duma retaliação. Neste sentido, quando a paz parece certa há pouca ou nenhuma dissuasão e quando a guerra parece certa a dissuasão colapsa. A dissuasão deve gerar o senso de prudência e cautela do potencial atacante, bem como relutância em enfrentar sérios riscos para ganhos incertos (Morgan, 1977, p.117). "Teoricamente, a dissuasão começará quando o risco for superior ao valor dos objetivos visados; psicologicamente, porém, o risco dissuade antes de se atingir aquela paridade, em virtude de diversos fatores de incerteza, entre os quais figura, como já vimos, a impossibilidade de se apreciar, com exatidão, o valor que cada adversário atribui ao pomo da discórdia. " (Couto, 1988, p.63).

1.3.1. Atribuição

Sempre que a estratégia de dissuasão assenta na ameaça de desencadear uma represália, o dissuasor deve ter a capacidade de atribuir o ataque com alto grau de certeza, e o potencial agressor deve perceber que o defensor tem essa capacidade de atribuição (Solomon, 2011, p.5), pois só assim a avaliação de custo benefício o dissuadirá.

No âmbito do ciberespaço, a atribuição é o processo capaz de determinar a identidade e a localização do atacante original (atribuição perfeita). Contudo, sendo tal objetivo muito

difícil de atingir, adotaremos como definição alargada o processo capaz de identificar a identidade ou localização do atacante ou de um intermediário do atacante (Larsen e Wheeler, 2003, p.1-2).

1.3.2. Capacidade

Para orquestrar uma estratégia de dissuasão é necessário dispor dos meios capazes de produzir um efeito desencorajador (Couto, 1988, p.59). Para além disso é necessária a factibilidade política e legal de os empregar, portanto, a relação entre a capacidade material e o *jus ad bellum* é estreita.

1.3.3. Comunicação

Para atingir o resultado psicológico da dissuasão, é necessário que o dissuadido assimile corretamente a «mensagem» que envia o dissuasor, sendo que o erro de entendimento pode conduzir a estratégia dissuasória ao fracasso (Couto, 1988, p.60). A mensagem deve transmitir os limites (Schelling, 1966, p.135) e a capacidade e determinação de executar a ameaça dissuasória (Haffa, 1992, p.8), abrindo a possibilidade de um confronto violento, mas sem fechar a porta à negociação, o que requer um nível adequado de ambiguidade (Cimbala, 1998, p.156).

Embora as nações tendam a manifestar as suas intenções em ações, nem sempre são corretamente recebidas ou interpretadas pelos seus interlocutores. Um exemplo desta situação pode acontecer quando um Estado que em princípio respeita as regras e o costume internacional procura estabelecer novas regras que lhe ofereçam mais opções. Nesse caso arrisca-se o mal-entendido, porque tal pode ser percecionado como uma recusa em respeitar as regras (Shelling, 1966, p.151).

1.3.4. Cooperação

Juridicamente, a cooperação assenta no princípio da soberania e na consequente igualdade entre os Estados, mas para além disso, obedece ao princípio do consenso e tem sempre subjacentes objetivos políticos (Ribeiro, 2009, p.200-203). A dissuasão é um assunto bilateral, por vezes multilateral, que envolve a cooperação entre amigos e inimigos indistintamente (Morgan, 2003, p.241).

1.3.5. Credibilidade

A credibilidade decorre da intenção declarada e a resolução credível de proteger um determinado interesse (Haffa, 1992, p.8). Desde a perspetiva da teoria da dissuasão perfeita[4],

[4] Esta teoria foi desenvolvida para ultrapassar as deficiências lógicas das teorias clássicas da dissuasão (Zagare e Kilgour, 2000).

as ameaças são credíveis quando é racional materializá-las, ligando assim credibilidade e racionalidade, o que é consistente com o tratamento da credibilidade pela teoria dos jogos (Quackenbush, 2011, p.9). Por outro lado, fazer a ameaça credível é uma das maiores dificuldades para o defensor - de natureza fundamentalmente política mais do que técnica - porque o adversário valorizará a credibilidade tendo por base uma profunda analise dos fatores estratégico, politico, económico e ideológico, mais que em função da retorica ou outros elementos de sinalização (George e Smoke, 1974 cit. por Morgan 1977, pp.141)

1.3.6. Sinalização

No processo da dissuasão, que envolve ameaças e demandas, propostas e contrapropostas, para além de comunicar os limites da tolerância própria, é preciso sinalizar ao adversário a nossa intenção, de forma a estabelecer um jogo colaborativo em que mediante pequenos sinais alternativos, os adversários consigam coordenar um desvio progressivo da direção, que os pode levar a ultrapassar o limiar desencadeante das hostilidades. Mas sem que o prestigio de nenhum deles fique afetado face aos seus parceiros. (Schelling, 1966, p.119,135)

1.3.7. Soberania

Os Estados atuais são unidades políticas independentes, que pretendem não reconhecer como superior qualquer outra autoridade, e soberanas, que pretendem exercer a sua autoridade em exclusividade num espaço bem definido. Assim, a soberania é um atributo superior dos Estados, que se traduz no não reconhecimento de qualquer autoridade externa como superior à sua no interior do seu território, o que inclui a capacidade de estabelecer relações com outros Estados. As fronteiras, como determinantes do espaço onde se exerce a soberania, são um elemento fulcral desta. (Couto, 1988, pp.19-21,39,255)

1.4. Opções para a dissuasão no ciberespaço

As opções para a dissuasão no ciberespaço estão diretamente relacionadas com a factibilidade de empregar a força. Porém, a questão de empregar a força nunca pode ser separada da questão de como empregá-la com efetividade. Portanto, se não houver uma resposta satisfatória para o "como", não será apropriado o seu emprego (Haass, 1994, cit. por Cimbala, 1998).

Por outro lado, a dissuasão e a defesa combinam bem quando a ameaça dissuasória não é credível antes de iniciada a ofensa, demostrando ao agressor que o preço a pagar é superior ao que tinha previsto (Schelling, 1966, p.78).

Configuram-se assim as duas opções dissuasórias básicas: punitiva e por denegação.

1.4.1. Dissuasão punitiva

A dissuasão punitiva assenta na ameaça de punição, de forma que não é capaz de impedir que o adversário obtenha o ganho decorrente do ataque, mas dissuade-o de atacar colocando-lhe a expetativa de custos superiores aos ganhos previstos (Snyder, 1960, p.163).

Para o êxito da dissuasão punitiva é necessária uma capacidade adequada de atribuição, comunicação, sinalização, credibilidade e resposta (Libicki, 2009a e Solomon, 2011).

A capacidade de atribuição com certeza, para além de existir deve ser percebida pelo potencial atacante de forma a que possa avaliar os custos. Adicionalmente, os terceiros dificultam esta forma de dissuasão, porque pode ser difícil justificar perante eles o ataque e porque podem aproveitar a oportunidade para lançar um ciberataque suplantando o defensor. A resposta retaliatória não precisa ser simétrica, nem proporcional ao ataque, para ser credível, desde que esses termos sejam inerentemente políticos. Este é um facto muito relevante, especialmente pela complexidade técnica de dispor das ciberarmas necessárias para uma resposta simétrica (Solomon, 2011, pp.4,13,17).

Como consequência das dificuldades que apresenta a dissuasão punitiva no ciberespaço, esta deve limitar-se a casos em que se ultrapasse claramente o limiar apropriado para cada tipo de resposta, o que permitirá ao adversário aumentar o número de sondagens. Neste caso é importante comunicar-lhe privadamente que a agressão corresponde a uma represália, não sendo relevante que o público seja ciente do ciberataque inicial nem da natureza da represália (Solomon, 2011, p.19 e Libicki, 2012, pp.155-158).

1.4.2. Dissuasão defensiva ou por negação

Originariamente, Glenn Snyder (1960, p.163) definiu a dissuasão por negação como a capacidade para negar à outra parte qualquer ganho decorrente da ação que se pretende dissuadir, mas para a finalidade deste trabalho adotar-se-á a definição de Davis (2014, p.2), porque salienta o papel da percepção: Dissuasão por negação é conduzir o adversário a perceber a capacidade credível para lhe impedir que atinja qualquer ganho capaz de motivar a sua ação.

Quando o atacante percebe que a segurança dum sistema é tal que repetidos ataques não conseguirão efeitos significativos, a avaliação do custo em termos económicos, políticos e de possível retaliação, podem levá-lo a desistir de continuar com os ataques. Neste sentido, um consenso internacional adequado em relação à culpa do atacante pode acarretar-lhe os custos suficientes para o dissuadir. Adicionalmente, a estratégia pode reforçar-se

comunicando previamente a resiliência do sistema, para influenciar a avaliação de custos e benefícios do atacante (Solomon, 2011, p.3-4,13).

1.5. Ciclo de vida das normas de direito internacional

Não podemos abordar um estudo no âmbito da aplicabilidade do direito dos conflitos armados à ciberguerra sem considerar a origem, mecanismos e condições das normas para influírem a política internacional.

Tabela 1 – Etapas de desenvolvimento das normas internacionais

	Etapa 1 **Emergência e impulso inicial da norma**	**Etapa 2** **Efeito cascata**	**Etapa 3** **Internacionalização**
Atores	Empreendedores normativos com plataformas organizacionais	Estados Organizações Internacionais Redes	Legisladores Profissionais interessados Burocratas
Motivos	Altruísmo Empatia Idealismo Compromisso	Legitimidade Reputação Estima	Conformidade
Principais mecanismos	Persuasão	Socialização Institucionalização Demostração	Costume Institucionalização

Fonte: Traduzido e adaptado de (Finnemore e Sikkink, 1998)

Trabalhos independentes no âmbito dos estudos legais, da sociologia e das relações internacionais, chegaram a um padrão em três etapas do ciclo de influência das normas internacionais. Na primeira etapa, a norma emerge impulsionada por empreendedores que, sustentados por uma estrutura organizacional e empregando a persuasão como principal ferramenta, conseguem que uma quantidade aceitável de Estados aceite a norma. Atingido este ponto de inflexão, decorre a segunda etapa, onde se produz uma aceitação em cadeia da norma por uma elevada quantidade de atores internacionais. Por fim, temos a internacionalização da norma, que passa a ser aceite como norma jurídica ou costume internacional e deixa de ser objeto de debate. Mas nem sempre todas as normas terminam o ciclo, algumas não chegam nunca ao ponto de inflexão, outras, depois de o superarem convertem-se na referência a substituir por novas normas em emergência. (Finnemore e Sikkink, 1998, pp.894-909)

1.6. O estado atual da questão jurídica dos conflitos armados no ciberespaço

Os numerosos casos de ciberconflito que aconteceram desde os finais do século XX têm impulsionado distintos atores estatais ou interestatais a promover a aceitação normativa do seu posicionamento jurídico respeitante aos conflitos no ciberespaço (Carr, 2010).

A nível global, são dois os posicionamentos jurídicos mais relevantes:

Um posicionamento, liderado pela Rússia e pela China, que já esta sob a forma de proposta formal de Código Internacional de Conduta para a Segurança da Informação (ONU, 2011a e ONU, 2015), pretende um tratamento jurídico do ciberespaço diferenciado dos restantes domínios.

Outro, liderado pelos EUA (Schmitt, 2012) e pela OTAN (NATO, 2014b), contando com a maioria dos aliados e das democracias ocidentais, mas ainda sem propostas oficiais para a aceitação internacional, cujo posicionamento assenta no pressuposto de que a legislação internacional existente é suficiente. Portanto, reduz o problema a uma questão de interpretação, do qual o Processo e o Manual de Tallinn são os instrumentos de legitimação mais relevantes.

Numa lógica diferente, e à escala regional, a União Europeia (UE) terminou recentemente um processo normativo com a aprovação da Diretiva 2016/1148, orientada a garantir um elevado nível de segurança comum nas redes e sistemas de informação na UE (UE, 2016). Uma das caraterísticas fulcrais da diretiva é colocar sobre os Estados e sobre os provedores de serviços digitais, obrigações relativas à segurança do ciberespaço, embora não entre em questões primordiais como a aplicação do principio de territorialidade na investigação dos ciberataques.

1.7. Metodologia

Partindo de um posicionamento ontológico próximo do construtivismo e um posicionamento epistemológico próximo do interpretativismo (Matias et al., 2016, pp.16-20), depois da análise inicial do contexto do problema, optou-se por adotar uma estratégia científica de investigação qualitativa.

Em síntese, escalpelizando o desenho de pesquisa segundo o esquema de camadas proposto por Saunders, Lewis e Thornhill (2012, p.160), estamos perante um desenho de filosofia interpretativista, de raciocínio hipotético dedutivo (Marconi e Lakatos, 2003, pp.95-100), metodologia qualitativa e estratégia de estudo de caso, assente em dados documentais.

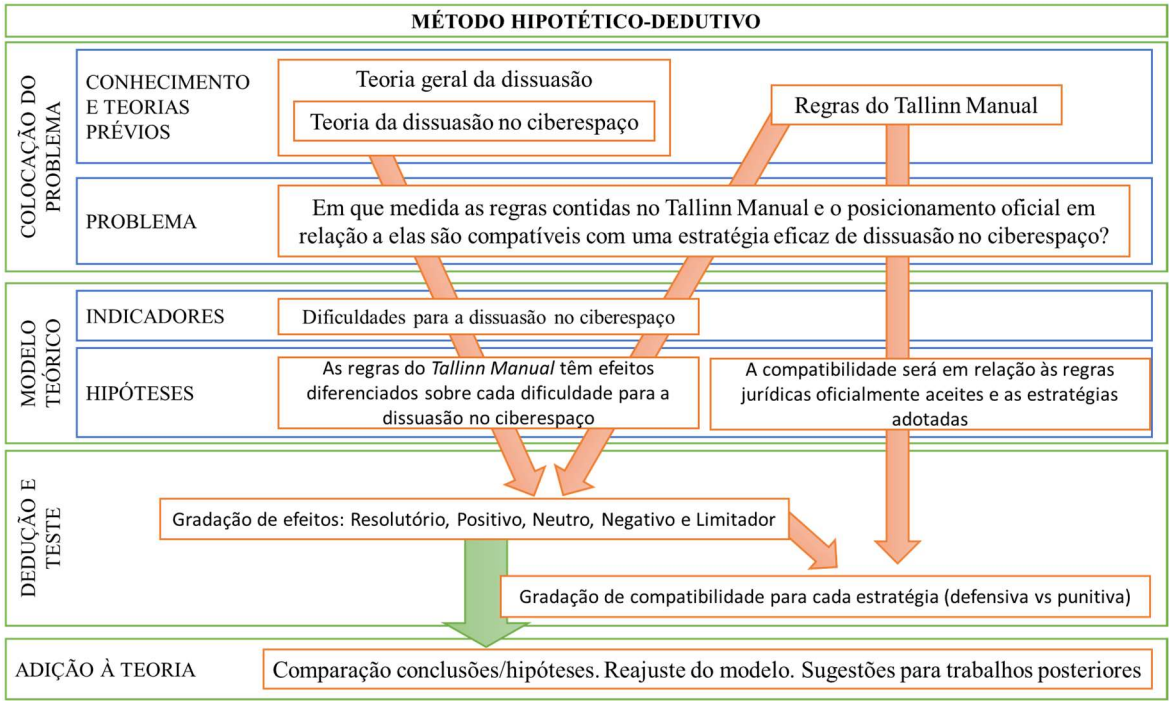

Figura 2 – Modelo de análise.

Fonte: (Autor, 2017)

Assim, tomando como ponto de partida duas teorias diferenciadas, a teoria da dissuasão aplicada ao ciberespaço e a teoria jurídica contida no TM (ver Fig. 2), pretende-se testar a compatibilidade destas quanto à sua aplicabilidade num caso e finalidade concretos: a procura de estratégias eficazes de dissuasão no ciberespaço. Uma vez colocado o problema e empregando como guia a primeira hipótese, escalpelizam-se as dimensões deste, obtendo como resultado a operacionalização de conceitos por meio de indicadores (Saunders, Lewis e Thornhill, 2012, p.140,144,146) que permite construir completamente o mapa conceitual do Apêndice C. A fundamentação teórica dos indicadores considerados inclui-se no Apêndice B. A fase de dedução e teste do modelo de raciocínio, desenvolvida nos capítulos dois e três, procura a construção de explicações (Saunders, Lewis e Thornhill 2012, p.580), mais do que testar as hipóteses por infirmação (Popper, 1935, pp.9-16,57-73). A estratégia de estudo de caso, é especialmente útil aqui, uma vez que permitirá avaliar a solução do problema de investigação respondendo as questões: que? como? e porquê? (Saunders, Lewis e Thornhill, 2012, p.179).

2. O *Tallinn Manual* e os problemas de dissuasão no ciberespaço

Como foi dito, as opções da OTAN para manter a capacidade de dissuasão alargada são inseparáveis da atuação em concordância com a legalidade internacional, e será à luz deste princípio que se desenvolverá a análise que se segue.

Abordemos então o processo dedutivo que visará avaliar se as regras do *Tallinn Manual* têm efeitos diferenciados sobre cada dimensão do problema da dissuasão no ciberespaço, e se tais efeitos poderão variar dependendo da existência de um posicionamento oficial a respeito destas regras.

2.1. Os limiares e o enquadramento legal dos ciberataques

O primeiro passo desta análise pretende esclarecer como o TM contribui para a legitimidade das respostas dissuasórias no ciberespaço ao mesmo tempo que garante o nível de ambiguidade necessário para dissuadir com eficácia.

Sendo que o êxito da dissuasão se atinge apenas no caso em que não se ultrapasse o limiar que obrigue a materializar a ameaça de retaliação, o primeiro ponto a abordar é a legitimidade de ameaçar com o "uso da força", uma vez que à priori está proibido pelo Artigo 2.4 Carta das Nações Unidas (CNU). O TM contribui positivamente para ultrapassar este paradoxo uma vez que a Regra 12.4 confirma a legitimidade de ameaçar com "uso da força" quando este for legítimo. Vejamos então com que formas de uso da força é legitimo ameaçar.

Da definição de "uso da força", feita pela semelhança em escala e efeitos aos das operações nos domínios clássicos (Regra 11), decorre a necessidade duma avaliação quantitativa e qualitativa dos efeitos dum ciberataque para determinar se atinge tal consideração. A interpretação da regra evita concretizar a definição, mas exclui dela a espionagem *per se* e formas de coação como a económica e a política, a psicológica não destrutiva, o simples financiamento do hacktivismo ou facultar santuário aos hackers, porém, inclui certas combinações destas. Pelo contrário, qualifica "uso da força" todos os ciberataques constituintes de "ataque armado" segundo a Regra 13.

Fica sem esclarecer que ações não qualificáveis como "ataque armado" constituem "uso da força", mas com a proposta de as qualificar pela avalição que em cada caso fizer a comunidade internacional. Isto liga-se com o papel a desenvolver pelo *Tallinn Manual Process* no quadro da primeira etapa do ciclo de vida normativo. Assim, a abordagem interpretativa proposta assenta na severidade do dano e numa série de fatores qualitativos, nomeadamente, mas não só: severidade, imediatismo, retidão da cadeia causal, invasão, mensurabilidade dos efeitos, caráter militar, envolvimento estatal e presunção de legalidade.

Assim, a interpretação da Regra 11, estabelece dois limiares com a nitidez e flexibilidade apropriada para a dissuasão:

- "Uso da força" para determinar possíveis violações do Artigo 2 da CNU.
- "Ataque armado" para determinar o direito a responder com o "uso da força" sem violar a CNU.

A Regra 13 concretiza a aplicabilidade do termo "ataque armado" e o direito de autodefesa. O critério do Grupo de Peritos[5] é que não deve ser equacionado "ataque armado" com "uso da força", apesar desta posição não ser aceite por todos os Estados (Schmitt, et al., 2013, p.55). Só quando se ultrapassar deteminado limiar, avaliado em termos de escala e efeitos, o "uso da força" qualifica como "ataque armado" e é legitimo responder empregando a força.

Apesar de que o Tribunal Internacional de Justiça não tem fornecido uma guia para aplicar estes critérios é consensual entre os Peritos que qualquer uso da força que cause feridos ou mortos, ou provoque danos ou destruição de bens, qualifica como "ataque armado". Podemos estar, portanto, perante a fase emergente duma norma positiva para a dissuasão.

No caso de ciberataques que não atinjam os limiares do "uso da força" ou do "ataque armado" o critério do TM (Regra 6) é que os Estados têm responsabilidade legal internacional pelas ciberoperações que lhes sejam imputáveis e que constituam a violação de uma obrigação internacional. A responsabilidade estatal também será atribuível pela conduta de atores não estatais quando atuem seguindo instruções ou direção e controle dum Estado. Também será atribuível a responsabilidade aos Estados pelo fornecimento de certos tipos de apoio - como facilitar ciberamas - a atores não estatais, o que é muito relevante para dissuadir o recurso a empresas ou cibermilícias de voluntários no ciberespaço (Ottis, 2009, pp. 177-182).

Embora a interpretação e aplicação do Art. 8 dos Artigos sobre responsabilidade dos Estados por atos ilícitos internacionais (ONU, 2001) não seja simples, a promoção da sua aplicabilidade ao ciberespaço e o seu contributo para a evolução do direito consuetudinário (Machado, 2013, p.638) são muito positivas para a factibilidade da dissuasão. Ainda mais quando habilitam uma modalidade de respostas adicional: as contramedidas.

[5] O Grupo de Peritos que elaborou o TM, empregou os comentários às regras para exprimir as suas diferenças de critério quanto ao âmbito e aplicação das regras. (Schmitt, 2013, pp.6-7)

A Regra 9 interpreta a questão das contramedidas, legitimando respostas às ações ilegais do adversário no ciberespaço sempre que, sem ultrapassar o limiar de "uso da força", sejam proporcionais e com a finalidade de fazer retornar à legalidade.

A Regra 9 inclui ainda limitações adicionais cuja avaliação em relação à dissuasão não é simples. Quanto ao momento da aplicação, não haverá lugar a contramedidas se o dano cessou, embora os Peritos duvidem do caráter consuetudinário desta limitação. Quanto às precondições para as aplicar, há dever prévio de notificação ao Estado infrator, exceto no caso de "contramedidas urgentes", que os peritos consideram consuetudinariamente bem recolhidos. Ambas as limitações são positivas para a estabilidade (Machado, 2013, p.650), mas limitadoras da capacidade de resposta, pelo que terão impacto na estratégia de dissuasão a adotar.

Adicionalmente a Regra 9.8, contribui para a dissuasão alargada ao incluir a possibilidade da tomada de contramedidas por outros Estados que não o lesado.

Para além das contramedidas, a Regra 9 também comtempla a possível invocação do estado de necessidade no ciberespaço. Se bem que, partindo da perspetiva da dissuasão punitiva, as condições e as controvérsias relativas a tais invocações fazem incerto o recurso a esta figura. Incerteza acrescentada porque para alguns juristas o emprego da força estaria condicionado à reparação posterior dos danos causados (Espada, 1987, pp.131-135). Assunto diferente seria a justificação de medidas defensivas na invocação do estado de necessidade (Regra 9.12).

Por debaixo do limiar das contramedidas, os Peritos ainda consideram a possibilidade de empregar a retorsão como resposta inamistosa mais legal a ações inamistosas legais ou ilegais. Adicionalmente cabem outras respostas aos ciberataques no quadro da luta contra o crime (Schmitt, et al.,2013, pp.4, Regras 13.16 e 14.2). Portanto, podemos afirmar que o TM contribui para limitar as formas mais brandas de confrontação.

Quanto à possibilidade de respostas encobertas, há pouca a nenhuma possibilidade de as executar no quadro interpretativo do TM. (Regras 9 e 17).

Já foi exposto que a implantação por potenciais oponentes de ciberarmas latentes e ocultas nos sistemas próprios constitui uma séria ameaça a dissuadir no ciberespaço. A Regra 15.6 aborda este problema desde a perspetiva da autodefesa contra um ataque iminente no quadro do *jus ad bellum*. Assim, a inserção de bombas lógicas qualificaria como "ataque armado iminente", caso as condições específicas de ativação sejam susceptíveis de ocorrer. Questão diferente é a das ciberarmas de ativação remota, que só cumpririam o critério de

iminência se o adversário já tivesse decidido o seu emprego efetivo, assentando a legalidade da resposta defensiva na razoabilidade da avaliação feita pelo defensor. O TM também aborda a questão no quadro do *jus in bello,* o que é relevante para a dissuasão porque é aplicável desde as primeiras hostilidades (Mulinen, 1987, p.7). Neste caso, embora sem unanimidade entre os Peritos, a Regra 30.14 qualifica a instalação de ambos os tipos de ciberarmas como "ataque", sob a condição das consequências intencionais atingirem o limiar do dano, inclusivamente se não forem ativadas.

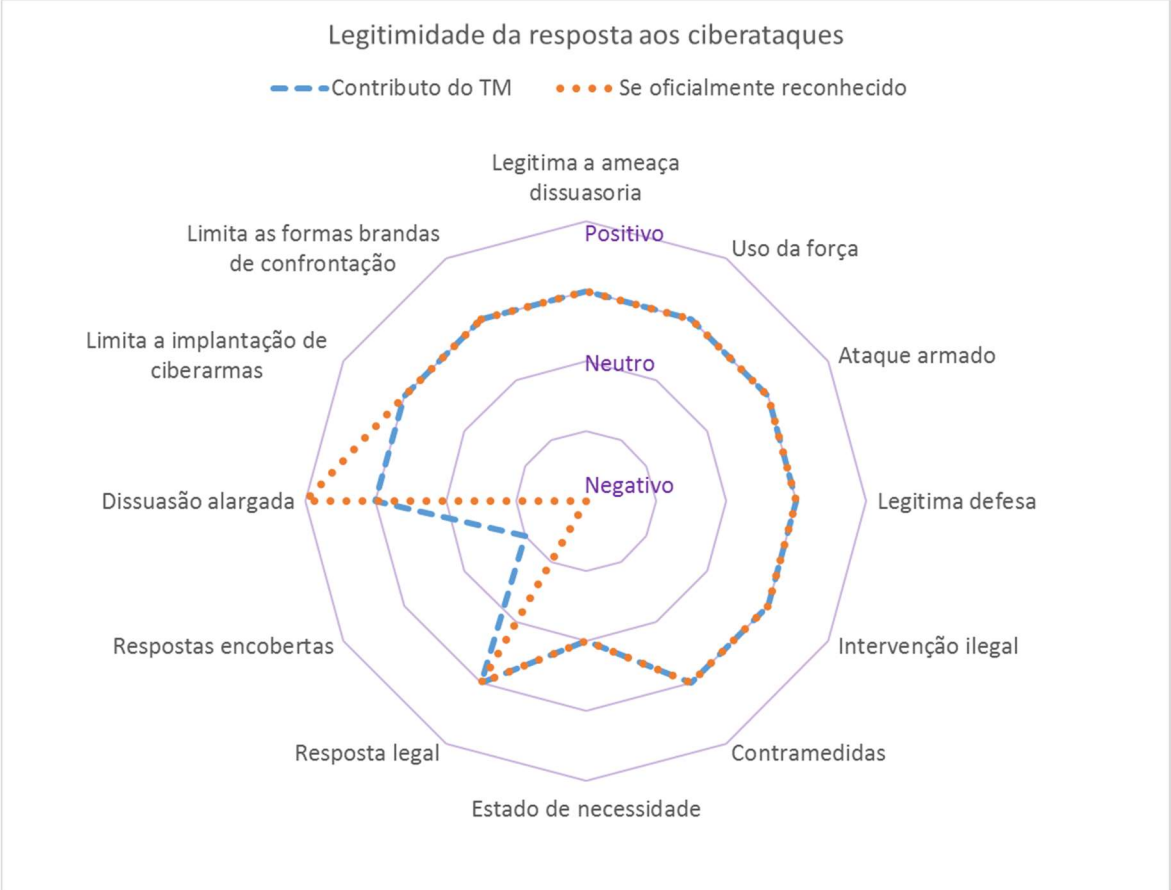

Figura 3 – Efeitos sobre a legitimidade da resposta aos ciberataques

Fonte: (Autor, 2017)

2.2. As regras, a ambiguidade e o fortalecimento da credibilidade

Acabamos de verificar que as interpretações do TM oferecem a possibilidade de responder legitimamente ao grande leque de ciberataques possíveis com um vasto repertorio de medidas legais. A possibilidade de empregar umas ou outras assenta na avaliação qualitativa e quantitativa da ofensa em termos de escala e efeitos (Regra 11), e na gradação da resposta segundo os princípios de necessidade, proporcionalidade, iminência e

imediatismo (Regras 14, 15). A capacidade e flexibilidade interpretativa atribuída ao atacado sobre estes assuntos garantem ao defensor a capacidade de ajustar a nitidez dos limiares, assim como a flexibilidade situacional necessária. Por exemplo, segundo a Regra 14.4 a necessidade julga-se desde a perspetiva do Estado atacado, e a Regra 15.9 permite ao atacado enquadrar em certas condições uma serie de ciberataques numa "ciber campanha" e continuar a legítima defesa até a campanha finalizar.

Estamos, portanto, em condições de afirmar que o TM contribui para estabelecer uma escala de limiares adequada para a dissuasão, cuja consolidação com a aceitação oficial do manual teria efeitos concluintes. Esta escala apresenta diferenças suficientemente claras entre patamares para permitir reconhecer a cada oponente o espaço de manobra que lhe é permitido e para distinguir se as iniciativas hostis do adversário passaram a um novo patamar. Mas também permite ajustar a nitidez dos limiares entre patamares para obrigar o adversário que não os quiser ultrapassar a deixar uma faixa de segurança.

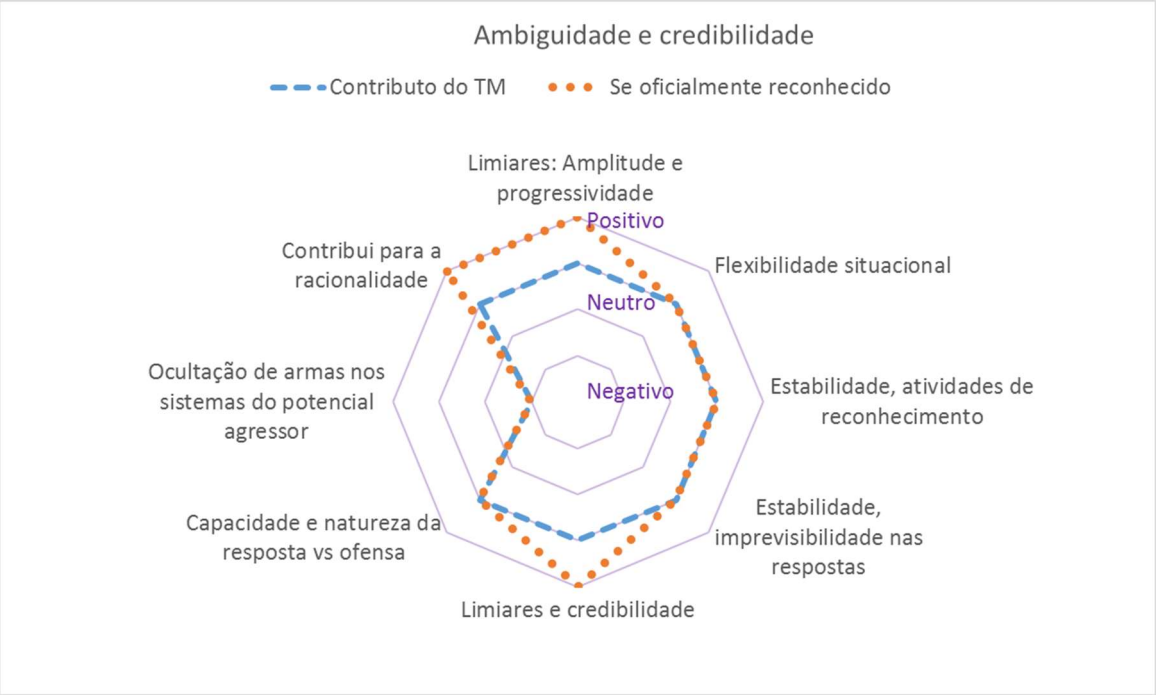

Figura 4 – Efeitos sobre ambiguidade e credibilidade

Fonte: (Autor, 2017)

O TM contribui para diminuir a instabilidade decorrente da ambiguidade limitando as atividades de reconhecimento de duas maneiras. Primeiro, coloca à disposição do defensor um leque de respostas legitimas contra atividades que não atingem o limiar de "ataque

armado". Segundo, a interpretação do princípio de proporcionalidade permite ao defensor um nível de imprevisibilidade adequado nas respostas. Assim, a Regra 14.5, para além de considerar que a natureza da força defensiva pode ser distinta da ofensiva, também interpreta que a quantidade de força legítima é dependente do contexto e, portanto, não está limitada pela quantidade de força empregue pelo atacante.

Por fim, contribui para a racionalidade porque no atual contexto de discrepância entre Estados quanto a aplicabilidade da lei atual aos assuntos ciber (Schmitt, et al.,2013, p.3), apresenta um modelo interpretativo que pode servir de referência para a avaliação racional das possíveis respostas dissuasórias do defensor (Deeks, 2015). Caso o TM fosse oficialmente aceite o modelo racional seria consolidado. Assim, ambiguidade, capacidade de resposta flexível e racionalidade contribuem para a credibilidade.

2.3. Soberania e a cooperação

Uma vez que o espaço onde o Estado pode exercer a soberania está definido pelas suas fronteiras, adotar medidas para assegurá-las demostra a determinação nacional para exercer a soberania, mesmo quando no ciberespaço a eficácia técnica da proteção possa ser reduzida. Assim as fronteiras podem constituir um instrumento para abordar os assuntos de segurança no ciberespaço e para comunicar a posição política nacional independentemente da localização física dos nodos. (Hare, 2009).

A Regra 1 reconhece que embora um Estado não possa pretender a soberania sobre o ciberespaço *per se*, sim pode exercer as prerrogativas da soberania sobre a infraestrutura e as atividades do ciberespaço dentro do seu território soberano. Tais prerrogativas incluem o controlo de acesso de acordo com a legalidade internacional e o direito exclusivo a exercer a jurisdição e a autoridade dentro do seu território. Adicionalmente as ciberoperações executadas por um Estado contra a infraestrutura localizada no território doutro Estado pode constituir uma violação de soberania. Fica, portanto, esclarecido o vínculo territorial das fronteiras no ciberespaço.

A problemática da não coincidência das fronteiras territoriais com as fronteiras de domínio é abordada com resultado positivo para os nossos fins na Regra 2, que estabelece a presença física ou legal de pessoas ou objetos como base principal para o exercício da jurisdição do Estado. Assim, a Regra 2.2 possibilita a jurisdição sobre entidades registadas na sua jurisdição, mas operando fisicamente no estrangeiro, também sobre os elementos no seu território administrados desde domínios registados no exterior. Adicionalmente, a Regra 2.3 esclarece a jurisdição sobe os sistemas distribuídos transfronteiriços, sendo que a

possibilidade dos dados e os processos residirem simultaneamente em múltiplas jurisdições, não impede o Estado de exercer a soberania no seu território. Com similar critério, a Regra 2.4 resolve a questão dos ciberataques a partir dos dispositivos móveis. Ainda confirma o exercício extraterritorial da jurisdição de acordo com a legislação internacional. Os contributos desta interpretação para a atribuição e a mitigação dos efeitos de terceiros são positivos, mas insuficientes para a dimensão do problema.

Em relação às fronteiras, a autoridade dos Estados para o controlo de acesso (Regra 1.4) e para restringir ou proteger total ou parcialmente o acesso à Internet (Regra 1.10) facilitam o controlo fronteiriço, quer efetivo, quer simbólico e perceptual (Andreas, 2001, pp.3,4).

Segundo o critério genérico do TM, assente em que o ciberespaço não constitui uma excepcionalidade legal, a questão da jurisdição é amplamente desenvolvida na Regra 2. Na Regra 3 quanto a Estados de Bandeira e Estados de Registo, e na Regra 4 quanto as questões de imunidade e inviolabilidade. O impacto do exercício da jurisdição sobre a atribuição e a mitigação do papel dos terceiros é evidente, e seria acrescentado pelo reconhecimento oficial do TM.

A cooperação também é facilitada, porque a Regra 1.8 legitima o consentimento dum Estado para que outro Estado execute ciberoperações a partir do território do primeiro. Por exemplo para complementar a capacidade técnica necessária para a defesa do seu ciberespaco.

Hare (2009, p.9-14) concluiu que a contribuição dum Estado para a cibersegurança pode influenciar outros Estados para atuar na mesma direção, até o ponto de a cooperação entre Estados chegar a delimitar uma fronteira de cibersegurança que deixa de fora os Estados não comprometidos, expostos às suas próprias ameaças e a ser assumidos como origem dos ciberataques. Na contribuição para esta segurança interdependente, sobressai a Regra 5, destacando: o facto de o direito internacional obrigar aos Estados a adotar medidas para impedir que desde o seu território se desenvolvam atividades, por eles conhecidas, contrarias aos direitos de outros Estados (Regra 5.3); a abrangência dos efeitos negativos a não permitir (Regra 5.5); a necessidade de avaliar em termos de natureza, escala e alcance os danos potenciais para ambos Estados para decidir sobre a intervenção (Regra 5.4); e a obrigação do Estado para requerer a intervenção de entidades privadas sob sua jurisdição quando for necessário (Regra 5.9).

Por fim, o TM contribui diretamente para a dissuasão alargada mediante a Regra 16, relativa à autodefesa coletiva, a Regra 19, relativa às organizações regionais, e mediante a comunicação da posição mais comumente aceite, embora não oficial, respeito à soberania no âmbito da OTAN (Regras 1 a 5). Os efeitos neste aspecto seriam resolutórios caso o posicionamento do TM fosse aceite oficialmente.

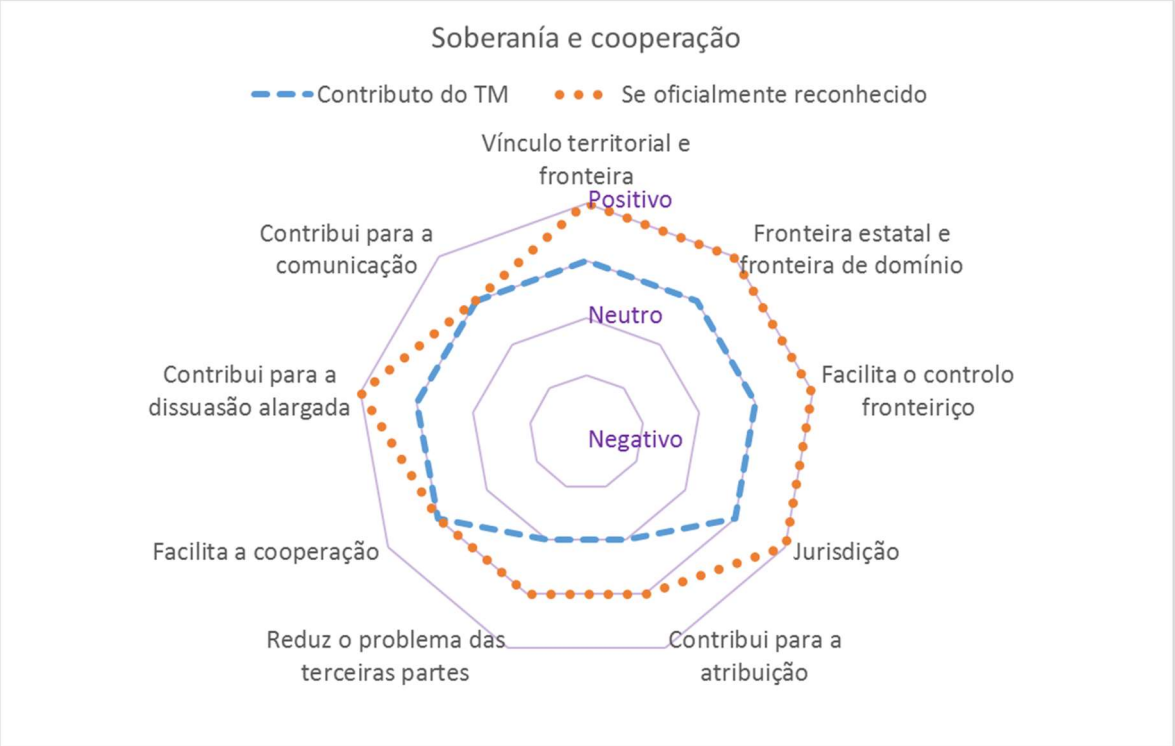

Figura 5 – Efeitos sobre a soberania e a cooperação

Fonte: (Autor, 2017)

2.4. As regras e os problemas de atribuição

O TM pode contribuir para ultrapassar as limitações decorrentes da demora do processo de atribuição técnica de duas formas.

A primeira, aportando os mecanismos legais para facilitar ao Estado um acesso mais rápido às evidências técnicas localizadas no espaço de soberania doutros Estados. O posicionamento geral do TM, não libertando os Estados da obrigatoriedade de cumprir no ciberespaço a legislação internacional - apesar de não terem uma orientação definitiva sobre a forma de o fazer - é o primeiro contributo (Schmitt, et al.,2013, p.3,14). Contudo, o mais relevante é o reconhecimento da jurisdição extraterritorial (Regra 2).

A segunda, permitindo certas respostas antes de o processo de atribuição técnica estar terminado, mas garantindo simultaneamente que o papel dos terceiros não leva à escalada.

Neste sentido, a posição do Chefe do *U.S. Cyber Command* (Alexander, 2010, p.11-12) é a de que no caso de um ciberincidente ser considerado um ataque que cumpre os critérios estabelecidos nas diretrizes ou regras políticas de empenhamento (SROE) para uma resposta em legítima defesa, poderiam tomar-se ações inclusivamente no caso de não ser identificado o atacante, sempre que se respeitassem os princípios de proporcionalidade e distinção. Mas a interpretação do TM não é tão simples. Aqui a questão a resolver é a possibilidade de distinguir quando previamente não se foi capaz de atribuir. No âmbito do *jus ad bellum* a Regra 13.21 condiciona a resposta em legítima defesa à identificação *ex ante* do atacante, mas no âmbito do jus *in bello*, a interpretação das Regras 49 e 50 à priori não necessita da identificação do atacante, mas sim duma delimitação do alvo restrita a objetivos militares legítimos. No âmbito do *jus ad bellum* o problema não termina com a identificação, porque não há unanimidade entre os peritos sobre a aplicabilidade da autodefesa contra todo tipo de atores (Regra 13.14-17). Todavia há outra saída: atribuir politicamente, o que adicionalmente permite preservar as técnicas forenses próprias.

No salto qualitativo para a legitimação da atribuição política, o incumprimento por um Estado das suas obrigações de controlo sobre a infraestrutura cibernética colocada no seu território ou sob o seu controlo exclusivo, seja de *jure* ou de facto, em geral e sem limitar-se aos casos de "uso da força" ou "ataque armado" (Regra 5), pode ser considerado como peça de evidência política, por exemplo no caso da Estónia em 2007 (Artiles, 2010, pp.179-180). A Regra é especialmente útil nos casos em que um Estado depois de ser notificado não adote medidas exequíveis para por fim aos ataques (Regras 5.6, 13.22), mas não é concluinte quanto à obrigação de policiamento dos Estados no ciberespaço, nem quanto à aplicabilidade aos Estados pelos que são roteadas as ciberoperações (Regras 5.11, 5.12). Adicionalmente, a Regra 6 contribui para a atribuição política quando permite atribuir responsabilidades aos Estados pela conduta de atores não estatais sob controlo ou seguindo instruções dum Estado, e também por omissões.

A possibilidade de escalada decorrente do papel de terceiros, nos casos de atribuição técnica imperfeita, é mitigada pelas restrições legais decorrentes do TM. Assim: a Regra 6.12 não permite atribuir a responsabilidade estatal exclusivamente pela localização geográfica de atos ou atores; a Regra 7 exige peças complementares e uma avaliação contextualizada para concluir a responsabilidade dum Estado por ciberataques originados na sua própria infraestrutura governamental; a Regra 8 considera insuficiente para atribuir responsabilidade a um Estado o roteamento de operações através da infraestrutura localizada

no seu território; for fim, a Regra 11.5, embora não por unanimidade dos Peritos, considera que facultar santuário a cibertacantes não estatais não basta para atribuir responsabilidade e deve estar ligado a outros atos.

Uma das consequências da atribuição política, é o emprego por alguns Estados para justificar restrições à privacidade ou à liberdade de expressão no ciberespaço. Embora o TM só aborda diretamente este assunto em relação com as obrigações da potência administradora no âmbito do *jus in bello* (Regra 88.3), devemos salientar a unanimidade dos Peritos quanto à aplicabilidade dos princípios do direito internacional no ciberespaço (Schmitt et. al, 2013, p.12). Portanto, implicitamente apoia a aplicabilidade no ciberespaço da Declaração Universal dos Direitos do Homem ou do Convénio Internacional sobre Direitos Civis e Políticos patrocinado pelas Nações Unidas. Apesar do ciberespaço ser posterior a estes convénios, o termo "por quaisquer meios" não deixa dúvida da sua vigência. Apesar de tratarmos direitos fulcrais, estes não são absolutos e devem ser avaliados em relação a outros como a reputação de terceiros ou a segurança nacional, adicionalmente a cultura exercerá uma notável influência ao balançar liberdades individuais e interesse público. Importa destacar que os Estados têm obrigações positivas, para assegurar o exercício dos direitos fundamentais, e negativas, para se autolimitar no constrangimento destes direitos. (Tikk, E., Kaska, K. e Vihul, L., 2010, pp.40-46). Uma vez que o custo da atribuição política pode ser a cessação de direitos e que o TM aponta respostas só indiretamente, avaliamos o impacto como neutro.

Para se proteger contra os riscos de sofrer a atribuição política decorrente das atividades de terceiros, é fundamental que os Estados adotem medidas para o setor privado se envolver na implementação de medidas de segurança no ciberespaço. Embora o TM não aborde a cibersegurança (Schmitt et. al, 2013, p.12), devemos retomar aqui a questão da responsabilidade estatal por ação ou omissão (Regra 6) e as obrigações estatais de controlo do ciberespaço soberano (Regra 5). Seguidamente salientamos dois casos onde é relevante o papel do setor privado:

Primeiro, no caso da ação capaz de acabar com uma ciberoperação só puder ser executada por uma entidade privada, a Regra 5.9 concorda na obrigação dos Estados de adotar todas as medidas à sua disposição para requerer que tal entidade adote as medidas necessárias para detê-la.

Segundo - embora sem unanimidade entre os peritos - no caso da possível responsabilização dos Estados que não adotem medidas razoáveis para impedir o roteamento duma ciberoperação pelo seu território (Regra 8.2).

Portanto, embora o TM não coloque regras de obrigatoriedade estatal para regulamentar as condições de segurança que devem ser impostas ao setor privado no ciberespaço, coloca o risco de os Estados despreocupados por tal segurança responderem pelas atividades ilegítimas de terceiros. Ciente dos riscos duma segurança inapropriada no ciberespaço soberano, e numa fase do ciclo de vida normativo mais evoluída que o TM, a Diretiva UE 2016/1148 (UE, 2016) coloca sobre os Estados membros a obrigação de traspor para a sua legislação a regulamentação duns padrões mínimos de segurança também para os atores privados (Millás, 2017).

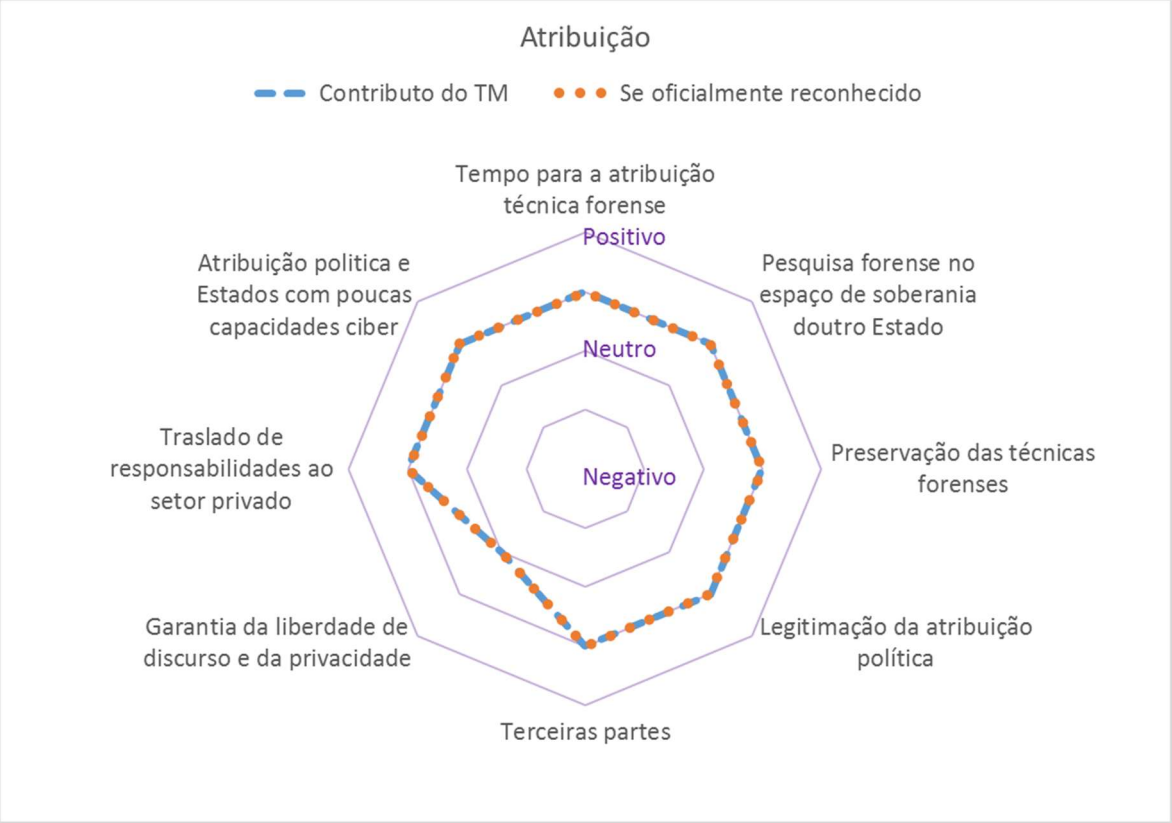

Figura 6 – Efeitos sobre os problemas de atribuição

Fonte: (Autor, 2017)

Por fim, abordamos os contributos do TM para mitigar os problemas da atribuição política a Estados incapazes de aplicar políticas de segurança adequadas. Neste aspecto, a Regra 7 limita o risco de atribuições incorretas quando os ataques forem iniciados a partir

de infraestruturas governamentais, ou de privados em funções governamentais, ao exigir provas adicionais contextualizadas para atribuir a responsabilidade ao Estado em questão. Numa perspetiva diferente, os Comentários 13.23 e 13.24 abordam a legitimidade de lançar operações defensivas a partir dum Estado ao qual não foi atribuído o ataque. No caso desse Estado consentir não há dúvida da legitimidade, mas em caso contrário, e sem consentimento do Conselho de Segurança da ONU (CSNU), não há consenso entre os Peritos. A maioria argumenta que seria legitimo, embora exigindo garantias adicionais contextualizadas (Regra 13.23), porque esse Estado estaria permitindo atos ilegais prejudiciais para outro Estado (Regra 5). Outros argumentam que a intervenção deveria assentar noutros fundamentos jurídicos, como o "estado de necessidade" (Regra 9). Portanto, o contributo do TM é levemente positivo, mas insuficiente, daí a necessidade de cooperar com aqueles países que não atingem os padrões mínimos de segurança no ciberespaço.

2.5. As regras, a capacidade e a credibilidade

No Apêndice B abordaram-se, tendo como ponto de partida a perspetiva técnica e de emprego estratégico, as dificuldades para obter e manter uma adequada capacidade de retaliação no ciberespaço. Aqui abordamos o desempenho do TM para ultrapassar essas dificuldades ou para empregar capacidades alternativas.

Começando pela capacidade de destruição de ciberarmas do adversário, de termos a capacidade técnica de o fazer, o TM não é conclusivo quanto à legitimidade dos ataques necessários para tal. Assim, não há acordo entre os Peritos quanto à legitimidade da "autodefesa antecipatória" porque não está explicitamente prevista no Artigo 51 da CNU. A aproximação ao problema que melhor se adapta ao caso em estudo, é a adotada pela maioria dos Peritos, assente na legitimidade da "autodefesa antecipatória" se o ataque defensivo se desencadeia na "última janela de oportunidade viável" para deter o atacante. É de salientar a unanimidade dos Peritos para rejeitar a tese de a "autodefesa antecipatória" ser só legitima depois de lançado o ataque, pois a velocidade dos eventos no ciberespaço faria esta opção ineficaz (Regra 15.2-15.5). Todavia a Regra 15.7 considera ilegítimos os ataques preventivos, reforçando assim a probabilidade de êxito da dissuasão (Knopf, 2010, p.7).

Estreitamente ligado com o anterior, está o problema decorrente da erosão mútua de capacidades ofensivas e de retaliação para as quais o TM não aponta nenhuma solução direta. Embora seja quase impossível destruir as ciberarmas armazenadas pelo potencial adversário, é possível tirar-lhes a efetividade, corrigindo as vulnerabilidades que exploram. A dificuldade está em encontrar essas vulnerabilidades antes de as ciberarmas serem

empregues. O atual debate (Goldman, 2015, p. 321) sobre os benefícios de os governos publicarem as vulnerabilidades destetadas, para que possam ser corrigidas, aponta para a possibilidade de adotar uma normativa que contribua para a estabilidade global, assunto que abordaremos no Capítulo 3.

Todavia, uma possibilidade para proteger a capacidade de resposta própria do desgaste, seria explorar vulnerabilidades nos sistemas do potencial agressor, para implantar neles ciberarmas ocultas que continuem a ser efetivas depois de fixar as vulnerabilidades iniciais (Bejtlich, 2005, pp.17,18). Aqui são apenas de interesse as ciberarmas de ativação remota no quadro do *jus ad bellum.* A Regra 15.6 considera que não incorreríamos em "ataque armado iminente" ao empregar este mecanismo intrusivo para garantir as capacidades próprias, pois essa condição só se cumpriria no caso de já termos decidido o emprego efetivo da ciberarma. Apesar disso, o facto de o TM colocar a faculdade de avaliação na razoabilidade de quem sofre a colocação da arma, não libera este mecanismo dum risco político e de credibilidade significativo.

No referente à capacidade de defesa ativa, na sua modalidade de contra ciberoperação automática sobre computadores atacantes, para além de não aportar soluções eficazes aos problemas operacionais e técnicos (Libicki, 2009a, p.61), o TM acrescenta uma dificuldade legal, desde que a Regra 41.4 inclui a ciberdefesa ativa na lista de "métodos de guerra", acrescentado a possibilidade de considerar a operação como um ataque no âmbito do *jus in bello* (Regra 30), com as respetivas obrigações, algumas, como a obrigação de verificar os alvos (Regra 53), difíceis de aplicar num sistema de resposta automática.

No caso de não se cumprir as condições apropriadas para uma resposta pública, o emprego não publicitado (*sub-rosa*) da capacidade de resposta permitiria ultrapassar certas limitações (Libicki, 2009a, pp.92-102). No caso da legitima defesa, a interpretação do TM limita parcialmente esta possibilidade, porque as medidas adotadas devem ser imediatamente comunicadas ao CSNU (Regra 17) e não o fazer constitui, para os Estados membros, uma violação do artigo 51 da CNU. Mas este facto não retira aos Estados o direito de legitima defesa uma vez que a obrigação de comunicação não constitui direito internacional consuetudinário. Neste sentido, a maioria dos Peritos concordam que o exercício do direito de autodefesa poderá continuar até que o CSNU retire esse direito ao Estado em questão e adote as medidas oportunas. A nível de contramedidas, a Regra 9.4 estabelece a obrigação não absoluta de pedir ao agressor que cesse a sua atividade ilícita antes de recorrer às contramedidas, mas considera direito consuetudinário a possibilidade de empregar

"contramedidas urgentes" na preservação dos direitos do estado, mesmo antes da lesão. A nível de retorção também não há obrigação de comunicação pública ou privada, desde que se trata de repostas legais, embora inamistosas. Esta interpretação resulta positiva em termos gerais, com a exceção do custo político que pode supor a violação da CNU no caso da atuação em legitima defesa sem informar ao CSNU e das limitações para o emprego de contramedidas sem informar o agressor.

Demonstrada a dificuldade técnica e legal de responder empregando ciberarmas, encontramos uma saída ao problema na aplicação dos critérios de necessidade e proporcionalidade (Regra 14). O critério de necessidade permite adotar medidas ciber ou cinéticas[6] razoáveis ao nível do "uso da força". Adicionalmente, o critério de proporcionalidade não restringe a quantidade de força à empregue pelo atacante, senão à necessária para estabelecer uma defesa efetiva de acordo com o contexto e os limites de escala, alcance, duração e intensidade necessários para deter o ataque. E o mais relevante, não é necessário que a natureza da força defensiva seja a mesma que a ofensiva, pelo que se podem ultrapassar as limitações das ciberarmas respondendo noutro domínio das operações ou atacando o nível físico com armas cinéticas.

Por debaixo do limiar do uso da força, também não é necessária uma identidade na natureza das contramedidas e das ações que as motivaram (Regra 9.7), constituindo as cibercapacidades um recurso adicional do Estado vítima para responder com proporcionalidade.

Já vimos que as caraterísticas técnicas das ciberarmas dificultam o emprego da ameaça cibernética para atingir efeitos específicos sobre o ciberespaço, o que pode ter um efeito significativo na credibilidade. A esta dificuldade acrescenta-se que a Regra 11 não é capaz de resolver a questão das ações que não constituindo "ataque armado" constituem "uso da força". Concluindo que na ausência dum limiar claramente definido, os Estados devem ser muito sensíveis à provável avaliação da comunidade internacional (Regra 11.8). Esta interpretação permite considerar uma nova capacidade de retaliação no ciberespaço, orientada a obter um balanço favorável da opinião pública internacional em relação à ofensa e à retaliação (Smith, 2009, pp.51-54, Libicki, 2012, pp. 14,39,46,49). Em relação a esta capacidade, abordamos de seguida as cibercapacidades de interferência política coativa.

[6] Medidas de guerra convencional que podem causar diretamente danos físicos, feridos ou mortos. (Applegate, 2013) inclui uma interessante discussão sobre *Kinetic Cyber*.

Nomeadamente, em relação ao termo "armas de informação" introduzido na proposta inicial do Código Internacional de Conduta para a Segurança da Informação (ONU, 2011b, p.4) liderado pela Rússia e pela China, é passível de se considerar uma resposta a eventos similares às Primaveras Árabes (Thomas, 2017, p.8), para classificar aplicações como o Twitter ou o Facebook[7]. Esta posição não é apoiada por muitos Estados no interesse da liberdade de expressão e de informação no ciberespaço (Rõigas, 2015). O TM aborda a questão em relação à proibição do uso da força (Regra 10.11), para concluir que algumas formas de interferência política coativa através do ciberespaço podem constituir uma intervenção ilegal. Aqui, o teste decisivo é a coerção, pelo que se pode ajustar o nível de coação, para adotar medidas de retorção ou contramedidas, sendo um contributo para o defensor. Os oito critérios de avaliação incluídos na Regra 11.9 podem constituir uma ajuda efetiva para sensibilizar a comunidade internacional sobre a necessidade dum determinado nível de resposta.

Evidentemente, a avaliação da credibilidade de emprego da capacidade retaliatória deve ser feita no quadro teórico da dissuasão ter falhado. No caso de falhar a dissuasão nuclear as consequências seriam catastróficas. Em contraste, no ciberespaço à priori não será assim, mas os efeitos colaterais poderão alcançar outros domínios (Cimbala, 2016, p.57). Daí que o dissuasor, para fazer credíveis as capacidades de resposta (Brodie, 1958, pp.23-24), possa avaliar os limites legais com maior amplitude no caso nuclear que no ciber. Portanto, as potenciais respostas no segundo caso devem limitar-se ao ordenamento do *jus ad bellum* (NATO, 2016). Consequentemente, as armas empregues devem permitir atingir alvos claramente definidos com efeitos concretizados, assim como a avaliação de danos prévia e posterior ao ataque retaliatório (Regras 43 a 59). Sem abordar em detalhe este conjunto de regras, é importante salientar que o TM analisa profundamente o alcance jurídico efetivo destas limitações, reduzindo a incerteza ao estabelecer um critério racional de avaliação que resulta positivo para fazer credível a factibilidade do emprego de cibercapacidades ofensivas partindo do respeito do ordenamento jurídico vigente.

Por fim, devemos referir que não foi possível estabelecer qualquer relação causal entre o TM e as possibilidades de verificação que pudesse contribuir para efetivar acordos de desarmamento no ciberespaço. Embora como comentávamos ao início desta seção, no

[7] A relevância do termo "armas de informação" não foi percebida por todos, assim o significado na tradução para o espanhol (ONU, 2011a, p.4) mudou para "armas informáticas" equivalente a ciberarmas.

próximo capítulo abordar-se-ão outros mecanismos que podem contribuir para a redução de armamento no ciberespaço.

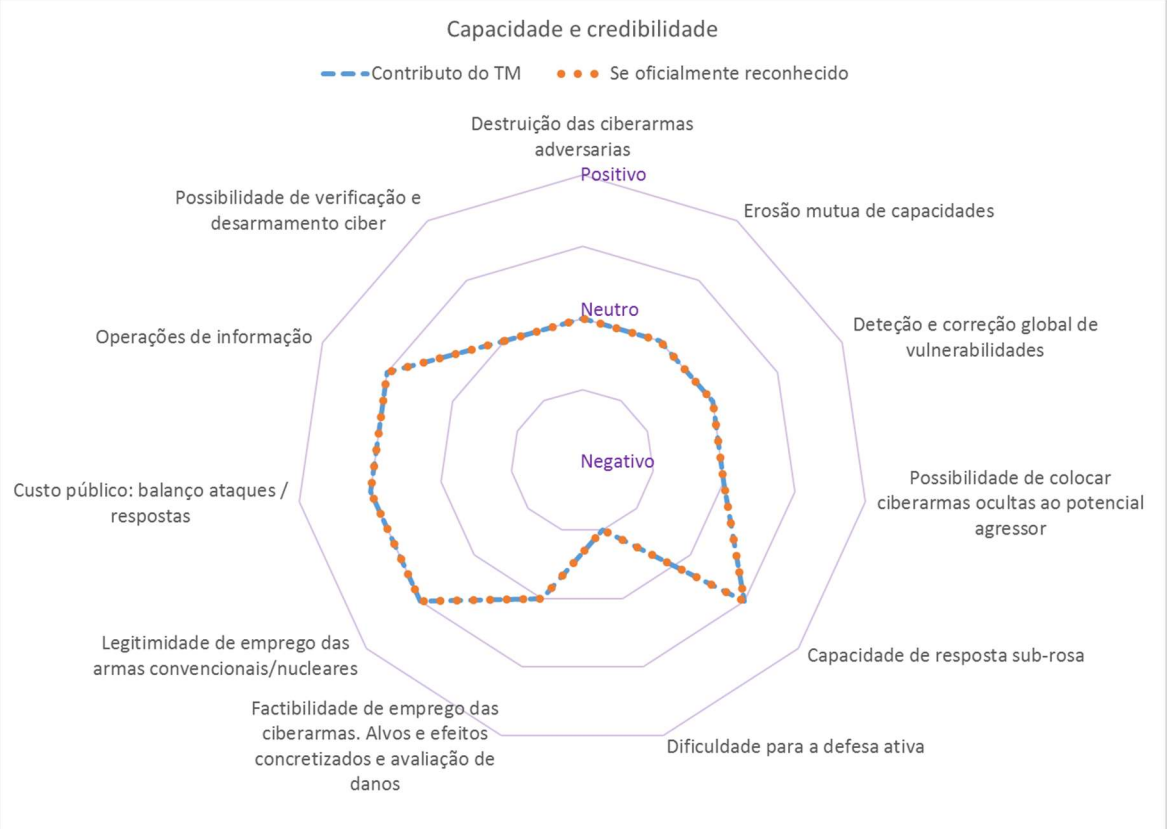

Figura 7 – Efeitos sobre as dimensões de capacidade e credibilidade

Fonte: (Autor, 2017)

2.6. gaComunicação e sinalização

A comunicação é um dos grandes problemas para a dissuasão no ciberespaço, complicado ainda mais pelo segredo das atividades nesse ambiente (Goldman, 2015, p.317,320). Neste sentido, verificamos ao longo deste trabalho que o TM, constitui *per se* uma potente ferramenta de comunicação, pois visa estabelecer um marco jurídico conceitual que permite o intercâmbio de mensagens com baixa probabilidade de erro na comunicação, transmite os limites em que devem desenvolver-se as atividades legítimas, abrindo a porta à legitimidade de responder pela força em certos casos e interpreta um elevado número de preceitos com a ambiguidade necessária para não fechar a porta à negociação com aqueles Estados que abordam a questão numa perspetiva diferente, ou que estão vinculados por Tratados distintos dos considerados pelo TM (Schmitt, 2013, p. 6). Nesta dimensão o TM não pode ser avaliado como instrumento isolado, senão no contexto do *Tallinn Manual*

Process, que pode considerar-se um potente processo de comunicação na fase de impulso e persuasão para conseguir que uma quantidade crítica de Estados aceite esta interpretação normativa comum. Daí que um posicionamento oficial respeitante à interpretação das regras possa ser prejudicial no momento atual, ao fechar as portas para a negociação que permita incorporar novos Estados ao processo. Assim, o posicionamento atual facilita vias para mudar as regras e permite mitigar o risco de que a prática legal no ciberespaço deixe para trás o entendimento mútuo quanto ao regime legal aplicável (Schmitt, et al., 2013, p.3,43).

Portanto, desde a perspetiva da sinalização, facilita a assimilação da mensagem implícita nas respostas, pois facilita o padrão de referência das atitudes que não são admissíveis, contribuindo para facilitar a percepção dos sinais. Como vimos na seção anterior, facilita a comunicação das capacidades dissuasórias que podem ser empregues e a factibilidade de as empregar respeitando a legislação internacional. Ainda mais, permite estabelecer uma narrativa pré-crise alargada que reflete os valores éticos nos que fundamentar as narrativas a empregar durante os processos de gestão de crises (Libicki, 2012, p.71).

O manual também contribui para permitir a intepretação correta dos sinais e o reajuste de atitudes, ao retirar legitimidade a algum dos mecanismos que não deixam tempo para decidir numa escala temporal humana. Assim, a rejeição unânime dos Peritos à interpretação da "autodefesa antecipatória" só ser legitima depois de lançado o ataque (Regra 15.3), contribui para a exclusão desta ferramenta da caixa da sinalização, permitindo substituí-la pela opção da "última janela de oportunidade" (Regra 15.4), muito mais apropriada para a gestão temporal da sinalização.

Conclui-se esta secção em condições de afirmar que, desde a perspetiva da sinalização, o TM contribui para a melhor qualidade dos limites em que se deve desenvolver a atividade dos Estados no ciberespaço. Limites discretos, distintos e finitos (ataque armado, uso da força, atuação ilegal, ação inamistosa, delito privado e, embora com diferente fundamento, estado de necessidade) avaliáveis qualitativamente em termos de escala e efeitos (Regras 11-15), mas também naturais e óbvios desde que assentam no princípio da aplicabilidade do direito internacional vigente ao ciberespaço, contextualizado em termos de alcance e aplicabilidade (Schmitt, et al., 2013, pp.5,6).

Figura 8 – Efeitos sobre as dimensões de comunicação e sinalização

Fonte: (Autor, 2017)

Ao longo deste capítulo analisaram-se os efeitos das interpretações do TM sobre cada dimensão do problema da dissuasão no ciberespaço, por forma a responder à primeira pergunta derivada. O processo permitiu verificar que os efeitos do TM sobre as dimensões mais problemáticas para a dissuasão no ciberespaço são diferenciados a nível de indicador e que, embora possam variar dependendo da existência dum posicionamento oficial respeito do TM, o efeito sobre as estratégias de dissuasão de tal posicionamento é muito menor do que à priori se podia pensar.

Adotando como ponto de partida os resultados deste capítulo, na procura duma resposta à segunda pergunta derivada, aborda-se de seguida a análise de compatibilidade do *Tallinn Manual* com as opções de dissuasão no ciberespaço.

3. Impacto das regras do *Tallinn Manual* nas opções para a dissuasão

Os avanços legais não só fornecem fatores que devem ser considerados no desenvolvimento doutrinal da dissuasão, como também aportam visões sobre as melhores formas de empregar a teoria da dissuasão para atingir fins estratégicos (Jensen, 2012, p.779). Avancemos então na procura de resposta à nossa segunda pergunta derivada, para determinar o impacto do TM nas opções de dissuasão.

3.1. Dissuasão punitiva

No capítulo anterior avaliou-se como positivo o impacto do TM sobre a dificuldade de atribuição, mas vejamos se é suficiente para uma dissuasão punitiva efetiva. Devemos considerar que antes da atribuição política é necessária alguma evidencia forense que, embora não se publique, oriente a decisão e permita articular um conjunto de evidências contextualizadas e sustentáveis politicamente (Waxman, 2011, pp.443-445). Mas o tempo necessário para a ação forense diluí a possibilidade duma resposta legítima, ainda tentando enquadrá-la numa "ciber campanha" (Regra 15.9). Perder-se-ia assim a qualificação de autodefesa para entrar no terreno da mera retaliação (Regra 15.8). No caso dos ciberataques não detectados durante algum tempo também não será possível a resposta legítima contundente, exceto no caso da Regra 15.9, que será mais difícil de justificar quanto mais tempo passe.

Ainda há outro problema fulcral não solucionado, a exigência da atribuição *ex ante* para legitimar a autodefesa no *jus ad bellum.* Porque se bem que a dificuldade é ultrapassável no âmbito do *jus in bello* (Regras 49 e 50), a sua aplicabilidade confirmaria que a dissuasão já falhou.

Os avanços na determinação da soberania são positivos, em especial quanto ao que significam para a atribuição política, em relação às obrigações de controlo dos Estados sobre a infraestrutura cibernética (Regras 5,6,13). Mas a exigência de reforçar com evidências adicionais a atribuição assente na soberania limita a dissuasão punitiva. Porque perante ciberoperações similares, nem sempre se estará em condições de responder legitimamente com similar intensidade e em tempo oportuno, o que pode afetar muito negativamente a dissuasão nas dimensões de comunicação e sinalização. Já que a sinalização usa ações para comunicar a seriedade do assunto em discórdia (Libicki, 2012, p.62).

Quanto aos limiares ativadores da resposta decorrentes das regras do TM (ataque armado, uso da força, ação ilegal, ação inamistosa e crime imputável a uma pessoa física ou

jurídica) vimos na secção 2.1 que cumpriam os critérios apropriados para uma comunicação, sinalização e credibilidades efetivas.

Desde que a dissuasão punitiva assenta na ameaça de castigo, a capacidade de resposta é fulcral. Já vimos que o TM, dificulta a defesa ativa e não permite avançar na solução dos problemas da capacidade de destruição das ciberarmas adversarias, da erosão das cibercapacidades de retaliação, ou da pré-implantação de armas nos sistemas do oponente. Portanto, a aplicação de mecanismos de ciberdissuasão punitiva parece pouco viável. Embora positivas, as soluções que aporta o TM quanto à legitimação do emprego das ciberarmas não permitem a balança reverter a favor da ciberdissuasão punitiva. Ainda pior, podem legitimar o aumento de tensão decorrente dos efeitos colaterais dos ciberataques. Sendo possível chegar a incorrer em "ataque armado" contra terceiros Estados, com independência de qual fosse o propósito do retaliador (Regras 13.12 e 13.9). Apesar destas situações nem sempre provocarem uma resposta em autodefesa, elas podem ter outros custos, especialmente a nível político. Contudo, não se pode descartar o risco de escalada do conflito noutros domínios e da confrontação, por exemplo, nuclear. Caso uma resposta inabilitasse os canais de comunicação político militar em condições de pressão, poderiam ativar-se respostas por delegação aos níveis subordinados, por receio de perder as opções de resposta, ou por redução das opções consideradas às mais potentes, face ao risco de estar confrontando a última opção (Cimbala, 2016, pp.58,59).

Por conseguinte, para a dissuasão punitiva ser eficaz é preciso sair do paradigma da ciberdissuasão e recorrer a outras capacidades de reposta. É aqui que o TM traz um dos grandes contributos para as estratégias punitivas, legitimando o emprego das armas convencionais ou nucleares (Regra 14.5). Permite assim tirar os benefícios de responder em todo o espectro das operações (Jensen, 2012, p.795), incluídas as operações de informação para as que já vimos que o TM contribui positivamente (Smith, 2009). As respostas neste domínio podem contribuir para mitigar o custo político de medidas cujas causas e efeitos são difíceis de transmitir ao público (Libicki, 2012, pp.47-49)

Outro problema ainda não controlado da dissuasão punitiva no ciberespaço é que as respostas para dissuadir a uns atores podem ser o incentivo para outros (Jensen, 2012, p.783). O contributo fundamental do TM em relação a terceiros é exigir garantias solidas de atribuição e de resposta para mitigar os efeitos interferentes daquelas, o que nos convida a pensar em estratégias não assentes na punição.

Apesar dos avanços decorrentes do *Tallinn Manual Process*, a dissuasão punitiva ainda não oferece respostas a outros problemas, como a detecção e correção de vulnerabilidades a escala global ou os processos de desarmamento no ciberespaço.

Portanto, é necessário analisar outras estratégias dissuasórias.

3.2. Dissuasão defensiva

Até chegar a este ponto, foi-se verificando que a dissuasão no ciberespaço, está muito limitada, quase até a inutilidade, pelo anonimato, o alcance global, a natureza distribuída e a interconexão do domínio cibernético (Lan e Xin, 2010, p.1). Dificuldades estas que se acrescentam no caso da dissuasão punitiva, e ainda mais no caso da ciberdissuasão punitiva. Depois de verificar na secção anterior que o TM, embora positivo, não permite ultrapassar os obstáculos necessários para uma dissuasão punitiva efetiva no ciberespaço, abordaram-se as estratégias de dissuasão defensiva.

A capacidade de atribuir com eficácia e em tempo oportuno era um dos grandes problemas para a dissuasão punitiva. Porque a impossibilidade de atribuir com um grau de certeza adequado à severidade da resposta dificulta a decisão política para responder no âmbito do *jus ad bellum,* minando as estratégias punitivas (Solomon, 2011, p.10-11). Porém, a partir de uma abordagem defensiva, o problema dilui-se porque a severidade da resposta não tem um papel fulcral na avaliação de custos e ganhos do potencial agressor. Ainda assim, a estratégia pode incluir respostas para acrescentar os custos do atacante, que geralmente serão de tipo político, por exemplo introduzindo elementos de "deslegitimação" (Wilner, 2011, pp.26-33). Estas respostas estarão normalmente por debaixo do limiar das contramedidas (Regra 9.13), ou dentro do âmbito da perseguição criminal (Regras 1, 2, 3, 13.16 e 14.2). Esta última medida pode atingir dimensões politicas muito relevantes, especialmente se forem imputados por crime funcionários doutros Estados (Hvistendahl, 2016). Assim a questão dos limiares deixa de ser um assunto fulcral, e o posicionamento do TM é plenamente compatível com a estratégia, embora o tema da cibersegurança desde a abordagem da luta contra o crime fique fora do âmbito do TM.

A dimensão da soberania é fulcral para as estratégias defensivas, pois nela assenta o domínio reservado aos Estados para lidar com terceiros e face a organizações internacionais (Miranda, 2016, pp.243). E, portanto, a capacidade para exercer o controlo das suas fronteiras no ciberespaço, para impor as obrigações necessárias para assegurar o ciberespaço no seu território e para exercer a jurisdição sobre as empresas do setor registadas no Estado. Na secção 2.3 concluiu-se o impacto positivo do TM nesta dimensão, mas devemos salientar

aqui a importância dalgumas regras pelo que contribuem para aumentar a resiliência do ciberespaço: da Regra 1.5, quanto ao direito exclusivo do Estado para exercer o controlo regulatório e legal da ciberinfraestrutura no seu território, não importando a finalidade nem a titularidade da propriedade; da Regra 1.10 quanto à capacidade do Estado para limitar ou proteger o acesso à Internet, sem prejuízo da legislação internacional aplicável; e da regra 5.9 relativa à obrigação do Estado para requerer a intervenção de entidades privadas sob a sua jurisdição quando não houvesse outra opção para pôr fim às ciberoperações que desde o seu território afetem outro Estado.

Na dimensão das capacidades, a primeira grande limitação para a dissuasão defensiva é técnica. Porque atualmente não é possível atingir a resiliência total dos sistemas e a transição para protocolos mais seguros como IPv6, embora podendo corrigir algumas deficiências, mas não trará a solução definitiva (Geers, 2012, pp.2,3,8)[8]. Duma perspetiva jurídica foram confirmados os contributos positivos do TM para promover a segurança no ciberespaço, especialmente no âmbito da jurisdição e da responsabilidade estatal. Também se verificou como se começam a materializar as medidas legais na EU (UE, 2016) e, embora ainda com caráter fundamentalmente de implementação voluntaria, nos EUA (U.S. Congress). 2014 e U.S. President, 2015). Contudo, visto que para atingir o sucesso completo mediante a dissuasão defensiva, o atacante não deve perceber nenhuma possibilidade de sucesso (Jensen, 2012, p.807), é necessário avaliar a capacidade de combinação com medidas de caráter punitivo. Aqui surge um novo problema, porque o fortalecimento da resiliência, na medida que diminuem os danos efetivos, isto é, os "efeitos", pode anular a legalidade da resposta em autodefesa (Regra 11) ou com contramedidas (Regras 5.5, 9.7, 11 e 13). O facto de que quanto maior for a segurança do sistema vulnerado, maior será o nível de invasão a considerar na avaliação de efeitos (Regra 11.9.d), mitiga levemente o problema. Tendo como ponto de partida a abordagem defensiva, importa salientar que enquanto o atacante desgasta as suas capacidades em cada ciberataque, o defensor obterá informação monitorizando os ataques (Jensen, 818) e manterá bem protegidas as ciberarmas próprias.

Adicionalmente, o facto de assentar mais em capacidades de ciberdefesa passiva que ativa, no sentido das respostas automática, acrescenta à dissuasão defensiva um aumento de compatibilidade com o TM.

[8] A transição a IPv6 decorre com lentidão. A 21MAY17 só o 17,88% dos usuarios que accedían a Google o empergaban (Google, 2017).

A credibilidade da abordagem defensiva, também será superior, não só pela compatibilidade como o TM, mas porque o menor número de êxitos do atacante desafia menos vezes a capacidade de resposta, porque ao limitar os efeitos da contra retaliação faz mais credível a retaliação e porque reduz os efeitos de terceiros e facilita a atribuição por eliminação (Libicki, 2009, pp.73-74).

Os efeitos positivos do TM sobre as dimensões de comunicação e sinalização aumentam ao adotar estratégias defensivas, visto que há disponível um leque de respostas de grande valor político, mas que ao mesmo tempo comportam pouco risco. Porque as respostas no âmbito da informação e da ação política, diplomática e legal têm melhor aceitação do que o emprego da força entre os atores nacionais e internacionais (Retter et. all, 2016, p.12). Para que o potencial agressor perceba adequadamente estes sinais deve ser-lhe comunicada a resiliência do sistema de forma a que avalie corretamente os custos de desenvolver o ataque, os reduzidos ganhos e os custos duma resposta muito difícil de deslegitimar (Solomon, 2011, p.4). Mas também deve saber que no caso pouco provável de o seu ataque ter êxito, poder-se-ão empregar respostas mais contundentes.

Posto que um dos pilares desta estratégia é a detecção e a correção global de vulnerabilidades, podemos afirmar o seu alto grau de compatibilidade com o conceito de fronteira de segurança e com o modelo de cooperação abordado na secção 2.3. Ainda assim, a persistência de vulnerabilidades e a grande disponibilidade de ciberarmas recomendariam chegar a algum tipo de acordo para o desarmamento ciber ou para a não agressão no ciberespaço, mas é mais difícil chegar a uma definição do que proibir e a questão das inspeções não parece viável (Geers, 2012, pp.6-8).

Na dissuasão contra formas mais brandas de confrontação, não especificamente proibidas, como o ciberespionagem, encontra-se um grau de compatibilidade superior ao das estratégias punitivas, desde que as Regras 6.4, 10.8 e 11.9.h colocam o limiar alto demais para responder a este tipo de interferências. Porem a compatibilidade com o TM acrescenta-se porque para atingir o sucesso contra um sistema mais resiliente deverá incrementar a agressividade dos ciberataques incrementado o risco de ultrapassar outros limiares (Regra 6.4).

Até este ponto verificou-se a segunda hipótese e acrescentou-se o grau de conhecimento quanto à compatibilidade do TM com as duas principais estratégias de dissuasão. Verificou-se também que a compatibilidade é maior no caso das estratégias

defensivas, e que a complementação destas como elementos punitivos incrementa a eficácia dissuasória mantendo a compatibilidade com o TM. Ainda assim na secção seguinte abordar-se-á a possibilidade de melhorar a eficácia dissuasória partindo de uma abordagem jurídica.

3.3. Na melhora da dissuasão e a redução de vulnerabilidades

A teoria da dissuasão no ciberespaço deve abranger um leque de adversários muito mais alargado e de tipologias mais diversas que noutros domínios, portanto deve cobrir todo o espectro de atores, tipos de ataque e níveis de ação (Jensen, 2012, p.782-784). Inclusivamente aqueles atores que não temem a retaliação, pela dificuldade desta, e adotam uma posição irracional que invalida a dissuasão por punição (Iasiello, 2013, p.64).

Se avaliarmos a dissuasão contra todos os atores do ciberespaço e o facto de 80-90% das vulnerabilidades corporativas poder corrigir-se com ações elementares, sendo menos de 5% inevitáveis por custos ou complexidade técnica, a correção de vulnerabilidades reduziria imensamente os ciberataques a gerir pelos Estados. Assim avaliada, a dissuasão defensiva torna-se mais barata que a punitiva (Iasiello, 2013, p.64, 67 e Lewis, 2013, p.2) e ainda traz contributos adicionais para outros setores como o económico, empresarial, emergências, etc. (Stockton, 2014, p.19).

Por outro lado, é possível traçar uma relação entre as dificuldades de verificação e desarmamento e o já comentado debate sobre os benefícios dos governos publicarem as vulnerabilidades detectadas. Assumida a impossibilidade de limitar as ciberarmas pela via da inspeção, duvidando que, no atual ambiente de predomínio da mentalidade ofensiva (Lynn III, 2010), a boa-fé dos Estados permita reduzi-las pela via da publicação voluntária de vulnerabilidades e conseguinte renuncia à sua futura exploração, seria interessante abordar o tema pelo lado da limitação legal do uso das ciberarmas.

Uma vez que o TM aborda a *lex lata*, sem entrar no terreno da *lex ferenda*, e reconhece a temporariedade das suas intepretações, decorrente da evolução no domínio cibernético (Schmitt, et al., 2013, pp.5,42), parece importante abordar a viabilidade da restrição aos cibertaques que altere o balanço custo benefício de os Estados manterem secretas certas vulnerabilidades.

Assim, parece interessante avaliar a utilidade dum acordo internacional para proibir o emprego de ciberarmas na adopção de contramedidas, e para restringir o seu emprego ao último limiar, a "legitima defesa". Ao diminuir a sua utilidade, a publicação e correção de vulnerabilidades tornaria ineficazes as ciberarmas da maioria dos atores (Goldsmith, 2014), estando estas só ao alcance de alguns Estados e corporações tecnológicas. O "Stuxnet" é um

exemplo deste tipo de ciberarmas apenas ao alcance duns poucos (Flanagan, 2011; Stark, 2011). Adicionalmente, à medida que o número de Estados não comprometidos com este fim se vai reduzindo, a fronteira de cibersegurança (Hare, 2009, p.14,15) colocá-los-ia numa situação mais comprometida. Adicionalmente o papel de terceiros reduzir-se-ia ao mínimo, cresceria a estabilidade e a atribuição seria muito mais simples porque só poucos teriam capacidade de desenvolver ciberarmas eficazes.

.

Conclusões

"…cyber war is less about arms (exploits) than about vulnerabilities."
(Libicki, 2009b)

Nas últimas duas décadas aconteceram numerosos casos de ciberconflito e a situação ainda não parece estar próxima duma estabilização, o que têm impulsionado diferentes atores a promover a aceitação internacional dum posicionamento jurídico que vá de encontro ao seu interesse relativamente aos conflitos no ciberespaço.

A nível global, são dois os posicionamentos jurídicos mais relevantes: dum lado, sob a liderança da Rússia e a China, pretende-se um tratamento jurídico do ciberespaço diferenciado do dos restantes domínios das operações. Do outro lado, sob a liderança dos EUA e da OTAN, com a concorrência maioritária dos aliados e das democracias ocidentais, fundamenta-se que a legislação internacional existente é aplicável no ciberespaço. Reduz-se assim o problema a uma questão de clarificação quanto à forma de aplicação, também de complementação daqueles aspetos pontuais que precisem um grau de compreensão adicional. Portanto, é necessário um processo de impulsão, adaptação e difusão desta posição interpretativa da que o Processo e o Manual de Tallinn são destacados instrumentos de legitimação.

Estas diferenças de posicionamento dificultam as possibilidades de segurança dos Estados no ciberespaço, desde que fazem diminuir as garantias de que não serão atacados, e obrigam-nos a adotar estratégias dissuasórias.

Assim sendo, a OTAN tem reconhecido o ciberespaço como um domínio mais das operações e acordou que a ciberdefesa faz parte nuclear do esquema de segurança coletiva, o que melhorará a sua habilidade para proteger e para conduzir operações nestes domínios; também para manter a liberdade de ação e de decisão em todas as circunstâncias, sustentado deste modo a sua capacidade de dissuasão e defesa. Na Cimeira de Varsóvia, a OTAN também reafirmou o seu compromisso para atuar de acordo com a lei internacional no ciberespaço, portanto, evidencia dois elementos que devem concorrer para atingir os seus objetivos: manter a capacidade de dissuasão alargada e atuar de acordo com a legalidade internacional, resultando que o posicionamento pormenorizado em relação ao segundo elemento condicionará a implementação do primeiro.

Pretendeu-se com presente trabalho, compreender como as regras de interpretação do direito internacional contidas no TM afetam a dissuasão no ciberespaço, e como afetariam caso fossem assumidas oficialmente pela NATO, ou seus membros.

Para tal formulou-se a seguinte pergunta de partida:

Em que medida as regras contidas no Tallinn Manual e o posicionamento oficial em relação a elas são compatíveis com uma estratégia eficaz de dissuasão no ciberespaço?

Que levou a duas perguntas derivadas:

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

PD2 - *Em que medida é compatível o posicionamento do Tallinn Manual com as opções de dissuasão no ciberespaço?*

A abordagem metodológica do problema, fez-se segundo um esquema de raciocínio hipotético dedutivo, assente numa metodologia de análise qualitativa e estratégia de estudo de caso, fundamentada em dados documentais.

Uma vez colocado o problema, desenhou-se o modelo teórico, que permitiu desenvolver o processo de dedução e teste conducente à elaboração de respostas para as perguntas de investigação.

O processo dedutivo desenvolveu-se em duas etapas:

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

HIP1 – *As regras do Tallinn Manual têm efeitos diferenciados sobre cada dimensão do problema da dissuasão no ciberespaço, que por sua vez poderão variar dependendo da existência de posicionamento oficial no que respeita a estas regras.*

De seguida desenvolveu-se a construção de explicações para avaliar a solução do problema da investigação em relação a cada uma das suas dimensões. Nesta fase do processo dedutivo, verificou-se a primeira hipótese e obtiveram-se respostas avaliativas a nível de indicador para a primeira pergunta derivada.

Estas respostas e as interpretações jurídicas do TM, adotaram-se a continuação como base teórica para a segunda etapa de raciocínio, onde o processo dedutivo partiu da hipótese:

HIP2 - *A compatibilidade do Tallinn Manual com as opções de dissuasão no ciberespaço está relacionada com o impacto das suas regras sobre as dimensões da dissuasão consideradas e às estratégias adotadas, o que permitirá delinear estratégias mais eficazes.*

E chegou à sua verificação, assim como a dar uma avaliação motivada do grau de compatibilidade do TM com as duas opções teóricas básicas de dissuasão, punitiva e defensiva. Aqui as respostas também se obtiveram a nível de indicador, o que permitirá avançar no desenho de opções dissuasórias mistas mais eficazes do que as básicas, assim como abordar o estudo de possíveis soluções para alguns problemas.

No âmbito da primeira dimensão do problema abordou-se o esclarecimento dos contributos do TM para legitimar a ameaça e emprego de respostas dissuasórias no ciberespaço sem afetar o nível de ambiguidade necessário para dissuadir com eficácia.

Depois de verificar que o TM contribui positivamente para confirmar a legitimidade de ameaçar com o emprego legítimo da força, verificou-se que estabelece um leque de limiares com a nitidez e flexibilidade apropriada para a dissuasão:

- "Ataque armado" para determinar o direito a responder legitimamente em "autodefesa" com o "uso da força".
- "Uso da força" para determinar possíveis violações do Artigo 2 da Carta das Nações Unidas (CNU). Sendo a natureza deste limiar distinta da do anterior, porque se estabelecem com fins diferentes.
- Violação de uma obrigação pela que seja exigível responsabilidade legal internacional. Habilita para responder com contramedidas que não atinjam o limiar do "uso da força".
- Invocação do estado de necessidade no ciberespaço. Se bem que, as condições e as controvérsias quanto as tais invocações fazem incerto o recurso à força sustentado nesta figura.
- Retorsão como resposta inamistosa, mais legal, a ações inamistosas legais ou ilegais.
- Crimes ordinários passiveis de ser perseguidos pela jurisdição do Estado agredido.

Fica sem esclarecer que ações não qualificáveis como "ataque armado" constituem "uso da força", mas aqui o papel a jogar pela comunidade internacional enlaça com o papel a desenvolver pelo *Tallinn Manual Process* no quadro da etapa de impulsão desta interpretação normativa.

Por outro lado, limita a possibilidade de empregar respostas encobertas e dá resposta à possibilidade de dissuadir contra a implantação de ciberarmas latentes e ocultas nos

sistemas próprios, com mais contundência no caso das bombas lógicas que das ciberarmas de ativação remota.

Verificou-se assim que as respostas legítimas visadas pelo TM para o grande leque de ciberataques possíveis são compatíveis com a amplitude e progressividade adequadas para a dissuasão. A legitimidade destas respostas assentará na avaliação qualitativa e quantitativa da ofensa em termos de escala e efeitos, e na gradação da resposta segundo os princípios de necessidade, proporcionalidade, iminência e imediatismo. Servindo a capacidade e flexibilidade interpretativa atribuída ao atacado sobre estes assuntos para garantir-lhe a flexibilidade situacional necessária.

O leque de respostas legitimas, o grau de nitidez dos limiares e o nível de imprevisibilidade nas respostas, decorrente da interpretação contextualizada do princípio de proporcionalidade, quanto a quantidade e natureza da resposta, contribuem para diminuir a instabilidade. Adicionalmente, o TM apresenta um modelo de referência para a avaliação racional das possíveis respostas dissuasórias do defensor. Assim, ambiguidade, capacidade de resposta flexível e racionalidade contribuem para a credibilidade

Cabe salientar que a aceitação oficial do manual previsivelmente teria efeitos ainda mais positivos sobre a racionalidade e sobre o contributo dos limiares para a credibilidade.

Na dimensão da soberania, verificou-se o grande contributo do TM para o exercício das prerrogativas soberanas sobre a infraestrutura e as atividades do ciberespaço dentro do território do Estado, incluindo o controlo de acesso e o direito exclusivo a exercer a jurisdição e a autoridade. Também ficaram esclarecidos os vínculos territoriais das fronteiras no ciberespaço, abordou-se com resultado positivo para os nossos fins, a problemática da não coincidência das fronteiras territoriais com as fronteiras de domínio, esclareceu-se a jurisdição sobre os sistemas distribuídos transfronteiriços e confirmou-se a autoridade dos Estados para o controlo de acesso através do ciberespaço. A aceitação oficial do TM podia acrescentar ainda os efeitos positivos nestes aspectos. Quanto aos contributos para a atribuição e a mitigação dos efeitos de terceiros, desde a perspetiva da soberania, são positivos e seriam reforçados pelo reconhecimento oficial do TM, mas não chegariam a ser conclusivos.

A abordagem da soberania feita pelo TM também contribui para a cooperação, para a dissuasão alargada e para a segurança interdependente. Destacam-se aqui elementos como a legitimação do consentimento dum Estado para que outro execute ciberoperações a partir do seu território, permitindo, por exemplo, complementar a sua capacidade técnica; obrigações

aos Estados para impedir que desde o seu território se desenvolvam atividades contrarias ao direito internacional; a legitimação do papel das organizações regionais; e, por fim, o efeito de promoção decorrente da comunicação da posição mais comumente aceite, embora não oficial, respeitante à soberania no âmbito da OTAN.

Já na dimensão da atribuição, verificou-se que o TM visa mecanismos legais para acelerar e facilitar o acesso às evidencias técnicas localizadas no espaço de soberania doutros Estados. Todavia, e ainda mais importante, o TM é compatível com certos graus de atribuição política, más com as salvaguardas adequadas para que o papel de terceiros não leve à escalada. Desde a perspetiva técnica isto é relevante porque permite salvaguardar as técnicas forenses e permite ultrapassar limitações temporais pouco compatíveis com estratégias dissuasórias efetivas. Duma perspetiva política, permite considerar o incumprimento de certas obrigações dos Estados como peça de evidência para a atribuição, mas não é conclusivo quanto à obrigação de policiamento dos Estados no ciberespaço, nem quanto a outros aspetos relevantes. Também não aborda o impacto que a atribuição política podia ter se alguns Estados a empregarem para justificar restrições à privacidade ou à liberdade de discurso no ciberespaço, devendo recorrer ao principio geral do TM quanto a aplicabilidade do direito internacional no ciberespaço.

Por outro lado, a necessidade dos Estados se protegerem contra os riscos de sofrer a atribuição política decorrente de atividades de terceiros, obriga-os a adotar medidas para envolver o setor privado na melhoria da segurança no ciberespaço. Portanto, embora o TM não aborde a cibersegurança nem coloque regras de obrigatoriedade estatal quanto às condições de segurança do setor privado no ciberespaço, promove sim, indiretamente que os Estados atendam a este assunto. No caso de os Estados incapazes de aplicar políticas de segurança adequadas, ficou clara a possibilidade de um terceiro Estado contribuir para a sua segurança sob consentimento do primeiro, mas não há acordo entre os peritos quanto à legitimidade de lançar operações defensivas desde um Estado ao qual não foi atribuído o ataque no caso de esse Estado ou o Conselho de Segurança da ONU não consentir. Daí a necessidade de cooperar com aqueles países que não atingem os padrões mínimos de segurança no ciberespaço.

Na dimensão das capacidades e seu impacto sobre a credibilidade, abordou-se a possibilidade de destruição das ciberarmas do adversário, caso fosse tecnicamente possível, para determinar que o TM não é conclusivo quanto à legitimidade dos ataques necessários para o fazer. Também não se detectaram contributos relevantes quanto aos problemas da

erosão mútua de capacidades, da detecção e correção global de vulnerabilidades, do desarmamento ou da possibilidade de ocultar ciberarmas nos sistemas do adversário para contribuir para a nossa capacidade de retaliação. Em contraste, o TM acrescenta uma dificuldade legal para empregar capacidades de defesa ativa, na sua modalidade de contra ciberoperação automática.

O contributo para a factibilidade de emprego das ciberarmas avaliou-se como neutro em termos gerais, desde que não permite ultrapassar as limitações decorrentes da necessidade de concretizar alvos e efeitos, nem de fazer uma avaliação de danos apropriada. O facto de permitir que a natureza da resposta seja distinta à do ataque facilita ultrapassar indiretamente as limitações da ciberdissuasão. Outros contributos positivos são a possibilidade de empregar capacidades *sub-rosa*, embora com limitações, ou de desenvolver operações de informação para impor custos públicos ao agressor.

Por fim, nas dimensões de comunicação e sinalização é que se encontraram os contributos mais positivos quanto a todos os indicadores, sendo de salientar dois assuntos. Pode afirmar-se que o *Tallinn Manual Process* constitui um potente elemento de comunicação. Também que um dos aspetos mais negativos da aceitação oficial do TM é que limitaria consideravelmente as vias para mudar as regras quando for preciso.

Depois de verificar a primeira hipótese e avaliar os efeitos do TM sobre cada dimensão do problema da dissuasão no ciberespaço, abordou-se o segundo processo dedutivo que para além de verificar a segunda hipótese permitiu obter as respostas para a correspondente pergunta derivada.

Em relação à dissuasão punitiva, apesar dos avanços nas dimensões de soberania e atribuição, a exigência de reforçar com evidências adicionais a atribuição política, continua a limitar as estratégias punitivas. Ainda mais, o TM, dificulta a defesa ativa e não permite avançar na capacidade de destruição das ciberarmas adversárias, nem nos problemas de erosão das cibercapacidades de retaliação, ou da consolidação de capacidades de retaliação implantando ciberarmas nos sistemas do oponente.

Apesar do TM legitimar o emprego das ciberarmas em certas condições, não permite ultrapassar todas as dificuldades apresentadas. Daí que seja preciso recorrer a capacidades de resposta fora do ciberespaço. Esta opção permitiria tirar benefícios de responder em todo o espectro das operações, mas não permite ultrapassar o facto de que as respostas para dissuadir uns atores possam ser o incentivo para outros. Também não oferece respostas a outros problemas, como a detecção e correção de vulnerabilidades à escala global ou os

processos de desarmamento no ciberespaço. Por fim, verificou-se que, no quadro jurídico do TM, aplicar uma estratégia punitiva sem solucionar os problemas anteriores pode afetar muito negativamente as dimensões de comunicação e sinalização.

A avaliação das estratégias defensivas resultou num grau de compatibilidade superior, mas também insuficiente. A dificuldade de atribuição dilui-se porque desde que a severidade da resposta não é fulcral, é possível encontrar respostas eficazes por debaixo do limiar das contramedidas; e com a vantagem adicional de dissuadir contra formas mais brandas de confrontação. Também se verificou o impacto positivo do TM na dimensão da soberania, na promoção da segurança no ciberespaço e na detecção e correção global de vulnerabilidades, atingindo um alto grau de compatibilidade com o conceito de fronteira de segurança. Adicionalmente, os efeitos positivos do TM sobre as dimensões de credibilidade, comunicação e sinalização acrescentam-se ao adotar estratégias defensivas.

Na dimensão das capacidades, a impossibilidade técnica de atingir a proteção completa dos sistemas obriga a incluir respostas de caráter punitivo. Mas o fortalecimento da resiliência pode anular a legalidade da resposta em autodefesa ou empregando contramedidas.

Até este ponto respondeu-se à pergunta de partida, verificando em que medida as regras contidas no *Tallinn Manual* são compatíveis com uma estratégia eficaz de dissuasão no ciberespaço e confirmam do que o posicionamento oficial apenas alteraria alguns indicadores.

No percurso da investigação levantaram-se duas questões adicionais.

A primeira, visa melhorar as estratégias dissuasórias pela via da incorporação de elementos punitivos a estratégias assentes no fortalecimento da defesa. Para tal fim, este trabalho permitiu caraterizar os ingredientes da receita, mas não se abordou a questão das proporções.

A segunda tem a ver com acrescentar a segurança global no ciberespaço pela via do desarmamento e a eliminação de vulnerabilidades. Assim, parece interessante avaliar a viabilidade duma restrição ao uso de ciberarmas que altere o balanço custo benefício de os Estados manterem secretas certas vulnerabilidades. A solução podia passar por um acordo internacional para restringir o seu emprego ao último limiar, a "legítima defesa". Ao diminuir a sua utilidade, a publicação e correção de vulnerabilidades detectadas pelos Estados tornaria ineficazes as ciberarmas ao alcance da maioria de atores.

Bibliografia.

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

Andreas, P., 2001. *Border Games: Policing the U.S.-Mexico Divide*. Ithaca & London: Cornell University Press.

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

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

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

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

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

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

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

Boebert, W.E., 2010. A Survey of Challenges in Attribution. Em: Committee on Deterring Cyberattacks, 2010. *Proceedings of a Workshop on Deterring Cyberattacks:*

Informing Strategies and Developing Options for U.S. Policy. [livro electronico] Washington: The National Academies Press. Pp.41-52. Disponivel em: https://www.nap.edu/download/12997 [Acedido em 22 mar. 2017].

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

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

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

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

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

CCDCOE, 2016. *CCDCOE Cyber Definitions*. [Em linha] Disponível em: https://ccdcoe.org/cyber-definitions.html#list [Acedido em 09 dic. 2016].

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Godwin, J.B., Kulpin, A., Rauscher, K.F., e Yaschenko, V., 2014. *Critical Terminology Foundations 2*, *Russia-US Bilateral on Cybersecurity*. East-West Institute, Policy Report 2/2014. [Em linha] New York: East-West Institute. Disponível em: https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf [Acedido em 04 abr. 2017].

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

Gómez de Ágreda, A., 2012. El ciberespacio como escenario de conflictos. Indentificación de las amenazas. Em: Casar Corredera., J.R., pres., 2012. *El ciberespacio. Nuevo escenario de Confrontación.* Monografías del CESEDEN, Nº 126. Madrid: Ministerio de Defensa. Cap. 4.

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

Google, 2017. Google IPv6, estadisticas. [Em linha] Disponível em: https://www.google.com/intl/es/ipv6/statistics.html [Acedido em 24 May. 2017]

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

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

Guitton, C., 2012. Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence. *International Journal of Cyber Criminology*, Vol 6, Issue 2 July - December 2012, pp.1030-1043.

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

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

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

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

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

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

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

Hua, J. e Bapna S., 2012. *How Can We Deter Cyber Terrorism?* Information Security Journal: A Global Perspective, 21, pp.102–114.

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

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

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

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

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

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

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

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

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

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

Lan, T. e Xin, Z., 2010. The View from China: Can Cyber Deterrence Work? Em: Nagorski, A. ed. 2010. *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*. New York: The EastWest Institute. [Em linha] Disponível em: https://www.eastwest.ngo/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf [Acedido em 29mar. 2017]

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

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

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

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

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

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

Linn III, W.L. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *United States Cyber Comand: Cyber Security* [Em linha] Disponível em: http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx [Acedido em 04 mar. 2013].

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

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

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

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

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

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

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

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

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

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

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

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

NATO, 2014b. *Wales Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#def-det2 [Acedido em 02 dic. 2016].

NATO, 2016. *Warsaw Summit Communiqué*. [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#def-det2 [Acedido em 02 dic. 2016].

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Thomas, T.L. 2017. Statement on Russia's Information War Concepts. Em: U.S. House of Representatives, Armed Services Committee. *Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment.* [Em linha]

Disponível em: https://armedservices.house.gov/legislation/hearings/crafting-information-warfare-and-counter-propaganda-strategy-emerging-security [Acedido em 10 abr. 2017]

Tikk, E., Kaska, K. e Vihul, L., 2010. Legal Considerations: Intenational Cyber Incidents. Tallin: CCDCOE.

Tikk, E., 2011. *Comprehensive legal approach to cyber security*. Dissertação de Doutoramento em Direito. Universidade de Tartu, Estonia.

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

UE. 2016. *Directiva del Parlamento Europeo y de Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. (DIRECTIVA UE 2016/1148 de 6 de julio de 2016). [Em linha] Disponível em: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES [Acedido em 04 abr. 2017]

U.S. Army War College. 2016. *Strategic Cyberspace Operations Guide.* [Em linha] Disponível em: http://www.csl.army.mil/usacsl/Publications/Strategic_Cyberspace_Operations_Guide_1_June_2016.pdf [Acedido em 12 dic.2016].

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Apêndice A — Corpo de conceitos

Uma vez que na OTAN não há um corpo conceitual comum para os termos Ciber, que podem ter significados e interpretações diferentes segundo as organizações ou nações que os empregam, neste trabalho sempre que for possível empregar-se-ão os termos no mesmo sentido que o CCDCOE, por ser este o quadro no que o TM foi desenvolvido. Desde que tais definições se baseiam em definições do TM ou em documentos sobre estratégias e políticas, não devem ser entendidas como assentes no contexto legal internacional. Assim, salvo indicação em contrário, os conceitos a seguir são traduções ou adaptações das definições dadas para cada conceito por distintas organizações e apresentadas (CCDCOE, 2016, p. Cyber Definitions) entre as que se escolheram por se considerarem as que melhor se ajustam aos objetivos deste trabalho.

Adversário - Pessoa, grupo, organização ou governo que conduz ou tem a intenção de conduzir atividades prejudiciais para aquele de quem se considere adversário.

Ameaça Avançada Persistente - Um adversário que possui níveis sofisticados de perícia e recursos significativos que lhe permitem criar oportunidades para atingir seus objetivos usando vetores de ataque múltiplos (por exemplo, ciber, físico e deceção).

Atacante - Um indivíduo, grupo, organização ou governo que executa um ataque. Definição estendida: uma parte atuando com propósito malicioso para comprometer um sistema de informação.

Ataque ativo no ciberespaço - Um ataque real perpetrado por uma fonte de ameaça que propositadamente tenta alterar um sistema, seus recursos, seus dados ou suas operações.

Ataque passivo no ciberespaço - Um ataque contra um protocolo de autenticação onde o atacante intercepta dados viajando ao longo da rede entre o transmissor e o recetor, mas não altera os dados (por exemplo, espionagem).

Capacidade de ciberdefesa - Conjunto de valências que se destinam à prevenção, deteção, defesa e recuperação de ciberataques contra a infraestrutura da informação. (Monteiro da Silva, 2012)

Capacidade de ciberdefesa ofensiva - Conjunto de valências que capacitam para iniciar um ciberataque que pode ser utilizado como ciberdissuasor.

Capacidade ciberdefensiva - Conjunto de valências que capacitam para proteger e repelir contra um ciberataque ou ciberexploração que pode ser utilizado como ciberdissuasor.

Ciberameaça - Capacidade passível de ser utilizada para perpetrar um ciberataque. (Monteiro da Silva, 2012)

Ciber, Cibernético - Relacionado com as Tecnologias da Informação e com o domínio do ciberespaço.

Ciberarma - Software, firmware ou hardware projetado ou aplicado para causar danos através do ciberespaço.

Ciberataque - Ações deliberadas, que previsivelmente podem causar lesão ou morte a pessoas ou danos a objetos, tomadas para interromper, negar, corromper ou destruir: informações num computador e/ou rede de computadores, ou o computador e/ou a própria rede de computadores, e/ou outros elementos conectados ou controlados desde o sistema atacado ou ao alcance dos efeitos de estes elementos. **Definição estendida:** Tentativa de obter acesso não autorizado aos serviços do sistema, recursos ou informações, ou de comprometer a integridade do sistema. Esta definição não se deve confundir com a de "*cyber attack*" feita na Regra 30 do *Tallinn Manual* para determinar se uma ciberoperação qualifica como "ataque" efeitos da aplicação do *jus in bello*.

Ciberconflito - Situação de tensão entre Estados-Nação e/ou grupos organizados da que podem resultar ciberataques.

Ciber contra-ataque - Uso de uma arma cibernética com intenção de causar dano a um alvo designado em resposta a um ataque.

Ciberdefesa - Conjunto de valências e ações que se destinam à prevenção, deteção, defesa e recuperação de ciberataques, e que contribuem dessa forma para a cibersegurança (Monteiro da Silva, 2012, p.54).

Ciberdefesa ativa - Uma medida pró-ativa para a deteção ou obtenção de informações quanto a uma intrusão ciber, ataque cibernético, ou ciberoperação iminente para determinar a origem de uma operação que possa implicar o lançamento de uma operação *preemptiva*, preventiva ou contra-operação cibernética contra a fonte da agressão. (Schmitt, et al., 2013, p.257)

Ciberdefesa passiva - Conjunto de valências e ações para a deteção e mitigação de intrusões cibernéticas e dos efeitos de ataques cibernéticos que não envolve o lançamento de operações preventivas ou de retaliação contra a fonte. Exemplo de medidas de ciberdefesa

passiva são *firewalls*, *patches, software anti-vírus* e ferramentas forenses digitais. (Schmitt, et al., 2013, p.257)

Ciberdissuasor - Mecanismo declarado que é presumidamente eficaz em desencorajar o ciberconflito e/ou a atividade ameaçadora no ciberespaço. Estes mecanismos incluem políticas, posturas, armas, capacidades e alianças. (Godwin et.al., 2014)

Ciberdissuasão - Dissuasão no ciberespaço com meios e opções do ciberespaço. (Autor, 2016)

Ciberespaço - Domínio global formado pelos sistemas de informação e de telecomunicações e outros sistemas eletrónicos, sua interação e os dados que são armazenados, processados ou transmitidos por esses sistemas. (NATO, 2014a)

Ciberespionagem - Operação no ciberespaço para obter acesso não autorizado a informações confidenciais através de meios secretos (Godwin et.al., 2014). Adota-se esta definição por ser mais abrangente que a da Regra 66 do *Tallinn Manual* aplicável no âmbito do *jus in bello*.

Ciberexploração - Aproveitar uma oportunidade presente no ciberespaço, por exemplo uma vulnerabilidade, para alcançar um objetivo.

Ciberguerra - Estado escalado de ciberconflito entre Estados em que os ciberataques são realizados por atores estatais contra a infraestrutura cibernética como parte de uma campanha militar. Pode ser declarada (formalmente declarada por autoria de uma das partes) ou de fato (com a ausência de uma declaração).

Ciberincidente – Qualquer anomalia detetada comprometendo ou com o potencial de comprometer sistemas de informação, comunicações ou outros sistemas eletrónicos, ou a informação armazenada, processada ou transmitida por estes sistemas. **(**NATO, 2013)

Ciberinfraestrutura – Os recursos de comunicações, armazenamento e computação sobre os quais os sistemas de informação operam. A Internet é um exemplo de uma infraestrutura de informação global.

Cibersegurança – Estado de não existência de perigo ou possibilidade de danos causados pela disrupção das TIC ou fruto de ações abusivas destas (Monteiro da Silva, 2012, p.54). Decorre da capacidade de proteger ou defender o uso do ciberespaço de ciberataques. A cibersegurança geralmente refere-se às salvaguardas e ações que podem ser usadas para proteger o domínio cibernético, tanto no campo civil quanto no militar, das ameaças que estão associadas ou que podem prejudicar suas redes e infraestrutura de informação interdependentes. A cibersegurança esforça-se para preservar a disponibilidade e a

integridade das redes, da infraestrutura e dos sistemas de informação, assim como a confidencialidade dos dados que contêm.

Ciberoperação - Ver operações no ciberespaço.

Dissuasão (*deterrence*) - A prevenção da ação pelo medo das consequências. A dissuasão é um estado de espírito provocado pela existência de uma ameaça credível de ação contrária e de consequências inaceitáveis. Este conceito está estreitamente relacionado com o de **opções de dissuasão**. Ambos conceitos serão objeto de aprofundamento neste trabalho. (US DoD, 2001)

Dissuasão no ciberespaço - É a dissuasão exercida aplicando quaisquer opções de dissuasão para a prevenção de ações adversárias não desejadas no ciberespaço. Quando apenas emprega meios e opções do ciberespaço definimo-la como ciberdissuasão.

Fronteira de domínio – Delimitação duma parte do ciberespaço determinada pelos sistemas que conectam a infraestrutura de rede dum provedor com o resto da rede. (Autor, 2017)

Forças cibernéticas - Médios organizados para conduzir ciberoperações.

Infraestrutura cibernética - Agregação de pessoas, processos e sistemas que constituem o ciberespaço.

Opções de dissuasão (*deterrence options*) - Cada um dos cursos de ação, desenvolvidos sobre o melhor julgamento económico, diplomático, político e/ou militar, destinado a dissuadir um adversário de um curso de ação ou das operações que contemple. (Ao construir um plano de operações, deve apresentar-se uma gama de opções para o efeito da dissuasão. Cada opção que requer o desdobramento de forças deve ter um módulo de força separado). (US DoD, 2001)

Operações no ciberespaço - Emprego de capacidades cibernéticas onde o propósito principal é alcançar objetivos dentro ou através do ciberespaço. Tais operações incluem *Computer Network Operations* e atividades para operar e defender a rede de informação global (GIG).

Operações defensivas no ciberespaço - Operações passivas e ativas no ciberespaço destinadas a preservar a habilidade de utilizar capacidades cibernéticas amigáveis e proteger dados, redes, capacidades centradas na rede e outros sistemas designados.

Operações ofensivas no ciberespaço - Operações no ciberespaço destinadas a projetar o poder pela aplicação da força no ou através do ciberespaço.

Resiliência - Capacidade para preparar-se para, adaptar-se a, suportar e recuperar rapidamente das perturbações resultantes de ataques deliberados, acidentes ou ameaças ou incidentes naturais.

Apêndice B — Análise das dimensões e determinação dos indicadores.

Ao longo deste Apêndice, analisam-se as dimensões do problema da dissuasão no ciberespaço por forma a explicitar os indicadores (Apêndice C) que permitem abordar o processo dedutivo de verificação e construção de explicações relativas à primeira hipótese.

B.1. O problema da ambiguidade

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

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

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

B.2. Ataque armado

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

Por outro lado, em alguns casos, o atacante visando erodir com o ataque certas capacidades, económicas, diplomáticas, etc., procurará ocultar o ataque, colocando assim ao

defensor, caso o detecte, numa situação difícil para justificar uma possível represália. Outras vezes pode ser o defensor, quem simule não ter detectado o ataque, para eludir responder sem perder credibilidade por não o fazer. (Solomon, 2011, p.12,13)

B.3. A dificuldade de atribuição

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

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

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

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

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

B.4. O problema da capacidade

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

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

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

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

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

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

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

B.5. As dificuldades de comunicação e sinalização

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

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

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

B.6. O problema da credibilidade

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

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

B.7. O problema da soberania

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

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

Apêndice C — Mapa conceitual e modelo de análise.

HIPÓTESE 1 - As regras do *Tallinn Manual* têm efeitos diferenciados sobre cada dimensão do problema da dissuasão no ciberespaço, que por sua vez poderão variar dependendo da existência de posicionamento oficial no que respeita a estas regras.		
CONCEITOS	**DIMENSÕES**	**INDICADORES**
Dissuasão no ciberespaço	Legitimidade da resposta aos ciberataques	Uso da força
		Ataque armado
		Legitima defesa
		Intervenção ilegal
		Contramedidas
		Estado de necessidade
		Resposta legal
		Respostas encobertas
		Limita a implantação de armas nos sistemas alheios
		Limita as formas brandas de confrontação
	Ambiguidade	Amplitude e progressividade do limiar
		Flexibilidade situacional
		Estabilidade e atividades de reconhecimento
		Estabilidade e nível de imprevisibilidade que demanda nas respostas
	Atribuição	Demora no processo de atribuição técnica forense
		Aplicabilidade de técnicas forenses no espaço de soberania doutro Estado
		Preservação das técnicas forenses
		Legitimação da atribuição política
		Terceiros
		Garantia da liberdade de discurso e da privacidade
		Traslado ao setor privado de responsabilidades decorrentes da atribuição política
		Atribuição política e Estados com poucas capacidades ciber
	Capacidade	Dificuldade para destruir as ciberarmas adversárias
		Erosão mútua de capacidades de ofensa e retaliação
		Deteção e correção global de vulnerabilidades
		Possibilidade de implantar armas no *hardware, firmware, software* do possível agressor
		Capacidade de resposta *sub-rosa*
		Dificuldade para a defesa ativa
		Factibilidade de emprego das ciberarmas. Alvos e efeitos concretizados e avaliação de danos
		Legitimidade de emprego das armas convencionais/nucleares
		Custo público: balanço ataques / respostas
		Operações de informação
		Possibilidade de verificação e desarmamento ciber

	Comunicação e Sinalização	Facilita a assimilação da mensagem
		Facilita a perceção de sinais quanto à nossa intenção
		Facilita a comunicação de capacidade e determinação
		Tallinn Manual Process
		Facilita vias para mudar as regras
		Promove tempos apropriados para o reajuste de atitudes
		Contribui para a qualidade dos limites
	Credibilidade	Limiar adequado
		Capacidade e natureza da resposta em relação à ofensa
		Colocação de armas ocultas nos sistemas do potencial agressor
		Contribui para a racionalidade
	Soberania	Vínculo territorial e fronteira
		Fronteira estatal e fronteira de domínio
		Facilita o controlo fronteiriço
		Jurisdição
		Reduz o problema dos terceiros
		Contribui para a atribuição
		Facilita a cooperação
		Contribui para a comunicação

HIPÓTESE 2 - A compatibilidade do *Tallinn Manual* com as opções de dissuasão no ciberespaço está relacionada com o impacto das suas regras sobre as dimensões da dissuasão consideradas e às estratégias adotadas, o que permitirá delinear estratégias mais eficazes.		
CONCEITOS	**DIMENSÕES**	**INDICADORES**
Opções de dissuasão	Dissuasão punitiva	Atribuição
		Soberania
		Limiares de resposta (ataque armado, uso da força, ação ilegal, ação inamistosa)
		Capacidade de resposta
		Ciberdefesa ativa
		Credibilidade
		Comunicação e sinalização
		Custo público: balanço ataques / respostas
		Operações de informação
		Contribuição para o desarmamento ciber
		Contribuição para a detecção e correção global de vulnerabilidades
	Dissuasão defensiva	Atribuição
		Soberania
		Limiares de resposta (ataque armado, uso da força, ação ilegal, ação inamistosa)
		Capacidade
		Ciberdefesa passiva
		Ciberdefesa ativa
		Credibilidade
		Comunicação e sinalização
		Custo público: balanço ataques / respostas
		Operações de informação
		Contribuição para o desarmamento ciber
		Contribuição para a detecção e correção global de vulnerabilidades
		Cooperação
		Dissuade contra a espionagem