Academia Militar

Direcção de Ensino

Mestrado em Ciência Militares – Especialidade de Infantaria

Trabalho de Investigação Aplicada

A GUERRA NO CIBERESPAÇO: PRINCÍPIOS DA GUERRA CLÁSSICA APLICADOS NA CIBERGUERRA

Autor: Aspirante Aluno de Infantaria Remi Peralez da Silva Peres

Orientador: TCor Inf Mestre José Carlos L. Martins

LISBOA, AGOSTO DE 2010

Academia Militar

Direcção de Ensino

Mestrado em Ciência Militares – Especialidade de Infantaria

Trabalho de Investigação Aplicada

A GUERRA NO CIBERESPAÇO: PRINCÍPIOS DA GUERRA APLICADOS NA CIBERGUERRA

Autor: Aspirante Aluno de Infantaria Remi Peralez da Silva Peres

Orientador: TCor Inf Mestre José Carlos L. Martins

LISBOA, AGOSTO DE 2010

DEDICATÓRIA

À minha família e todos aqueles que sempre me apoiaram!

AGRADECIMENTOS

Este trabalho de investigação aplicada, por muito que digamos que seja um processo solitário a que qualquer investigador está destinado, reúne o contributo de várias pessoas.

Desde o início do mestrado, contei com a confiança e o apoio de inúmeras pessoas e instituições, que em muito ajudaram para que esta investigação se concretizasse.

Ao Tenente-Coronel de Infantaria Mestre José Carlos Lourenço Martins, meu orientador do trabalho, agradeço o apoio, a partilha do saber e as valiosas contribuições para o trabalho, e acima de tudo por me ter acompanhado nesta jornada e por estimular constantemente, de forma assídua, o interesse pelo conhecimento e pela vida académica.

Ao Exm. General Doutor Loureiro dos Santos pela sua disponibilidade em realizar a entrevista.

Ao Tenente-Coronel de Transmissões Doutor Paulo Viegas Nunes, pela oportunidade de assistir à sua aula de Pós-Graduação/Mestrado em Guerra de Informação/Competitive Intelligence, que representou uma oportunidade ímpar de crescimento académico e também pessoal.

Ao Tenente-Coronel de Artilharia Palma Rosinha pela sua partilha de saber que em muito contribuiu para a realização do trabalho.

À Dona Paula da biblioteca pela sua paciência e disponibilidade, durante a fase de pesquisa de documentos que abordassem a temática.

Aos meus pais, Luís José da Silva Peres e Catherine Hélène Françoise Lilette Peralez Peres, por me terem apoiado em todos os momentos da minha vida, transmitindo-me sempre confiança e segurança.

Ao João Pais pela amizade e disponibilidade em me ajudar com pequenas dicas para o trabalho.

E volto a reiterar o apoio do meu orientador, a quem ficarei muito grato para o resto da minha vida!

RESUMO

O presente estudo centra-se na Guerra no Ciberespaço, mais concretamente nos Princípios da Guerra aplicados à Ciberguerra, no qual se pretende verificar se os Princípios da Guerra Clássica identificados e definidos em várias doutrinas militares são aplicáveis à Ciberguerra. Deste modo estudam-se os Princípios da Guerra contemplados em diversas doutrinas militares, de forma a realçar a importância que é dada a estes na conduta de guerras.

Define-se o conceito de Ciberespaço e de Ciberguerra e identifica-se a importância que os Estados e Organizações Internacionais têm vindo a dar a estas novas formas de perpetrar Guerras.

Este assunto revela-se importante nos dias de hoje, visto ser um assunto genuíno e ainda pouco debatido no seio da instituição militar, merecendo a sua devida atenção, não só pelo facto de constituir, nos dias de hoje uma real ameaça para os Estados, mas também porque é necessário acompanhar a evolução tecnológica de modo a conseguir tirar vantagens dela, e precaver-se de eventuais ameaças.

Para garantir o rigor nos resultados obtidos fez-se um estudo essencialmente interpretativista e qualitativo, tendo como suporte de investigação: a Revisão de Literatura, a Análise de Conteúdo, o Estudo de Caso e a Entrevista.

Para além da Análise de Conteúdo de diversos documentos militares doutrinários, estudam-se fundamentalmente dois prováveis casos de Ciberguerra (os ataques cibernéticos contra a Estónia em 2007 e a Guerra dos cinco dias entre a Rússia e Geórgia em 2008), com o intuito de procurar identificar e analisar os Princípios da Guerra Clássica pretendendo, no final do estudo, concluir se os Princípios da Guerra Clássica permanecem actuais, e se podem ser aplicáveis à Ciberguerra. Procura-se desta forma que no futuro, os chefes militares possam eventualmente aplicar esses mesmos princípios, na fase de planeamento de acções de Ciberguerra.

Com este estudo exploratório pode-se concluir que o princípio do Objectivo, Ofensiva, Massa, Manobra, Segurança, Surpresa e Simplicidade são aplicáveis à Ciberguerra e que as acções de Ciberguerra no Ciberespaço podem ser planeadas tendo em conta esses mesmos princípios.

Palavras-chave: Princípios da Ciberguerra; Princípios da Guerra Clássica; Ciberguerra; Ciberespaço

ABSTRACT

The present study is placed upon war on Cyberspace and more specifically on the Principles of War which are applied to the Cyberwar, upon which one aims to verify if the Principles of Classical War, which are identified and defined in various military doctrines are applicable to the Cyberwar. Thus, one studies the Principles of War, which are contemplated on several military doctrines, in order to reveal the importance that is given to those Principles at the war conduct.

One defines the concept of Cyberspace and Cyberwar and identifies the importance that International Countries and Organizations have been valuing to these new ways of enduring wars.

Nowadays this subject is considered important, because it is genuine and less debated among our Military Institution. Therefore, it deserves special attention, not only due to nowadays threat for the Countries, but also due to the necessity of following the technological evolution, in order to take advantages from it and to guard itself from eventual threats.

In order to grant the results strictness, one made an essentially interpretative and qualitative study, having as investigation foundation the Literature´s Revision, the Content´s Analysis, the Case's Study and the Interview.

Besides the content analysis of several military doctrinal documents, one studies mainly two probable Cyberwar cases (Cyber attacks against Estonia in 2007 and the five-day war between Russia and Georgia in 2008), in order to identify and analyse the Principles of Classical War, aiming, at the end of the study, to conclude if they remain valid and if they might be applied to the Cyberwar. By achieving this, one aims that, in the future, the military leaders may, eventually, apply those same Principles in the Cyberwar actions planning.

Through this exploratory study, it may be concluded that the principles of Objective, Offensive, Mass, Maneuver, Security, Surprise and Simplicity are applicable to the Cyberwar and that the Cyberwar actions in the Cyberspace might be planned, bearing in mind those same Principles.

Key Words: Principles of Cyberwar; Principles of Classical War; Cyberwar; Cyberspace

ÍNDICE GERAL

LISTA DE ABREVIATURAS

C2	Comando e Controlo
C2I	Comando e Controlo e Informações
C2W	Guerra de Comando e Controlo
C4ISR	Comando, Controlo, Comunicações, Computadores, Informações, Vigilância e Reconhecimento
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CIMIC	*Civil Military Cooperation* (Cooperação Civil-Militar)
CNA	*Computer Network Attack* (Ataque a Redes de Computadores)
CND	*Computer Network Defence* (Defesa de Redes de Computadores)
CNE	*Computer Network Exploitation* (Exploração de Redes de Computadores)
CNO	*Computer Network Operations* (Operações sobre Redes de Computadores)
COTS	*Commercial Off-The-Shelf* (Software Comercial)
DDoS	*Distributed denial-of-service Attack* (Ataque distribuído de negação de serviço)
DoS	*Denial-of-service Attack* (Ataque de negação de serviço)
EE	Espectro Electromagnético
EMP	Impulso Electromagnético
EW	*Electronic Warfare* (Guerra Electrónica)
GAO	*U.S. Government Accountability Office*
GE	Guerra Electrónica
INFO OPS	*Information Operations* (Operações de Informação)
ONGs	Organizações não Governamentais
OPSEC	Segurança das Operações
OSCE	*Organization for Security and Co-operation in Europe* (Organização para a Segurança e Cooperação na Europa)
OTAN	*North Atlantic Treaty Organization* (Organização do Tratado do Atlântico Norte)
PIO	*Press/Public Information Officer* (Oficial de Informação Pública)
POLAD	*Political Advisor* (Assessor Político)
PSYOPS	Operações Psicológicas
RPC	*People's Republic of China* (República Popular da China)
SIC	Sistemas de Informação e Comunicação
TI	Tecnologias de Informação
TIA	Trabalho de Investigação Aplicada
TO	Teatro de Operações

ÍNDICE DE FIGURAS

ÍNDICE DE QUADROS

INTRODUÇÃO

Nos dias de hoje, a importância dos Sistemas de Informação e Comunicação (SIC) e das Tecnologias de Informação (TI), no quotidiano individual, organizacional e social é uma realidade e uma certeza no futuro, onde cada vez mais se caminha para uma dependência perante estes, sendo necessário acompanhar a evolução, onde obrigatoriamente será necessário desenvolver capacidades técnicas para desenvolver guerras num novo campo de batalha. O Ciberespaço tem vindo a ganhar grande relevo nos últimos anos, proporcionando vantagens competitivas, comunicação entre pessoas, novas formas de gerir e organizar, sustentar o funcionamento de infra-estruturas críticas, entre outros.

Quando foi dada a oportunidade de escolher um tema a desenvolver no trabalho de investigação aplicada (TIA), pretendeu-se abordar algo que fosse actual e desafiante, sendo que, após breves e claras conversas com o meu orientador, surgiu a ideia de abordar o tema da Guerra no Ciberespaço.

Assim, na elaboração do trabalho de investigação aplicada (TIA), pretende-se abordar o tema da "Guerra no Ciberespaço", com o objectivo de procurar evidências de uma possível aplicação dos Princípios da Guerra Clássica na Ciberguerra. Ou seja, a propósito deste estudo procura-se responder se os princípios da guerra clássica são relevantes para uma acção de Ciberguerra no Ciberespaço.

Contudo foi necessário delimitar o estudo, de forma a procurar enquadrar a Ciberguerra. Chegou-se à conclusão que as operações de Ciberguerra, nos manuais, tinham a designação de Operações sobre redes de Computadores (*CNO*) e que estas se enquadram dentro da Guerra de Comando e Controlo (*C2W*), que por sua vez estão enquadradas nas Operações de Informação (*INFO OPS*), como podemos verificar na Figura 1.

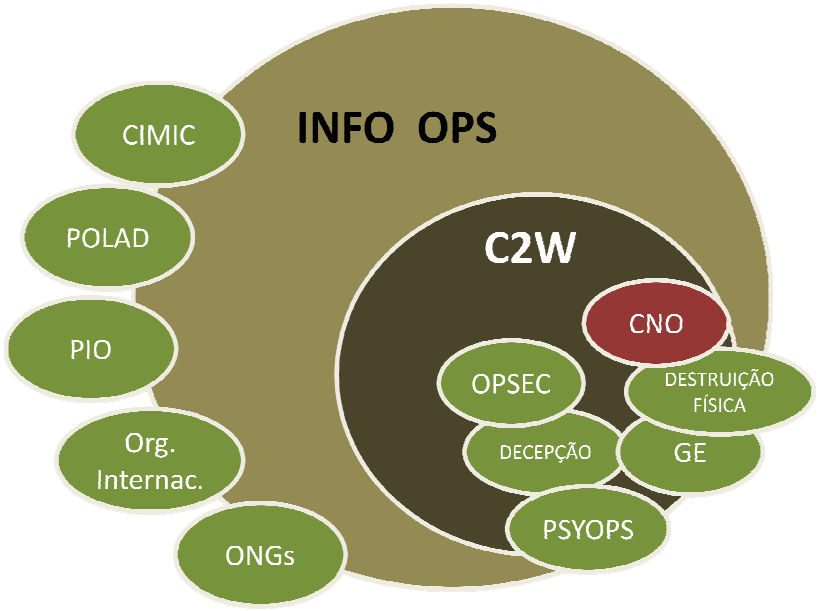


Figura 1. Operações de Informação
Fonte: Adaptado de Nunes (2010)

De acordo com o Tenente-Coronel Viegas Nunes, facilmente se pode constatar com a Figura 1[1], que as Operações de Informação englobam um conjunto de capacidades militares (*OPSEC*, Decepção, *CNO*, Destruição Física, *GE*, *PSYOPS*) e capacidades não militares (*CIMIC*, *POLAD*, *PIO*, Org. Internac. e *ONGs*). Dessas capacidades, as que interessam para a Guerra do Comando e Controlo (*C2W*[2]) são, apenas, as capacidades militares.

Segundo Nunes, as Operações de Informação são o "*conjunto de todos os efeitos gerados de forma coordenada contra o processo de tomada de decisão de um adversário, apoiado por todas as actividades de intelligence*[3]*, com o objectivo de o influenciar, perturbar ou destruir, enquanto simultaneamente se melhora e protege o nosso processo de tomada de decisão contra os efeitos de tais acções e contra qualquer evento involuntário ou casual*" (Nunes, 2010), sendo que, as operações de informação englobam um conjunto de métodos no qual se pode constatar (Figura 2) que as Operações sobre redes de Computadores (*CNO*) fazem parte. Ou seja, considera-se ao longo do trabalho que Operações de Ciberguerra constituem-se num método para desenvolver Operações Militares, permitindo realizar guerras no Ciberespaço.

1 Imagem retirada de uma aula de Pós-Graduação/Mestrado em Guerra de Informação/Competitive Intelligence ministrada pelo Tenente-Coronel Viegas Nunes.
2 É um conceito mais restritivo por se aplicar só a situações de guerra.
3 Produto do resultado da recolha, tratamento, integração, analise, avaliação e interpretação da informação disponível de um Pais ou área.

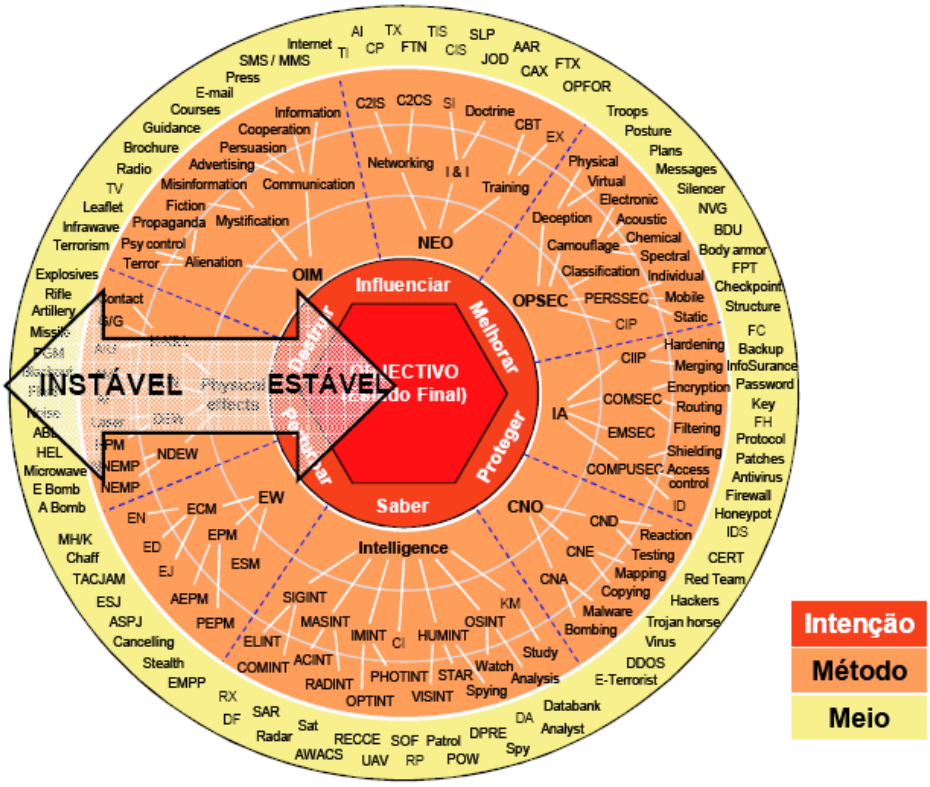


Figura 2. Métodos usados em Operações de Informação
Fonte: Adaptado de Nunes (2010)

Delimitado o âmbito do estudo, a investigação prossegue, com o objectivo de procurar a informação que justifique a relevância da temática e, simultaneamente, permita perceber o "estado-da-arte".

A investigação para este trabalho foi suportada numa pesquisa bibliográfica realizada, primeiramente, a partir de relatórios Nacionais e Internacionais de incidentes no ciberespaço de fontes credíveis, como seja o caso, a título exemplificativo, dos ataques efectuados através da Internet (e.g. *Denial of Service*) à Estónia em 2007 e Geórgia em 2008. Em segundo lugar, foram também determinantes alguns relatórios de segurança da informação, (e.g. *McAfee*) e manuais de doutrina de países, como os Estados Unidos da América, o Reino Unido e a França. Acederam-se a trabalhos académicos já realizados no âmbito desta temática, e por fim realizou-se uma entrevista ao Exmo. General Loureiro dos Santos. Esta possibilitou, através dos dados verbais obtidos, consolidar os principais conceitos que acompanham o trabalho.

O presente trabalho encontra-se dividido em seis capítulos, reflectindo a abordagem da metodologia de investigação aplicada. Após a introdução, dedica-se um capítulo à metodologia de investigação empregue, de modo a centrar num capítulo o objectivo da investigação, bem como a questão central levantada a que nos propomos responder, com as respectivas questões derivadas e pressupostos. Ainda, neste capítulo será apresentada a

revisão de literatura realizada e apresentado o modelo conceptual de validação da problemática, proposto para realizar o trabalho.

O segundo capítulo é dedicado aos princípios da guerra, com o objectivo de enunciar e analisar os princípios da guerra clássica, em estudo neste trabalho de investigação aplicada (TIA). Procura-se simultaneamente, enunciar alguns princípios da guerra, identificados em doutrinas de outras potências militares, e demonstrar a importância dos princípios da guerra na condução da guerra.

No terceiro capítulo, demonstra-se a relevância e actualidade das Operações de Ciberguerra, que são desenvolvidas essencialmente no domínio do Ciberespaço. Para tal, é feita uma delimitação e define-se o âmbito de estudo, apresentando os conceitos de Ciberguerra e de Ciberespaço adoptados no trabalho.

No quarto capítulo analisam-se dois estudos de casos: o ataque cibernético[4] contra a Estónia em 2007 e a Guerra dos cinco dias entre a Rússia e a Geórgia em 2008, que do nosso ponto de vista e até à actual data, se podem classificar como prováveis casos de Ciberguerra de acordo com a definição adoptada neste estudo. É simultaneamente neste capítulo que se materializa o objectivo do trabalho, ou seja, é da análise destes estudos de casos que será possível responder à questão central, em conjunção com a diversa documentação analisada e validada e ainda com a entrevista semi-estruturada realizada ao Exmo. General Doutor Loureiro dos Santos.

O quinto capítulo será dedicado à entrevista semi-estruturada, realizada ao Exmo. General Doutor Loureiro dos Santos. Assim, serão citados excertos da entrevista realizada, que do nosso ponto de vista, são importantes para validar a questão derivada e consequentemente a questão central

O estudo termina com a apresentação das conclusões, entendidas como adequadas e ajustadas ao objectivo do presente trabalho, assim como do identificar de algumas das suas limitações e do enunciar de possíveis estudos a realizar no âmbito desta temática.

4 Entendem-se por ataque cibernético, ataques no Ciberespaço a Infra-estruturas críticas da Internet (como o caso de sítios de Bancos, Comunicação Social…)

1. METODOLOGIA DE INVESTIGAÇÃO

1.1 OBJECTIVOS

O processo metodológico inicia-se através de uma pesquisa bibliográfica (e.g., artigos científicos, documentos doutrinários militares e relatórios de segurança Nacionais e Internacionais), após o que se procura efectuar uma revisão de literatura, de modo a obter, sobre o tema em questão, a matriz de conceitos. Definiu-se, em seguida, a questão central que orienta a investigação.

A abordagem metodológica seguida é fundamentalmente interpretativista e baseia-se, essencialmente, na análise documental, no estudo de casos da Estónia (crise russo-estoniana de Maio de 2007), na guerra dos cinco dias entre a Rússia e a Geórgia em Agosto de 2008, e numa entrevista semi-estruturada ao Exmo. General Doutor Loureiro dos Santos, tendo como objectivo principal chegar a conclusões que possibilitem responder à questão central.

Pretende-se com este estudo, identificar os princípios da guerra clássica mais relevantes para a Ciberguerra, de acordo com as fontes de materiais empíricos referenciados.

1.2 FORMULAÇÃO DO PROBLEMA

A metodologia de investigação seguida no trabalho obedece ao esquema apresentado na Figura 3 de *Quivy* e *Campenhoudt* (Quivy, et al., 1992). Assim, após a formulação da pergunta de partida, efectuou-se uma revisão de literatura, tendo em vista conhecer o estado da arte nesta temática. Posteriormente, foi definida com rigor a questão central, a questão derivada e os pressupostos a seguir no estudo. A abordagem de investigação efectuada é interpretativista e qualitativa, tendo como suporte os métodos de investigação: Análise de Conteúdo, o Estudo de Caso e a Entrevista.

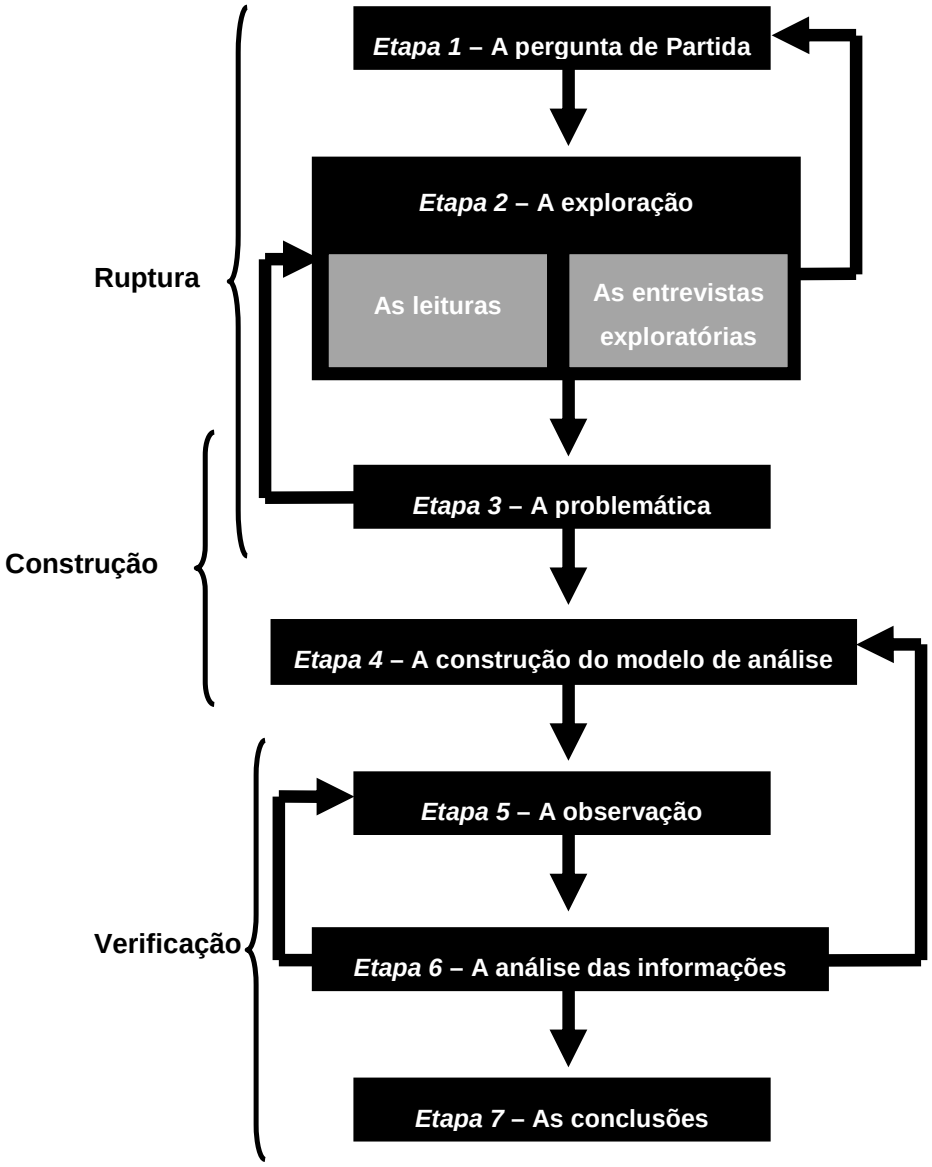


Figura 3. Metodologia de Investigação

Fonte: Quivy e Campenhoudt (1992, p.30)

A **questão central** à qual se pretende responder é a seguinte: **São os Princípios da Guerra clássica aplicáveis à Ciberguerra?**

Assim sendo, e para dar resposta à questão central, levantou-se a seguinte questão derivada: Quais os princípios da guerra clássica mais relevantes na Ciberguerra, atendendo aos nove princípios da guerra clássica?

Por sua vez, para responder à questão derivada, levantou-se como pressupostos, a possível utilização de cada princípio da guerra clássica na Guerra no Ciberespaço (*Objectivo*, *Ofensiva*, *Massa*, *Economia de Forças, Manobra*, *Unidade de Comando*, *Segurança*, *Surpresa* e *Simplicidade*). Procura-se validar esses mesmos pressupostos e responder deste modo, à questão derivada e consequentemente, à questão central, através

de uma análise pormenorizada de cada um dos princípios da guerra clássica, com base em conceitos doutrinários, estudos académicos já realizados no âmbito da temática, análise dos casos particulares de Ciberguerra na Estónia e na Geórgia e na entrevista possível realizada.

1.3 REVISÃO DE LITERATURA

Apresenta-se, nesta secção, as principais fontes de suporte teórico e prático do trabalho, as quais permitiram definir a matriz de conceitos, que se apresenta no Quadro 1 e validar a questão central apresentada.

Quadro 1. Matriz de Conceitos

Conceito	Definição
Operações de Informação	"*As INFO OPS definem-se como, acções coordenadas que visam influenciar decisores e o processo de decisão do inimigo/adversários ou terceiros, em apoio dos nossos objectivos políticos e militares, afectando os seus sistemas de Comando e Controlo e Informações (C2I) e os seus Sistemas de Informação e Comunicação (SIC), ao mesmo tempo que exploram/protegem os nossos sistemas C2I e SIC. Existem duas categorias principais de INFO OPS, dependentes da natureza das acções desenvolvidas: INFO OPS ofensivas e INFO OPS defensivas*" (RC-OP, 2005 p. 1).
Guerra Electrónica (EW)	"*A GE define-se como a acção militar que explora o EE, englobando a intercepção e a identificação de emissões electromagnéticas, o emprego de energia electromagnética, incluindo a energia dirigida, para reduzir ou impedir o uso hostil do EE e as acções que garantem o seu uso efectivo pelas nossas forças*" (RC-OP, 2005 p. 1).
Computer Network Operations (CNO)	"*A oportunidade e eficácia das Operações sobre Redes de Computadores (CNO), é proporcional à dependência do adversário dos SIC e Tecnologias de Informação (TI). As CNO compreendem o Ataque, Exploração e Defesa de Redes de Computadores em sentido genérico*." (RC-OP, 2005 p. 1-7)
Computer Network Attack (CNA)	Medidas tomadas por meio do uso de redes de computadores para interromper, negar, corromper ou destruir informações em computadores e redes de computadores ou os computadores e as redes próprias. (Joint Publication 3-13, 2006)
Computer Network Defence (CND)	Medidas tomadas por meio do uso de redes de computadores para proteger, monitorar, analisar, detectar e responder a actividades não autorizadas no âmbito dos sistemas de informação e redes de computadores. (Joint Publication 3-13, 2006)

Quadro 1. Matriz de Conceitos (continuação)

Conceito	Definição
Computer Network Exploitation (CNE)	"*A Exploração de Redes de Computadores consiste no conjunto de acções tomadas para ganhar acesso aos Sistemas de Informação (SI), explorar a informação neles residente e de uma forma geral, fazer uso, para proveito próprio, de Sistemas de Informação e Comunicação (SIC) de terceiros."* (RC-OP, 2005 p. 1-8)
Ciberguerra	Acto de Guerra entre grupos políticos, no Ciberespaço, destinado a submeter o adversário à sua vontade, visando determinado fim politico.
Teatro de Operações	*"O teatro de operações é a parte do teatro de guerra necessária à condução ou apoio das operações de combate*" (RC-OP, 2005 p. 10).
Ciberespaço	É um ambiente virtual, suportado através de uma rede mundial de computadores interligados pela infra-estrutura de comunicações, no qual se realizam interacções entre pessoas ou agentes de software, permitindo uma comunicação de muitos para muitos e com o objectivo principal de partilhar informação.
Hacker	"*Individuo que usa a tecnologias dos computadores de maneira não prevista pelo vendedor. É comum aplicar este termo às pessoas que atacam outras pessoas usando computadores."* (Krekel, 2009 p. 77)
Hacktivism	"*Acções com o intuito de comunicar uma mensagem social ou política, ou apoiar a posição de um grupo político ou ideológico. Estas actividades incluem o roubo de dados, desfiguração de sítios, ataques de negação de serviços, redireccionamento e outros.*" (Krekel, 2009 p. 78)
Hacktivist	"*Atacante que pratica hacktivism."* (Krekel, 2009 p. 78)
Ataques de negação de serviços (DDoS)	Ataques que visam "*bloquear ou esgotar os recursos disponíveis de uma máquina impedindo que os outros lhe acedam*" (Santos, et al., 2008 p. 169).

Em termos de metodologia de investigação, seguiu-se o método científico de Raymond Quivy e Luc van Campenhoudt, apresentado no seu livro "*Manual de Investigação em Ciências Sociais*" (1992). Procura-se, na elaboração e aplicação de Inquéritos (aplicação da entrevista), reflectir as boas práticas, segundo os conceitos apresentados por *Ghiglione* e *Matalon* (2001). Por fim, na abordagem aos estudos de caso, teve-se como referência os conceitos apresentados por Ferreira e Serra (2009).

No segundo capítulo, "Princípios da Guerra" efectua-se a identificação e análise dos princípios, utilizando como fontes documentais os livros de *Sun Tzu* (2006) e *Carl Von Clausewitz* (2003), que permitem estabelecer uma ligação entre os princípios da guerra utilizados na antiguidade e os actuais. Na abordagem aos princípios da guerra utilizados na actualidade em vários países tivemos, como grande auxílio, o livro de José Lopes Alves (1998) e um documento escrito por *Robert Frost* (1999). Por último, conclui-se o capítulo,

tendo como auxílio o manual de doutrina militar Portuguesa (RC 130-1 , 1987), que aborda os princípios da guerra actuais e aceites.

No capítulo "Doutrinas de Ciberguerra" utilizam-se como referências:

- No que respeita à delimitação e definição de Ciberespaço o manual de doutrina dos E.U.A "*Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*" (JP 2-01.3, 2000), o dicionário de termos militares dos E.U.A. "*Department of Defense Dictionary of Military and Associated Terms*" (JP 1-02, 2009), a política para o Ciberespaço da Casa Branca "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*" (Casa Branca, 2009), a estratégia de cibersegurança do Reino Unido "*Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space"* (OCS, 2009), o Livro Branco de Defesa e Segurança Nacional da França (Le Livre Banc, 2008), o livro "*As Guerras que já aí estão e as que nos esperam - se os políticos não mudarem*" do General Loureiro dos Santos (Santos, 2009), o Livro Verde relativo a um Programa Europeu de Protecção das Infra-estruturas Críticas (Livro Verde, 2005) e a entrevista realizada ao Exmo. General Doutor Loureiro dos Santos;

- No que respeita à delimitação e definição de Ciberguerra, tem-se como referências a 55º sessão da Assembleia Europeia de Segurança e de Defesa (Chope, et al., 2008), um trabalho ("*La Cyberguerre*") realizado por um ex-consultor do Ministério de Defesa em França, especialista em assuntos militares e guerra da informação *Laurent Murawiec* (Murawiec, 1999), bem como a entrevista realizada ao Exmo. General Doutor Loureiro dos Santos;

- Utiliza-se ainda como referências a doutrina de segurança da informação da Federação Russa, onde está explícito oficialmente a totalidade das metas, objectivos, princípios e directrizes básicas para garantir a segurança da informação na Federação Russa (DISRF, 2000), relatórios *Wilson Clay* que abordam a temática dos *Cyber Attacks* (Clay, 2001; Clay, 2007)*,* um relatório de *Bryan Krekel* sobre as capacidades da *RPC* para conduzir Ciberguerra e *CNE* ("*Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*") (Krekel, 2009).

No capítulo de "Estudo de casos" utiliza-se como referências principais, para justificar a presença dos princípios da guerra nos casos a estudos, relatórios de *Wilson Clay*, dos serviços de pesquisa para os Congressos (*CRS*) da Federação de Cientistas Americanos (*FAZ*) que abordam a temática dos *Cyber Attacks* (2001; 2007; 2008)*,* bem como um relatório do centro de excelência de ciberdefesa da Organização do Tratado do Atlântico Norte - *OTAN* (Tikk, 2008), entre outros.

1.4 PROBLEMÁTICA E MODELO DE ANÁLISE

A Figura 4 indica as fases do modelo conceptual de validação da problemática proposto para realizar o trabalho.

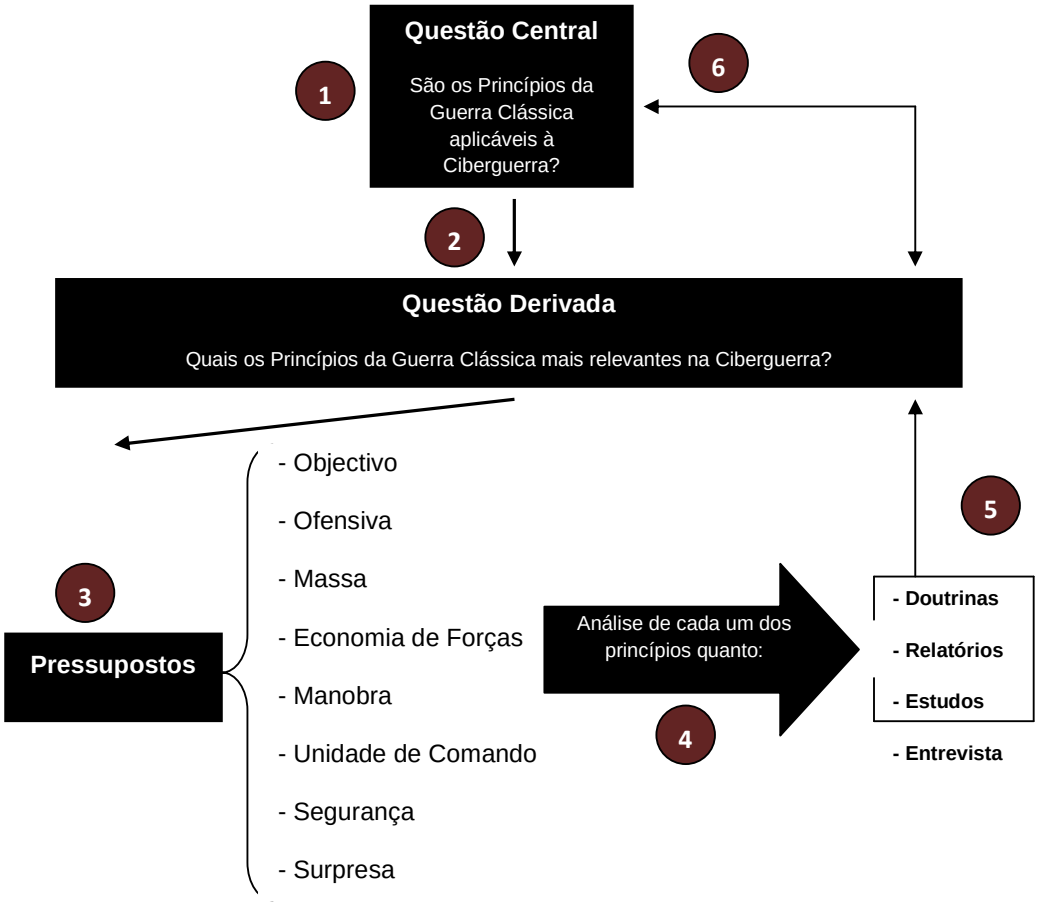


Figura 4. Modelo Conceptual de Validação da Problemática

Após (1) formulada a questão central, (2) a questão derivada e (3) levantados os pressupostos, (4) efectuou-se uma análise pormenorizada de cada um dos princípios da guerra em questão, tendo como apoio as doutrinas militares de superpotências, os relatórios de segurança, alguns estudos relevantes e ainda através da entrevista efectuada como método de investigação aplicado nesta investigação, com o objectivo de (5) responder à questão derivada e consequentemente (6) à questão central.

> "*Os Princípios são assunto de senso comum, de julgamento, a sua aplicação varia com as circunstâncias; não se escrevem, não se ensinam*…"[5] (Foch, 1903, prefácio)

2. PRINCÍPIOS CLÁSSICOS DA GUERRA

Este capítulo tem por objectivo identificar e apresentar os Princípios da Guerra em causa neste estudo, adoptados pelo Exército Português e descritos no Regulamento de Campanha 130-1 Operações de 1987.

Para tal, na primeira secção "*Definição, origem e importância dos Princípios da Guerra*" é feita uma primeira abordagem do tema, relacionando três conceitos (Leis, Princípios e Regras), sendo que, após esta relação entre conceitos é apresentada uma definição de Princípios da Guerra, adoptada no Regulamento de Campanha do Exército Português de 1987 (RC 130-1). Após apresentar a definição, é feito um pequeno enquadramento da origem dos Princípios da Guerra, apresentando dois estrategistas (*Sun Tzu* e *Carl von Clausewitz*), que em termos históricos tiveram grande influência no presente, na medida em que, os textos destes estrategistas (Arte da Guerra de *Sun Tzu* e Princípios da Guerra de *Clausewitz*) tiveram grande influência no processo de evolução dos Princípios da Guerra que conhecemos hoje.

Na segunda secção "*Princípios da Guerra em doutrinas militares*" é apresentado os Princípios da Guerra adoptados por algumas superpotências militares (e.g. E.U.A., Reino Unido, Austrália, ex-união Soviética, França e República Popular da China), de forma a mostrar que apesar de adoptarem Princípios da Guerra diferentes, todos eles concorrem para o mesmo objectivo, de auxiliar o comandante na tomada de decisão.

Finalmente, na terceira secção "*Princípios da Guerra adoptados por Portugal*" são apresentados os Princípios da Guerra adoptados pelo Exército Português no RC130-1.

Na última secção são feitas algumas considerações finais, de modo a reforçar quais os Princípios da Guerra fundamentais, e justificar a escolha destes para o trabalho de investigação aplicada.

2.1 DEFINIÇÃO, ORIGEM E IMPORTÂNCIA DOS PRINCÍPIOS DA GUERRA

Antes de enumerar e definir os Princípios da Guerra é necessário enquadrar estes princípios tendo em conta a distinção de conceitos diferentes como as leis, os princípios e as regras.

[5] Tradução livre da responsabilidade do autor

"*Enquanto as «leis» nos caracterizam o fenómeno «guerra», no que este tem de permanente e evolutivo, os princípios e regras dizem-nos como nos devemos comportar perante o fenómeno, ou melhor, como actores no fenómeno.*" (Couto, 1988 pp. II-34)

Apesar dos princípios e regras se apresentarem muito idênticos entre si, pode-se destacar algumas diferenças. Segundo *Litre* os princípios são os primeiros preceitos de uma ciência ou arte, ou seja, os Princípios da Guerra são os preceitos primeiros (ou básicos) da arte da guerra (Litre *apud* Couto, 1988).

Os princípios são normas primárias, que se apresentam em número reduzido e podem ser aplicados a todas as situações, apresentando-se imutáveis no tempo e no espaço. Ao contrário das regras que são normas secundárias (que derivam dos princípios) e se apresentam em maior número. Todavia, as regras podem variar ao longo do tempo (Couto, 1988). Ainda de referir que os princípios são produto de ampla liberdade espiritual, e aplicáveis a todas as situações, ao contrário das regras, em que o seu o âmbito se restringe ao concreto e limitado, sendo o valor prático delas maior que o dos princípios. Os princípios não são influenciados pela Organização e pela Tecnologia ao contrário das regras que são directamente influenciadas pela Organização e pela Tecnologia (Alves, 1998).

Os Princípios da Guerra "*são normas de acção fundamentais que devem ser respeitadas na conduta da guerra para permitir e facilitar o êxito na prossecução da mesma. A sua adequada aplicação é essencial ao exercício do comando e à condução, com sucesso, das operações militares. Os princípios da guerra estão relacionados entre si e, conforme o caso, podem tender para mutuamente se reforçarem ou se oporem. Consequentemente, o grau de aplicação de um determinado princípio variará com a situação.*" (RC 130-1 , 1987 pp. 3-3)

Em termos históricos pode-se verificar que os Princípios da Guerra estão presentes em diferentes épocas e que foram sujeitos à evolução de acordo com a mentalidade e conhecimento do Homem nos diferentes momentos da história.

A título de exemplo, pode-se enumerar duas grandes personalidades de diferentes épocas: *Sun Tzu* na antiguidade e *Carl von Clausewitz* no séc. XVIII.

Sun Tzu viveu entre 544 – 496 A.C e é considerado um dos maiores estrategistas de todos os tempos e para muitos o Pai da Estratégia, sendo autor de um famoso clássico intitulado "*A Arte da Guerra*". Esta obra é um tratado de Estratégia escrito há mais de 2400 anos que continua a ser aplicado nos dias de hoje, não só no domínio militar como também no domínio da gestão. Ao longo do seu livro ele desenvolve um conjunto de pressupostos essenciais para orientação dos chefes militares.

Carl von Clausewitz viveu entre 1 de Junho de 1780 a 16 de Novembro de 1831 e também ele considerado um grande estrategista militar, é autor de um clássico "*Princípios da Guerra*".

Pode-se verificar que estes clássicos da estratégia (*A Arte da Guerra* e *Princípios da Guerra*), tiveram grande influência no processo de evolução dos princípios da guerra e constituem a base daquilo que são hoje os princípios da guerra, sendo que, no Quadro 2 se verifica isso mesmo. Ou seja, ao longo dos textos de *Sun Tzu* e *Clausewitz*, encontram-se frases (Consultar Apêndice A) onde implicitamente se encontram os princípios da guerra em estudo neste trabalho. Por exemplo, numa frase de *Sun Tzu*, "*toda a guerra é baseada no engano*" (Tzu, 2006 p. 69) podemos constatar isso mesmo, ao associar esta frase ao princípio da surpresa, na medida em que a surpresa consiste em criar situações inesperadas, ou seja, enganar o inimigo e impedir que ele consiga reagir eficazmente em tempo oportuno.

Quadro 2. Alguns princípios da guerra actuais presentes em textos de Tzu e Clausewitz.

Princípios da Guerra actuais (RC 130-1)	Estrategistas	
	Sun Tzu	Carl von Clausewitz
Objectivo		**X**
Ofensiva	**X**	**X**
Massa	**X**	**X**
Economia de Forças	**X**	**X**
Manobra	**X**	
Unidade de Comando	**X**	
Segurança	**X**	
Surpresa	**X**	**X**
Simplicidade	**X**	

Estes longos e complexos textos, ao longo do tempo e com o acumular de experiências decorrentes das Guerras, foram sofrendo alterações, dando origem a curtas listas de normas com a finalidade última de facilitar a acção de comando dos militares.

Desta evolução surgem os Princípios da Guerra, que desde o final da II Guerra Mundial constituem a base da doutrina militar e orientam a conduta dos chefes militares em todo o Mundo.

Por fim é de salientar que não podemos encarar os princípios da guerra como sendo uma receita infalível para o sucesso das operações militares. Contudo, há que ter em conta que se bem interpretados, aplicados e combinados entre si, os chefes militares terão ao seu dispor um conjunto de normas de acção fundamentais, que devem ser respeitadas na conduta da guerra e consideradas durante o planeamento, de modo a contribuir para o sucesso das operações militares.

2.2 PRINCÍPIOS DA GUERRA EM DOUTRINAS MILITARES

Com o termo da II Guerra Mundial, grande parte dos Estados achou necessário a existência de uma doutrina que permitisse com maior facilidade e fiabilidade, preparar e empregar todos os recursos disponíveis, com base nas experiências colhidas em conflitos passados e ideias dos pensadores, antigos e modernos. (Alves, 1998 p. 80)

A existência de uma doutrina tem por objectivo englobar "*um conjunto de princípios e regras que visam orientar as acções das forças e elementos militares, no cumprimento da missão operacional do Exército na prossecução dos objectivos nacionais*". (RC-OP, 2005 p. 6)

Apareceram várias classificações de forma a classificar a informação em categorias lógicas e sistematizando-as com o objectivo de melhorar o seu entendimento. Em todo o Mundo as Forças Armadas, com mais ou menos experiência no tempo e espaço, acabaram por adoptar Princípios da Guerra. As variações e diferenças entre os diferentes Princípios da Guerra adoptados por vezes são mínimas ou quase imperceptíveis. (Alves, 1998)

Na doutrina do Exército dos E.U.A. são 9 (nove) os Princípios da Guerra adoptados: Objectivo, Ofensiva, Massa, Economia de Forças, Manobra, Unidade de Comando, Segurança, Surpresa, Simplicidade.

Estes Princípios da Guerra poucas alterações sofreram entre 1921 e a actualidade, sendo que, apenas dois dos princípios actualmente aceites, Manobra e Unidade de Comando, eram respectivamente designados de Movimento e Cooperação.

Para além destes nove Princípios da Guerra que consideram fundamentais para o desenrolar de qualquer acção, têm ainda em conta outros princípios (Iniciativa, Agilidade, Profundidade, Sincronização e Versatilidade) não menos importantes e essenciais para alcançar a vitória, que por si não garantem o sucesso, mas na sua ausência correm-se riscos (FM3-0, 2001).

Na doutrina militar do Reino Unido são adoptados dez Princípios da Guerra (Selecção e manutenção do Objectivo, Manutenção do Moral, Acção Ofensiva, Segurança, Surpresa, Concentração da força, Economia de esforço, Flexibilidade, Cooperação e Sustentabilidade) que foram publicados após a I Guerra Mundial e aperfeiçoados ao longo das décadas seguintes, até à actualidade. Segundo o manual de defesa e doutrina do Reino Unido *"os Princípios da Guerra guiam os comandantes e a sua equipa no planeamento e condução da guerra. Eles estão resistindo, mas não são imutáveis, verdades absolutas e não fornecem base adequada para todas as actividades militares. A relativa importância de cada um pode variar de acordo com o contexto, e a sua aplicação requer julgamento, senso comum e inteligência para interpretá-los*"[6] (JDP 0-01, 2008 pp. 2 - 3).

[6] Tradução livre da responsabilidade do autor

Na ex-união Soviética de acordo com *Raymond Garthoff* citado em Alves, são considerados seis princípios fundamentais (ofensiva e defensiva, manobra e iniciativa, concentração e economia de forças, força viva e progressão, aniquilamento, unidade e acção combinada) e doze princípios secundários, também eles importantes (manobra em retirada, reservas adequadas, planeamento, comando e direcção, moral e controlo político, previsão, informação e reconhecimento, decepção, surpresa, segurança, preparação, imposição e solidez das retaguardas) (1998).

Em França, os Princípios da Guerra adoptados desde 1903 são apenas três (Liberdade de Acção, Concentração do Esforço e Economia de forças. Do ponto de vista de Ferdinand Foch existem várias maneiras de apresentar os Princípios da Guerra, podendo a partir destes divergir em muitos outros princípios. Por exemplo, no princípio da Economia de força, anteriormente referido, deverá ter-se em conta o princípio da velocidade, surpresa, escolha do momento, cooperação, máxima intensidade, Concentração máxima dos meios (Foch, 1903).

No caso do Exército da República Popular da China, os princípios apresentados são em elevado número, dos quais se apresentam os seguintes:

"- Atacar primeiro os grupos isolados do inimigo e só depois as suas forças mais poderosas;

- Do mesmo modo, conquistar inicialmente as pequenas povoações e só mais tarde as grandes cidades;

- O objectivo principal é a destruição das forças inimigas;

- É necessário dispor de forças duas, três, quatro ou mesmo cinco vezes superiores às do inimigo a fim de o envolver por todos os lados e de o aniquilar totalmente;

- Não travar combates não preparados nem sem perspectivas de sucesso;

- Os combatentes devem lutar com todo o vigor, não olhando a sacrifícios ou fadigas nem hesitando em travar combates sucessivos sem repouso;

Actuar sobre o inimigo quando se desloca, mas simultaneamente, preparar a conquista e a ocupação dos seus pontos fortes e das suas bases;

- Reforçar-se com o pessoal e com as armas tomados ao inimigo - «as fontes de homens e material é na frente que se encontram»;

- Utilizar os períodos de pausa entre as campanhas para reorganizar as unidades, instruir as tropas e dar-lhes repouso – tais períodos não devem, porém, ser muito longos pelos inconvenientes que a inacção das tropas e a falta de pressão sobre o inimigo representam." (Alves, 1998 p. 84)

O Quadro 3 apresenta o resumo dos Princípios da Guerra adoptados pelos Países mencionados. Neste quadro, apesar das últimas três colunas constituírem uma interpretação americana dos princípios da guerra (Frost, 1999) adoptados pelos respectivos países, a análise do quadro permite verificar que apesar das diferenças encontradas nos diferentes

países, a base dos princípios são comuns a todos eles, ou seja, apesar dos diferentes países utilizarem designações diferentes para alguns princípios, o conteúdo que nela abordam é o mesmo (e.g. é chamado por princípio da ofensiva nos E.U.A., enquanto que no Reino Unido, Austrália e República Popular da China designam para o mesmo princípio por acção ofensiva).

Quadro 3. Princípios da Guerra em vários Países

E.U.A.	Reino Unido e Austrália	Ex-união Soviética "Princípios da Arte Militar"	França	República Popular da China
Objectivo	Selecção e Manutenção do Objectivo			Selecção e Manutenção do Objectivo
Ofensiva	Acção Ofensiva			Acção Ofensiva
Massa	Concentração da Força	Massa e Correlação da força	Concentração do Esforço	Concentração da Força
Economia de Forças	Economia de Esforço	Economia e Suficiência da força		
Manobra	Flexibilidade	Iniciativa, Mobilidade e Tempo		
Unidade de Comando	Cooperação	Interoperabilidade e Coordenação		Iniciativa e Flexibilidade
Segurança	Segurança			Segurança
Surpresa	Surpresa	Surpresa	Surpresa	Surpresa
Simplicidade				
	Sustentabilidade e Manutenção do Moral	Ataques simultâneos a todos os níveis, preservação da eficácia de combate	Liberdade de Acção	Moral, Mobilidade, Mobilização Politica, Liberdade de acção

Fonte: Adaptado de (Frost, 1999 p. 6)

Estas diferenças surgem pelo facto de alguns países serem detentores de uma experiência mais rica, fruto das várias actividades militares, no tempo e no espaço, que possibilitaram retirar delas um maior número de lições aprendidas, e por outro, pelo facto de nações com menos experiência no campo de batalha, adoptarem princípios oriundos da doutrina do seu principal aliado, ou ainda quando integrados em organizações, como o caso de Portugal em relação à *OTAN*.

É interessante verificar, que no Quadro 3 existem princípios transversais a todos os países, e outros princípios que são tidos em conta apenas por alguns. Por exemplo, o

princípio da Surpresa é transversal e designado da mesma forma em todos os países mencionados. Verifica-se também que existe o Princípio da Massa nos E.U.A. que é transversal a todos os restantes Países, contudo com designações diferentes nos restantes. Ou então, o Princípio da Simplicidade que apenas é tido em conta nos E.U.A.

Pode-se consequentemente afirmar que os princípios adoptados surgiram com a finalidade de proporcionar ao chefe militar um conjunto de pontos-chave a ter em consideração para realizar um planeamento racional e fiável conduzindo-o ao sucesso.

2.3 PRINCÍPIOS DA GUERRA ADOPTADOS EM PORTUGAL

Após se ter apresentado a origem dos Princípios da Guerra adoptados por algumas superpotências e a sua importância, apresentam-se de seguida os Princípios da Guerra, em estudo neste trabalho de investigação aplicada.

Também em Portugal os Princípios da Guerra adoptados pelo Exército Português sofreram alterações ao longo do tempo. Exemplo disso, é o livro escrito em 1952 pelo General Frederico Lopes da Silva (antigo professor na Escola do Exército e chefe do Estado-Maior do Exército em 1956) intitulado de "*Os Princípios da Guerra: Factores da Guerra, Leis da Ciência, Regras da Arte*". Neste livro, decidiu compilar uma síntese de conceitos com o objectivo de tornar mais claro e acessível àqueles que pretendessem explorar os segredos para alcançar uma boa liderança e conduzir bem as suas tropas. No Anexo A encontra-se uma tabela dos princípios que segundo ele seriam importantes a ter em conta, não para resolver qualquer situação de Guerra, mas sim, para ajudar o chefe a discernir as situações que enfrenta e escolher o melhor caminho para resolver os problemas. (Silva, 1952)

Contudo, por imperativo de acordos político-militares com outras nações do Ocidente, como a *OTAN*, levou a que o Exército Português abandonasse os princípios da guerra aceites até começo dos anos 50, adoptando outros princípios com vista a uniformizar conceitos dentro das alianças. (Alves, 1998)

Os Princípios da Guerra presentemente considerados na doutrina militar nacional[7] são os seguintes: Objectivo, Ofensiva, Massa, Economia de forças, Manobra, Unidade de Comando, Segurança, Surpresa, Simplicidade, para os quais se procura neste estudo verificar a sua aplicabilidade às novas tipologias de guerra, designadamente às operações de Ciberguerra desenvolvidas num novo domínio designado de Ciberespaço.

É de salientar que, com o Quadro 3, podemos verificar que os princípios da guerra adoptados por Portugal e que são objecto de estudo desta investigação, são os mesmos

[7] Para uma consulta mais pormenorizada, encontra-se no Anexo B os Princípios da Guerra adoptados na doutrina militar nacional.

adoptados pelos E.U.A e por outros países, apesar de em alguns princípios atribuírem designações diferentes.

Estes nove princípios da Guerra apresentados no Quadro 4, conjuntamente com os respectivos indicadores, irão permitir orientar a análise realizada ao estudo de casos propostos e a outros documentos referenciados para que a análise de conteúdo a documentos relevantes (e.g. relatórios institucionais de descrição de incidentes no ciberespaço), possibilite justificar a utilização na Ciberguerra dos diversos Princípios da Guerra referidos.

Quadro 4. Princípios da Guerra Clássica e respectivos indicadores

Princípios da Guerra (RC 130-1)	INDICADORES	
	Definição	**Palavras-Chave**
Objectivo	- Qualquer operação militar deverá contribuir para obtenção do **objectivo último** da guerra (aniquilamento das forças armadas do adversário e da sua vontade de combater);	Objectivo último
	- **Objectivos definidos de forma clara** e inequívoca;	Objectivos claros
	- Devem ser **exequíveis** e alcançados com os meios que a força dispõe;	Objectivos exequíveis
	- Objectivos escolhidos **em função da missão**, dos **meios disponíveis**, do **inimigo** e das **características da área de operações**.	
Ofensiva	- Acção Ofensiva necessária para **obter resultados decisivos** e para conservar ou reconquistar a liberdade de acção;	Resultados decisivos
	- Acção Ofensiva permite tomar iniciativa, impor a sua vontade ao inimigo, marcar o ritmo e influenciar o curso da batalha e explorar os **pontos fracos do inimigo**.	Pontos fracos do IN
Massa	- **Empregar potencial de combate superior** ao inimigo no local e momento decisivo;	Potencial superior
	- Este princípio em conjugação com os outros princípios permite a forças numericamente inferiores no seu conjunto, obtenham uma superioridade local e momentânea, decisiva para o desenrolar das operações.	
Economia de Forças	- **Emprego judicioso dos meios** à sua disposição, reduzindo ao mínimo o desgaste desses meios e procurando empregá-los de forma decisiva no local e momento mais adequados;	Emprego judicioso dos meios
Manobra	- **Dispor as forças** de forma a colocar o Inimigo em posição desvantajosa;	Disposição das forças
	- Permite a correcta aplicação do princípio da massa e o **princípio da economia de forças**;	Massa e Economia de Forças
	- Contribui para **conservar liberdade de acção**, manter **iniciativa** e **explorar os resultados do combate.**	Liberdade de acção Iniciativa
Unidade de Comando	- **Acção coordenada** de todas as forças de forma a fazer convergir os seus esforços tendo em vista um objectivo comum;	Acção coordenada
	- Existência de Unidade de **Doutrina e de Comando** a orientarem a acção das forças;	Unidade de Doutrina e Comando
	- **Investir num único Comandante a autoridade necessária**.	Autoridade única

Quadro 4. Princípios da Guerra Clássica e respectivos indicadores (continuação)

Princípios da Guerra (RC 130-1)	INDICADORES	
	Definição	**Palavras-Chave**
Segurança	- Permite **conservar liberdade de acção**;	Liberdade de acção
	- **Permite negar ao Inimigo a possibilidade de obter informações sobre as forças amigas e os seus planos** e evita-se ser surpreendido pelo adversário;	Informação
Surpresa	- **Criar situações inesperadas** para o qual o Inimigo não esteja em condições de reagir eficazmente em tempo oportuno;	Situações inesperadas
	- Permite retirar ou **limitar liberdade de acção do adversário**, colocando-o em posição desvantajosa;	Posição desvantajosa
	- Contribui para a surpresa a velocidade, a decepção, a concentração inesperada de forças num dado local e momento;	Manobra Ofensiva Segurança
	- A surpresa **facilita a manobra**, estimula a **ofensiva** e favorece a **segurança**.	
Simplicidade	- **Planos simples** e os objectivos e as ordens claras e concisas.	Plano simples

2.4 CONSIDERAÇÕES FINAIS

Em suma, podemos concluir que os Princípios da Guerra tiveram uma evolução ao longo dos tempos, com o objectivo de facilitar a acção de comando e controlo dos chefes militares, auxiliar no planeamento das operações militares, tornando-se em pontos-chave que não podem ser descurados, apesar de consistirem em orientações de âmbito geral aplicáveis a todas as situações.

No final deste capítulo, após ter evidenciado a importância de adoptar na doutrina militar, princípios que facilitam os chefes militares na condução das suas operações militares e apontar quais os princípios da guerra de referência neste estudo de investigação justificando a escolha dos mesmos, está-se em condições de passar à fase seguinte da investigação.

A próxima etapa consiste em demonstrar as evidências da existência de operações de Ciberguerra associadas a um novo domínio, o qual se designa de Ciberespaço, com vista a posteriori verificar se realmente os Princípios da Guerra fixados anteriormente como referencial também podem ser aplicados à Ciberguerra. Apresentam-se no final do próximo capítulo uma definição possível de Ciberguerra, i.e. uma nova tipologia de guerra, e uma definiçao de Ciberespaço, i.e. um novo teatro de operações.

> *"O ciberespaço está aberto à entrada de quem quiser. Quem entrar pode fazê-lo com variadas intenções, das mais razoáveis, passando pelas acções ilícitas, até àquelas que visam impor a sua vontade política a outros actores."* (Santos, 2009 p. 56)

3. DOUTRINAS DA CIBERGUERRA

Este capítulo tem por objectivo apresentar conceitos que demonstrem actualmente a existência de Operações de Ciberguerra e que esta é desenvolvida essencialmente no domínio do Ciberespaço.

Para tal, na secção "*Nova dimensão da Guerra – Ciberespaço*" irá ser feita uma descrição deste novo domínio, apresentando uma definição possível, para um novo espaço, onde possivelmente no futuro se poderão desenvolver operações militares, de forma isolada ou em coordenação com operações militares levadas a cabo em terra, no ar, mar e no espaço e, ainda uma definição de Ciberguerra.

Nas restantes secções, apresentam-se evidências de que a Ciberguerra é já preocupação de alguns Estados (e.g. E.U.A, Reino Unido, Rússia, China, França) e da Organização do Tratado do Atlântico Norte (*OTAN*), com base documentos que provam as iniciativas e soluções até agora tomadas para fazer face a esta nova tipologia de guerra (e.g. a solução tomada pela OTAN, com a criação do seu ciber-comando para a cibersegurança – *Cyber Defence Management Authority* – em Bruxelas de modo a centralizar capacidades operacionais em tempo real de ciberdefesa em toda a aliança).

3.1 NOVA DIMENSÃO DA GUERRA – CIBERESPAÇO

Esta secção tem por objectivo delimitar e definir o âmbito de estudo deste trabalho de investigação aplicada visto que "*o primeiro passo para preparar qualquer campo de batalha é de definir o domínio para o ataque e a manobra*" (Wilkin, et al., 2009 p. 17), apresentando-se uma definição de Ciberespaço e de Ciberguerra.

Com o surgimento da Internet a partir de um projecto criado pelo departamento de defesa do governo dos E.U.A. em 1969, antigamente designada por *ARPANET* (Advanced *Research Projects Administration NETwork*), que inicialmente seria constituída por apenas três computadores, mas que rapidamente se difundiu com a adesão exponencial, exigindo uma separação dessa rede em duas redes menores, de um lado computadores de instituições militares, e do outro lado computadores de instituições não militares, possibilitou

o desenvolvimento de um grande número de actividade que antes era difícil ou mesmo impossível de desenvolver a distância, como por exemplo, o trabalho cooperativo à distância, o ensino à distância, a medicina à distância, as compras à distância e até mesmo actividades militares, como o caso de operações de Ciberguerra (Lemos, 1998).

A Internet na sua origem não foi desenhada com a preocupação de proporcionar segurança, e muito pouco tem sido o incentivo dado aos programadores de software de tornar a segurança uma prioridade, onde em muitos dos casos o software produzido é destinado ao consumo e/ou utilização em pequenas empresas (Rohozinski, 2009), tornando os sistemas militares mais vulnerável a ataques com o uso de software comercial (*COTS*) (RC-OP, 2005).

Com a proliferação dos sistemas informáticos nos governos, empresas e organizações civis, onde em muitos casos e principalmente nos países em desenvolvimento existe a falta de recursos e mão-de-obra qualificada, os computadores normalmente estão equipados de software pirata, que por sua vez os seus utilizadores são pessoas com pouca experiência ao invés de contratarem especialistas na área. Face a isto, os Cyber-espiões encontraram uma vantagem enorme para conduzir as suas acções de exploração e ataques a redes de computadores (*CNE* e *CNA*), decorrente das vulnerabilidades[8] encontradas (Rohozinski, 2009).

Surge então em 1984 uma nova dimensão denominada de Ciberespaço, "*conceito tornado popular pelo escritor de ficção William Gibson, no seu livro Neuromancer*" (Lemos, 1998 p. 2), visto cada vez mais como um potencial, e "*verdadeiro campo de batalha digital*" (Santos, et al., 2008 p. 100), por onde circula informação[9] considerada como "*elemento estratégico e táctico valioso, quer no plano do ofensor, quer no do defensor*" (Santos, et al., 2008 p. 100), na qual os ataques às redes, aos servidores, computadores, software e informação são realidades que geram grandes fluxos económicos e financeiros, que nas mãos erradas poderá ter consequências, produzindo danos enormes e afectar o normal funcionamento das actividades de um País.

Várias são as definições encontradas para o conceito de Ciberespaço, no entanto identificam-se e apresentam-se de seguida as que são consideradas mais esclarecedoras para o objectivo do estudo.

No ponto de vista dos E.U.A. e na sua doutrina militar, o aumento significativo do uso dos sistemas de informação para o apoio das operações militares aumentou

[8] "*Característica física ou atributo operacional que torna uma entidade aberta à exploração ou susceptíveis a determinado perigo."* (USDHS, 2009 p. 112)

[9] *"Informação é um recurso criado a partir de duas coisas: fenómenos (dados) que são observados, mais as instruções (sistemas), necessários para analisar e interpretar os dados para lhe dar significado. O valor da informação é reforçado pela tecnologia, tais como redes e bancos de dados de computador, que permite aos militares (1) criar um nível superior de consciência comum, (2) sincronizar melhor o comando, controle e informação, e (3) traduzir a superioridade da informação em poder de combate."* (Clay, 2001 p. 2)

significativamente a dimensão do Ciberespaço como campo de batalha (JP 2-01.3, 2000), levando a definir Ciberespaço no dicionário de termos militares, como "*um domínio global dentro do ambiente de informação consistindo em redes inter-dependentes de infra-estruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores, integrando processadores e controladores.*" (JP 1-02, 2009 p. 139)

Outra definição descrita nas directivas NSPD-54[10]/HSPD-23[11], de 8 de Janeiro de 2008 e 5 de Junho de 2008 respectivamente, da administração *George W. Bush*, refere que o Ciberespaço é o conjunto de "*redes inter-dependentes de infra-estruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores, integrando processadores e controladores em indústrias críticas. O uso comum do termo também se refere ao ambiente virtual de informação e interacções entre pessoas.*" (Casa Branca, 2009 p. 1)

No Reino Unido a estratégia de cibersegurança do centro de operações de cibersegurança (*OCS*) define que o "*Ciberespaço engloba todas a formas de rede, actividades digitais; este inclui o conteúdo e as acções conduzidas através das redes digitais.*" (OCS, 2009 p. 7)

Em França, no Livro Branco de Defesa e Segurança Nacional, afirma-se que este novo domínio surgiu como um "*novo campo de acção, dentro do qual já se desenrolam operações militares*" (Le Livre Banc, 2008 p. 53), constituído por uma série de redes, diferentes do espaço físico, sem fronteiras, evolutivo, anónimo e onde a identificação de um agressor é muito delicado, sendo que uma definição possível para este novo domínio encontra-se no dicionário de referência da língua francesa *Petit Robert*, como sendo o "*espaço de comunicações criado pela interconexão mundial de computadores"* (Petit Robert, 2010)

Uma outra definição, é apresentada por Manuel Lemos no seu livro, como sendo "*um espaço imaginário onde a mente humana se funde com a máquina (mundo cibernético)*" (1998 p. 2).

Por último, apresenta-se uma definição de Ciberespaço do General Loureiro dos Santos, resultado da entrevista realizada, que define este espaço como sendo "*o espaço virtual, gerado pelos elementos tecnológicos dos computadores, toda essa área da informática, onde se efectuam interacções entre as pessoas, organizações, entre países, de toda a natureza, interacções económicas, sociais, politicas, espaço virtual, sustentado, apoiado, gerado por tecnologia que nos permite fazer isso*" (2010).

[10] NSPDs – São directrizes que são utilizadas para promulgar as decisões presidenciais sobre questões de segurança nacional
[11] HSPDs – Directivas que regem a política de segurança interna dos E.U.A.

De todas as definições apresentadas de Ciberespaço, podemos concluir que todas elas andam à volta do mesmo conceito, sendo que, decidiu-se criar a seguinte definição de Ciberespaço, que será adoptada no estudo:

Definição de Ciberespaço

É um ambiente virtual, suportado através de uma rede mundial de computadores interligados pela infra-estrutura de comunicações, no qual se realizam interacções entre pessoas ou agentes de software, permitindo uma comunicação de muitos para muitos e com o objectivo principal de partilhar informação.

O Ciberespaço tornou-se essencial no funcionamento da vida social, sustentando e controlando grande parte das infra-estruturas críticas.

A titulo de exemplo e para uma consulta mais pormenorizada encontra-se em Anexo C uma lista indicativa de sectores (Sector da energia, Sector da informação, comunicações e tecnologias, Sector da água, Sector da alimentação, Sector da saúde, Sector da economia, Sector público, jurídico e de segurança, Sector da administração civil, Sector dos transportes, Sector da indústria química e nuclear, Sector do espaço e investigação) e respectivos produtos e serviços considerados como Infra-estruturas Críticas que "*podem ser danificadas, destruídas ou perturbadas por actos deliberados de terrorismo, catástrofes naturais, negligência, acidentes, actos de pirataria informática, actividades criminosas e comportamentos mal intencionados*" (Livro Verde, 2005 p. 2) (por exemplo, distribuição de electricidade, gás e petróleo, Internet, controlo da qualidade da água, pagamento de serviços, serviços de emergência, forças armadas, tráfego aéreo, assistência medica e hospitalar, comunicações rádio e navegação…), retirado do Livro Verde relativo a um Programa Europeu de Protecção das Infra-estruturas Críticas, apresentado pela comissão, (COM(2005) 576final) e datado de 17 de Novembro de 2005, com o intuito, de mostrar que hoje e caminhando a passos largos para um futuro em que praticamente tudo estará ligado ao Ciberespaço e sujeito a ameaças. (Livro Verde, 2005)

Neste amplo espaço virtual "*podem ser levadas a cabo operações de combate de grande intensidade que visam coagir adversários a ter o comportamento que nos interessa, interceptando, controlando e/ou destruindo os nós onde as redes informáticas se apoiam, ou simplesmente alterando a semântica associada à informação*" (Santos, 2009 p. 302).

Com as nações cada vez mais dependentes do Ciberespaço, onde a informação está interligada digitalmente, onde cada vez mais empresas optam pelo uso da Internet como meio principal de comunicação, emerge um possível e novo tipo de guerra a qual designamos de Ciberguerra, onde a aquisição e a gestão de informação é uma das suas

principais características, sendo crucial proteger as infra-estruturas críticas (IC)[12] das ameaças que surgem no Ciberespaço. Do ponto de vista do Exmo. General Loureiro dos Santos, as operações de Ciberguerra "*podem ser executadas isoladamente de quaisquer outras, para obterem objectivos próprios, paralisando ou destruindo redes de apoio de sistemas de vida e/ou sistemas de combates dos adversários. Mas também podem ser conduzidas em coordenação ou em apoio de acções noutros domínios, por exemplo com operações militares, como aconteceu durante a crise russo-estoniana de Maio de 2007 (tensão provocada pela deslocação do monumento ao soldado soviético, de uma praça pública para o cemitério) e na guerra dos cinco dias entre a Rússia e a Geórgia de Agosto de 2008. Ou ainda em coordenação e no âmbito de operações económicas, financeiras, mediáticas, etc.*" (2009 p. 304).

Para o conceito de Ciberguerra, também são identificadas definições que apresentam-se de seguida, com o objectivo de tornar mais esclarecedor do que se trata.

Na Quinquagésima - quinta sessão plenária da Assembleia Europeia de Segurança e de Defesa, realizada entre 2 e 4 de Dezembro de 2008, uma definição de Ciberguerra foi apresentada por *Christopher Chope* e *Tarmo Kõuts*, como uma guerra com "*recurso a computadores e Internet para levar a cabo uma guerra no Ciberespaço (denominada também de guerra cibernética) "* (Chope, et al., 2008 p. 28).

Em França, no dicionário de referência *Petit Robert*, Ciberguerra é descrita como toda a "*agressão electrónica contra os sistemas informáticos perpetrados com o objectivo de utilizar como meio de propaganda e de desinformação ou de paralisar as actividades vitais de um País*" (2010)

Estas definições, tendo por suporte a interpretação de documentos diversos, não se adequam de forma rigorosa ao termo Ciberguerra porque se corre o risco de estar a generalizar um conceito, que deverá ser diferenciado de actos de Cibercrime e Ciberterrorismo que também podem ser desenvolvidos no Ciberespaço. Para tal complementam-se as definições anteriores, apresentando a seguir, outras definições, que de acordo com a perspectiva apresentada é mais correcta para esta nova tipologia de guerra, por se restringir mais ao âmbito militar. Segundo, *Laurent Murawiec* (1999 p. 3), ex-consultor do Ministério de Defesa em França e especialista em assuntos militares e guerra da informação, a Ciberguerra é o "*conjunto de actividades de ordem e importância militar que têm lugar no seio desta nova dimensão*", o Ciberespaço.

Por último, apresenta-se uma definição de Ciberguerra do General Loureiro dos Santos, resultado da entrevista realizada, que define a Ciberguerra como sendo "*o conjunto*

[12] *"Uma rede de sistemas independentes feitos pelo homem, incluindo componentes físicas e lógicas (*hard *e* soft*) que funcionam em colaboração e em sinergia para produzir um fluxo contínuo de bens e serviços essenciais" (PCCIP1997).*

de acções que é possível fazer no Ciberespaço, para obrigar um actor político a agir da forma que o actor que desencadeia essas acções pretende que haja" (2010).

A definição de Ciberguerra adoptada neste trabalho, surgiu da análise efectuada com base nas definições apresentadas anteriormente:

Definição de Ciberguerra

Acto de Guerra entre grupos políticos, no Ciberespaço, destinado a submeter o adversário à sua vontade, visando determinado fim politico.

Face a esta dependência das TIC no mundo actual, onde cada vez mais vivemos num Mundo interligado, será requisito cada vez maior, obter uma capacidade tecnológica no domínio da segurança, pelo que, uma superioridade nesta área, poderá ser decisivo para o sucesso de qualquer campanha militar, "*exigindo estruturas próprias de ciberdefesa e cibersegurança, capazes de deter os ataques de adversários e levar a cabo ataques cibernéticos preventivos como manobras de antecipação e/ou resposta num conflito armado ou não.*" (Santos, 2009 p. 303)

É com esta preocupação que os diversos Estados e Organizações Internacionais têm investido nesta área, onde iremos referir algumas das medidas tomadas por parte delas, com o objectivo de tornar claro que, nos dias de hoje, Estados e Organizações Internacionais (e.g. E.U.A., Rússia, China, França e *OTAN*) têm manifestado preocupação quanto à possibilidade de ocorrerem Ciberguerras no novo domínio que atrás designámos de Ciberespaço.

3.2 SOLUÇÃO DOS EUA

Segundo um relatório do *GAO* (*Government Accountability Office*) dos Estados Unidos, "*vários são os países que estão a trabalhar agressivamente para desenvolver uma doutrina de Guerra da Informação. Estas capacidades permitem que uma única entidade consiga ter impacto significativo e grave interferindo nos abastecimentos, comunicações, e infra-estruturas económicas que suportem o poder militar*." (GAO, 2004 p. 4)

A Ciberguerra segundo a doutrina americana, pode ser conduzida contra qualquer um dos meios que tenha acesso ao Ciberespaço, podendo incluir *Hardware*, Redes, *Software*, Dados, Procedimentos e operadoras que fornecem acesso à internet, visto existir relativa vulnerabilidade em cada um desses componentes. Essa vulnerabilidade existe por várias razões, como por exemplo a falta de treino adequado do utilizador, más instalações físicas combinado ainda com o nível de sofisticação do inimigo para levar a cabo ataques a Redes de Computadores (*CNA*) (JP 2-01.3, 2000).

No seguimento dos vários ataques que os E.U.A têm vindo a ser alvo, surgiu uma preocupação crescente, que levou à criação em 2007 um "*Cyber Command*", atribuindo como missão à USAF (U.S. Air Force) "*voar e lutar no ar, no espaço e ciberespaço*" (Clay, 2007 p. 7). A criação deste "*Cyber Command*" e a atribuição de uma nova missão, revela o surgimento de uma nova forma de fazer a guerra (i.e. a Ciberguerra), e a existência de uma preocupação por parte dos E.U.A com a defesa e o controlo do Ciberespaço.

Em 2009, no dia 23 de Junho foi criado uma componente de ciberdefesa dentro do Comando Estratégico dos E.U.A. (*USSTRATCOM*), o *Cyber Command* dos Estados Unidos (*USCYBERCOM*) sob o comando do General Keith B. Alexander. Este *Cyber Command* entrou em actividade a 21 de Maio de 2010 e prevê-se com prontidão operacional em Outubro deste ano, tendo como missão planear, coordenar, sincronizar e conduzir operações de defesa das redes de informação do departamento de defesa e preparar para, quando solicitado conduzir operações no Ciberespaço a fim de permitir acções em todos os domínios, certificando-se que os E.U.A. e seus aliados consigam ter liberdade de acção no Ciberespaço e negar o mesmo aos adversários (Alexander, 2010).

As acções militares no Ciberespaço englobam as *CNO* e *EW*, ou seja, no que respeita às *CNO*, as acções militares desenvolvidas são principalmente assegurar a protecção das suas infra-estruturas críticas, redes e defenderem-se de possíveis ataques maliciosos a partir da Internet, e no que respeita à *EW*, são todas as acções que se podem desenvolver no espectro electromagnético (Clay, 2007).

3.3 SOLUÇÃO DA RÚSSIA

Os Russos acreditam que a probabilidade de ocorrer uma Ciberguerra é uma das mais perigosas ameaças a seguir às armas nucleares, sendo que se reservam o direito de usar armas nucleares contra os meios, forças e Estados que ataquem no Ciberespaço infra-estruturas críticas da Rússia. Defendem ainda que as actividades levadas a cabo com a guerra da informação têm como objectivo competir e manter vantagens de informação em relação ao adversário (Clay, 2001).

A 9 de Setembro de 2000, o presidente, *Vladimir Putin*, aprovou a doutrina de segurança da informação da Federação Russa onde está explícito oficialmente a totalidade das metas, objectivos, princípios e directrizes básicas para garantir a segurança da informação na Federação Russa (DISRF, 2000), sendo que a nova doutrina "*representa uma tentativa parcial por parte da Rússia para lidar com as ameaças cibernéticas de que poderá ser alvo por parte de fontes nacionais ou estrangeiras*" (Clay, 2001 p. 11).

3.4 SOLUÇÃO DA CHINA

O Governo da República Popular da China (*PRC*) tem vindo a desenvolver desde 1990 até aos dias de hoje, a sua doutrina do Ciberespaço e capacidades defensivas e ofensivas, como parte do plano de modernização do exército, atribuindo ao Ciberespaço um dos seus principais pilares da estratégia de segurança nacional. Desenvolve activamente uma capacidade operacional no Ciberespaço e identifica correctamente como alcançar a paridade estratégica, senão mesmo uma superioridade perante os Estados Unidos da América e seus aliados na guerra do Comando e Controlo (C2), capaz de coordenar operações militares em terra, no ar, no mar, no espaço, e em todo o espectro electromagnético[13], tanto em tempo de paz como em períodos de conflito (Rohozinski, 2009).

Apesar de ainda não ter publicado formalmente uma estratégia de *CNO* no seu principal corpo doutrinário (*CMC*[14], *AMS*[15]), desenvolveu uma estratégia da Guerra da Informação (*IW*) denominada "*Integrated Network Electronic Warfare*" (*INEW*) que é caracterizada pelo emprego combinado de Guerra Electrónica (*EW*) e Operações de Redes de Computadores (*CNO*) contra os sistemas adversários de comando, controle, comunicações, computadores, inteligência, vigilância e reconhecimento (*C4ISR*) nas fases iniciais de um conflito, devendo marcar o início de uma campanha militar, permitindo assim o sucesso operacional global. Esta estratégia, no que respeita à Guerra Electrónica (*EW*) tem por finalidade enganar e suprimir a aquisição de informação por parte do inimigo, bem como as capacidades de processamento e disseminação da informação; e os Ataques a Redes de Computadores (*CNA*) destinando-se a sabotar o processamento de informação de modo a atacar as percepções do Inimigo e negar ao inimigo o acesso a informações essenciais para continuar as operações de combate, utilizando técnicas como a interferência electrónica, fraude electrónica e supressão para interromper a aquisição de informação, lançamento de vírus ou ataques de hackers para sabotar o processamento de informação (Krekel, 2009).

Ou seja, num possível conflito com os Estados Unidos, a China pretende utilizar as suas capacidades de *CNO* para atacar alvos pré-planeados como por exemplo a *NIPRNET*[16] e *CONUS*[17], com o objectivo de atrasar a colocação de forças dos E.U.A. no terreno e influenciar a eficácia de combate das tropas já no teatro de operações (Krekel, 2009).

[13] A China considera muito importante o controlo do espaço para alcançar uma verdadeira posição dominante e hegemonia no controlo da informação, e muitos especialistas consideram a guerra espacial como um subconjunto da guerra da informação. A China, para tal, tem vindo a desenvolver armas antiespaciais de alta velocidade para atingirem directamente satélites, ou ainda, armas de energia dirigida (lasers).
[14] **CMC** – Central Military Commission
[15] **AMS** – Academy of Military Sciences
[16] Military's Non-classified Internet Protocol Router Network
[17] Unclassified DoD and civilian contractor logistics networks in the continental US

Os defensores da estratégia *INEW* especificam ainda que o objectivo é atacar alvos específicos por onde passam os dados de comando e controlo, e ainda a informação respeitante à logística que apoiem os objectivos estratégicos de uma campanha, de modo a influenciar na tomada de decisão, as operações e moral do inimigo (Krekel, 2009).

Em segundo plano, e não menos importante, temos a comunidade chinesa de *hackers,* ou seja, o hacker é o "*indivíduo que possui um conhecimento aprofundado dos computadores, sistemas electrónicos e Internet, que ele utiliza para contornar os mecanismos de segurança de um determinado sistema e explorar as suas funções e limitações*" (Chope, et al., 2008 p. 30), que pratica *hacktivism* i.e. *"Ataques a computadores com a intenção de comunicar uma mensagem social ou política, ou apoiar a posição de um grupo político ou ideológico. Actividades de hacktivism incluem roubo de dados, desfiguração de sítios, negação de serviços, redireccionamentos e outros"* (Krekel, 2009 p. 78). Esta comunidade desenvolveu um conhecimento técnico profundo nesta área, ganhando reconhecimento mundial pelos seus pares, na medida em que movidos politicamente e ideologicamente de um fervor nacionalista mostraram disponibilidade em participar em grande escala em ataques de negação de serviços (*DoS* e *DDoS*), na destruição de dados, e nas invasões a redes estrangeiras, entre outros. (Krekel, 2009)

Esta comunidade de *hacktivistas* revela-se importante na nova estratégia militar da China para o ciberespaço, pois permite integrar indivíduos[18] altamente qualificados ou pequenos grupos da comunidade hacker nos seus ataques como complemento a uma campanha militar de *CNO.* Contudo, a China parece ainda estar relutante quanto a esta possível opção pois poderá ferir alguns dos princípios como a Unidade de Comando como oportunamente referirei. (Krekel, 2009)

Em resumo, o papel fundamental da estratégia *INEW* é criar janelas de oportunidade, perturbando a capacidade de tomada de decisão do inimigo, para que outras forças possam operar correndo risco mínimos de possíveis contra-ataques, explorando assim períodos de "cegueira", "surdez" ou "paralisia" criadas pelos ataques de informação. (Krekel, 2009)

3.5 SOLUÇÃO DA FRANÇA

Podemos verificar no caso da França, com base num relatório de *Cyberwarfare* de 2001, dos serviços de pesquisa para o Congresso (CRS) da Federação de Cientistas Americanos (FAS), e no Livro Branco de Defesa e Segurança Nacional de 2008 publicado

[18] Um exemplo, são os líderes de grupos hackers, capazes de unir em massa muitos outros e disseminar ferramentas de ataque a partir dos seus sítios assegurando uma participação em massa, contra alvos que tenham insultado o seu Pais.

em França, que tem havido uma mudança de mentalidade face ao surgimento da Ciberguerra.

De acordo com o relatório mencionado constata-se que a França divide a Ciberguerra em dois campos (Militar e Económico/Civil), sendo que atribui maior importância e grande aplicabilidade da Ciberguerra no campo económico/civil, desprezando e duvidando de uma futura aplicação da Ciberguerra no campo militar. (Hildreth, 2001)

Contudo, em 2008, no Livro Branco de Defesa e Segurança Nacional publicado em França, está bem presente a preocupação deste Estado quanto à Ciberguerra. Onde define que o Ciberespaço, como o conjunto de redes, radicalmente diferente do meio físico, sem fronteiras, em constante evolução, anónimo, que aparece como um novo campo de acção dentro do qual já ocorrem operações militares, sendo que, face a esta nova dimensão a França diz ser crucial desenvolver uma capacidade de luta neste novo espaço, bem como regras de empenhamento apropriadas, tendo em conta as considerações jurídicas aliadas a este espaço que terão de ser elaboradas (2008).

Face a isto, tem vindo a desenvolver estratégias coma finalidade de atingir dois objectivos: o primeiro, a criação do conceito de ciberdefesa, organizada em profundidade e em coordenação com a nova agência de segurança de sistemas de informação (*SGDSN*), com a missão de detectar ataques, prevenir ameaças, aconselhar e assistir, comunicar e sensibilizar; e o segundo, o estabelecimento de uma capacidade ofensiva de Ciberguerra (Le Livre Banc, 2008).

3.6 SOLUÇÃO DA *OTAN*

Na *OTAN* há muito que se está familiarizando com a defesa contra a guerra da informação e a guerra electrónica, desenvolvendo esforços significativos para conduzir operações de guerra centrada em rede e respectivas capacidades em rede, sendo que em 2002, na cimeira de Praga, dirigentes da *OTAN* decidiram reforçar as defesas contra ataques cibernéticos, o que resultou num conjunto de decisões, das quais se salienta o programa de ciber-defesa, envolvendo vários órgãos (*OTAN Communication and Information Systems Services Agency*, *OTAN Information Security Technical Centre*, *OTAN Information Security Operations Centre* e *OTAN Computer Incident Response Capability*) (Cornish, 2009).

Desenvolver dois centros de excelência até ao momento, sendo que uma delas está direccionada para um nível mais operacional, criando o seu ciber-comando para a cibersegurança (*OTAN Cyber Defence Management Authority – CDMA*) em Bruxelas de modo a centralizar capacidades operacionais em tempo real de ciberdefesa em toda a aliança (Hughes, 2009). A segunda organização refere-se a uma plataforma mais intelectual, doutrinária e estratégica projectada e pensada a longo prazo, desenvolvida após os ataques

cibernéticos contra a Estónia em 2007. Preocupados com os problemas da Ciberguerra decidiram acelerar o desenvolvimento do centro de excelência de ciberdefesa do Ciberespaço (em desenvolvimento desde 2004 denominado de *Cooperative Cyber Defence Centre of Excellence*) que ficaria situado na capital da Estónia (*Tallinn*), estabelecido formalmente a 14 de Maio de 2008, a fim de aumentar a capacidade de defesa da *OTAN*. Este centro de excelência recebeu acreditação plena da *OTAN* a 28 de Outubro de 2008, alcançando o status de Organização Militar Internacional. Sendo que a missão atribuída a este centro de excelência é de aumentar a capacidade de cooperação e partilha de informação dentro da *OTAN*, nações pertencentes à *OTAN* e parceiros em ciberdefesa, por força da educação, investigação e desenvolvimento, lições aprendidas e consulta (CCDCOE, 2009).

A *CCDCOE* conta com sete Nações patrocinadoras (Estónia, Alemanha, Itália, Letónia, Lituânia, Eslováquia e Espanha), sendo que em Novembro de 2008 os E.U.A aceitou fazer parte desta organização e a Turquia anunciou a intenção de fazer o mesmo. (Cornish, 2009)

3.7 CONSIDERAÇÕES FINAIS

Depois de definidos os conceitos de Ciberespaço e de Ciberguerra e demonstrada a importância que estes conceitos têm vindo a assumir por parte das grandes potências militares, torna-se fácil compreender que estamos perante uma nova forma de fazer a guerra, que certamente terá grande aplicação certamente no futuro, mas com evidências já no presente.

Como tal, assumiremos que o conceito de ciberespaço é um ambiente virtual, suportado através de uma rede mundial de computadores interligados pela infra-estrutura de comunicações, no qual se realizam interacções entre pessoas ou agentes de software, permitindo uma comunicação de muitos para muitos e com o objectivo principal de partilhar informação, onde se efectuam interacções digitais e que o conceito de Ciberguerra é um acto de Guerra entre grupos políticos, no Ciberespaço, destinado a submeter o adversário à sua vontade, visando determinado fim político.

De maneira a objectivar de que forma a Ciberguerra poderá ser aplicada, no próximo capítulo irei apresentar a análise de dois estudos de caso em que está presente de forma clara o conceito de guerra no Ciberespaço e de Ciberguerra, de acordo com o referencial apresentado e definições adoptadas, nos quais procuraremos identificar os princípios da guerra adoptados pelo Exército Português no RC 130-1, referenciados no capítulo 2 (Princípios clássicos da guerra), de modo a responder à questão central: São os Princípios da Guerra clássica aplicáveis à Ciberguerra?

> *"O método do estudo de caso … não é uma técnica específica. É um meio de organizar dados sociais preservando o carácter unitário do objecto social estudado."* (Goode, et al., 1969 p. 422)

4. ESTUDO DE CASOS

Este capítulo tem por objectivo abordar dois estudos de caso, que de acordo com a revisão de literatura realizada, entrevista efectuada ao General Loureiro dos Santos e os conceitos de Ciberguerra apresentados, se podem classificar de Ciberguerra. Para tal, o capítulo está dividido em quatro secções.

Na primeira secção deste capítulo, temos por objectivo ilustrar a importância que cada vez mais é dada ao estudo de casos na área das ciências sociais e humanas, bem como a aplicação destes na elaboração de trabalhos de investigação.

Na segunda e terceira secção deste capítulo, apresentam-se os estudos de caso, de onde se procura através de uma interpretação com base nos documentos referidos, extrair os princípios da guerra presentes nesses mesmos estudos de caso. Com base no Quadro 4 (p. 18) e respectivos indicadores procura-se chegar às principais conclusões e responder à questão central do trabalho de investigação.

Na última secção é feito um resumo dos dois estudos de caso, sintetizando numa tabela os princípios da guerra mais relevantes encontrados nestes mesmos estudos de caso, que segundo a interpretação realizada, justificam a sua utilização na Ciberguerra.

4.1 INTRODUÇÃO – IMPORTÂNCIA DO ESTUDO DE CASOS

"*O método de estudo de casos, como método de aprendizagem e investigação, tem sido amplamente utilizado por estudantes de licenciatura, mestrado e doutoramento para as suas teses, ou dissertações finais de curso*" (Ferreira, et al., 2009 p. 91).

Ao recorrer a este método, de estudo de casos, está-se exposto a potenciais críticas como por exemplo à falta de objectividade e rigor. A subjectividade está presente, visto o estudo de casos ser o resultado de uma interpretação de dados qualitativos. Contudo, um ponto positivo no uso dos estudo de casos é o facto de permitir tomar decisões e procurar evidências (informações especificas na análise documental e entrevista efectuada) que as fundamentem, tendo proporcionado flexibilidade, mas simultaneamente atribuindo responsabilidade de criatividade e inovação, sendo que, o estudo de casos "*é um método válido e valioso de pesquisa, com características distintas das análises empíricas em*

amostras alargadas, que os tornam ideais para certos tipos de pesquisa" (Ferreira, et al., 2009 p. 101).

Após se ter formulado a questão central e questões derivadas, procurou-se seleccionar cuidadosamente os casos a estudar de forma a identificar os princípios da guerra mais relevantes na Ciberguerra e responder às questões formuladas.

A escolha destes e não de outros, é resultado da limitação no acesso a documentos militares classificados e no caso da Indústria pela inexistência da divulgação de incidentes de segurança.

4.2 ESTUDO DE CASO DA ESTÓNIA

Em Abril e Maio de 2007, após uma série de ataques cibernéticos contra os sistemas informáticos do Governo da Estónia, a *OTAN* e os Estados Unidos enviaram especialistas na área da segurança para ajudar este Estado a recuperar desses mesmos ataques, bem como apurar as fontes desses ataques e analisar os métodos utilizados (Clay, 2008).

Este incidente contou com alguma controvérsia, na medida em que foi, e ainda é difícil apurar as responsabilidades destes ataques, dificultando a tarefa de definir se é um mero crime, ou seja, Cibercrime, se é Ciberterrorismo, ou se é um caso de Ciberguerra.

De início, alguns especialistas na área da segurança suspeitaram da eventual participação de manifestantes políticos que teriam alugado serviços a grupos de criminosos, possivelmente uma rede em grande escala de computadores infectados, chamados de "*botnets*" com o objectivo de destabilizar o Governo da Estónia, sendo que inicialmente o Governo Russo teria sido acusado por autoridades da Estónia pelos ataques cibernéticos, havendo portanto acusações de Ciberguerra (Clay, 2007). Contudo, após algumas investigações, vieram a concluir que os ataques cibernéticos teriam sido apenas o produto raiva espontânea, com fontes de ataques em todo o mundo, não existindo qualquer ligação com o Governo Russo (Clay, 2008).

Apesar de este estudo de caso se situar na indefinição, ou seja, não se tirar conclusões precisas de modo a definir se é caso de Ciberguerra, não o podemos colocar de parte porque, porque a 6 de Março de 2009 surgiram revelações[19] por parte de um deputado Russo (*Sergei Markov*), de que os ataques teriam sido incentivados e coordenados por um dos seus assistentes do qual não podia revelar a sua identidade, e portanto este é um evento que temos de ter em conta como possível modelo de Ciberguerra, estudá-lo de

[19] Revelações em *http://news.softpedia.com/news/Two-Years-Old-Cyber-attack-on-Estonia-Again-in-the-Spotlight-106353.shtml* e *http://www.rferl.org/content/behind_the_estonia_cyberattacks/1505613.html* (consultado a 22 de Julho de 2010 às 15h55)

forma a procurar extrair deste caso os princípios da guerra clássica mais relevantes para a Ciberguerra.

4.2.1 Antecedentes e contexto dos ataques cibernéticos contra a Estónia

A Estónia é um dos países mais pequenos pertencentes à *OTAN*, contudo, em contrapartida é dos mais desenvolvidos a nível das Tecnologias de Informação (*TI*) e dependente do Ciberespaço. Actualmente, na Estónia, em cada 100 habitantes existem 57 utilizadores ligados à Internet, muitos dos serviços podem ser executados via Internet, foi dos primeiros países a proporcionar aos seus habitantes participar nas eleições via Internet, 97% das empresas têm acesso à Internet, mais de 97% das transacções bancárias são feitas via Internet, mais de 10% das facturas são electrónicas, o pagamento e identificação pode ser feita a partir do telefone, declarar impostos, todo o Governo está ligado em rede, e quase 100% das transacções podem ser executadas utilizando a Internet (Tikk, 2008).

Face a todo este desenvolvimento ao nível das *TI* é também dos Países mais vulnerável a ataques a Infra-estruturas críticas da Internet, e portanto alvo de ciberataques (CCDCOE, 2009).

A 27 de Abril de 2007 o País viveu o que muitos consideram como a primeira guerra no ciberespaço. Uma ofensiva foi lançada contra a Estónia, com o objectivo de bloquear sítios oficiais como por exemplo do Primeiro-Ministro, Parlamento, da Presidência da República, destabilizar as operações dos maiores bancos da Estónia, serviços de saúde e tecnologia, e afectaram os sítios de vários jornais diários (TVNET, 2009). Os tipos de ataques lançados são designados de Ataques *DDoS*, ou ainda denominados ataques de Negação de Serviços que segundo a *CERT*[20] são caracterizados por solicitações em massa direccionados para um site ou servidor, fazendo com que ele não suporte as solicitações e fique indisponível, ou seja, impedir que utilizadores legítimos tenham acesso a determinado serviço.[21]

Este conflito decorreu após a remoção de uma estátua de bronze situada na capital da Estónia (*Tallinn*) com destino ao cemitério militar, que suscitou ânimos diferentes na Estónia. Para os estonianos a estátua, era considerada símbolo de terror, opressão e lembrava um passado mau (período entre 1949-1959) que marcou o início da ocupação ilegal por parte dos soviéticos e de um regime de terror que executou certa de 19.000 estonianos. Para a população Russa que representa cerca de 25% da população residente na Estónia, a

[20] **CERT** (Computer Emergency Response Team) - Serviço de resposta a incidentes de segurança informática da Universidade de *Carnegie Mellon* em *Pittsburgh*, Pensilvânia.
[21] Larry Rogers, "*What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?"*,em [http://www.cert.org/homeusers/ddos.html no dia 22 de Fevereiro de 2010 às 14h14min]

estátua do soldado de bronze representava e assinalava o triunfo soviético sobre as tropas nazis.

A 15 de Fevereiro de 2007, o Parlamento Estoniano aprovou a lei para desmantelar o Soldado de Bronze num prazo de 30 dias, situada na capital e construída há mais de 50 anos, faltando apenas a assinatura do Presidente da República da Estónia para avançar com o desmantelamento da estátua.

Vários foram os países[22] que precaveram a Estónia de uma eventual retaliação por parte da Rússia, aconselhando a Estónia a não semear actos de discórdia e criar problemas desnecessários. Mas a Estónia acabou por ignorar os pedidos e seguiu com o desmantelamento do Soldado de Bronze a 26 de Abril de 2007.

Tomada a decisão e após iniciar a remoção da estátua do local, a população estoniana de descendência Russa saiu à rua organizando protestos e vandalizaram lojas. Outra forma de protesto mais silenciosa foi desencadeada por Hackers e teve início a 27 de Abril de 2007, tendo provocado danos enormes na economia.

Os ataques cibernéticos fizeram-se sentir num período de 1 mês (27 de Abril a 18 de Maio de 2007) (Tikk, 2008) e foram conduzidos em cinco fases como forma de protesto com o objectivo de paralisar a economia da Estónia e impedir que a disseminação de informação se fizesse para o exterior.

Numa primeira fase (27 de Abril a 30 de Abril) fizeram-se sentir pequenos ataques DoS, envio de correio electrónico com spam, servidores e portais de informação ficaram off-line, sítios ficaram sobrecarregados 400 vezes mais que o normal com excesso de visitas resultando que muitos deles ficassem off-line no início do conflito.

Numa segunda fase (4 de Maio) deu-se o primeiro ataque DDoS em grande escala.

Numa terceira fase (9 de Maio a 11 de Maio) verificou-se ataques ao maior banco da Estónia (Hansapank) que ficou off-line cerca de hora e meia e, novamente, outro ataque DDoS em grande escala.

Numa quarta fase (15 de Maio) foram efectuados ataques ao segundo maior banco da Estónia (SEB bank) que acabou por ficar off-line durante cerca de uma hora.

Numa quinta fase (18 de Maio) deu-se o último ataque DDoS.

4.2.2 Análise dos Princípios da Guerra Clássica à luz do Estudo de Caso da Estónia

Após ter inteirado o leitor do caso que pretendemos estudar, chegou o momento de analisar cada princípio da guerra *per si*, de forma a tentar encontrar evidências de que os

[22] Por exemplo o Presidente Waldus Adamcus, da Lituânia disse: "*Deveríamos deixar o Soldado de Bronze onde está, e seguir em frente. Devemos deixar de olhar para trás, criando problemas desnecessários.*" (Pravda, 2007 p. 1)

princípios da guerra clássica continuam actuais e por sua vez, relevantes para uma acção de Ciberguerra no Ciberespaço.

1) **Princípio do Objectivo** – Podendo haver operações militares no Ciberespaço, estas devem contribuir necessariamente para a obtenção do objectivo último da guerra que é o aniquilamento das forças armadas do adversário e da sua vontade de combater. Os objectivos traçados numa operação de Ciberguerra serão forçosamente diferentes dos objectivos traçados numa operação Terrestre, área, marítima, por via dos meios utilizados e das respectivas características da área de operações. Nestes ataques Cibernéticos dirigidos contra a Estónia podemos verificar que os objectivos foram as *"infra-estruturas críticas da Internet*" (Hughes, 2009 p. 8) com o objectivo de bloquear sítios oficiais como por exemplo do Primeiro-Ministro, Parlamento, da Presidência da República, destabilizar as operações dos maiores bancos da Estónia, serviços de saúde e tecnologia, e afectaram os sítios de vários jornais diários (TVNET, 2009).
2) **Princípio da Ofensiva** – Podemos verificar este princípio da guerra neste caso na medida em que, lançando uma ofensiva Cibernética contra as infra-estruturas críticas da Internet da Estónia, este Estado teve dificuldade em recuperar ("*os ataques duraram semanas, ao invés de horas ou dias*" (Clay, 2008 p. 7)), sendo que foram explorados com sucesso os pontos fracos da Estónia ("*grande dependência da Estónia em relação às Tecnologias da Informação*" (Clay, 2008 p. 7)), remetendo a Estónia a uma posição defensiva, na medida em que a OTAN e os Estados Unidos enviaram peritos na área da segurança para ajudar a Estónia a recuperar dos ataques, analisar os métodos utilizados pelo inimigo e tentar determinar as fontes dos ataques.
3) **Princípio da Massa** – Este princípio facilmente se pode verificar neste caso de Ciberguerra, visto que para conseguir destabilizar o normal desenrolar das operações, por exemplo as operações dos maiores bancos da Estónia via Internet, lançaram-se ataques de negação de serviços (ataques DDoS) que consiste em "*bloquear ou esgotar os recursos disponíveis de uma máquina impedindo que os outros lhe acedam*" (Santos, et al., 2008 p. 169). Estes ataques normalmente têm início a partir de um computador (denominado de computador "*Master*") que tem sob seu comando milhares de outros computadores infectados espalhados por todo o Mundo (denominados de computadores "*Zombies*") que são preparados para lançarem ataques à ordem do computador "*Mestre*" contra um determinado recurso de um servidor com o objectivo deste não conseguir dar resposta a todos os pedidos, obrigando o servidor a reiniciar ou mesmo a ficar indisponível durante algum tempo.

4) **Princípio da Economia de Forças** – Este é um princípio da guerra que no caso da Estónia não conseguimos tirar conclusões precisas, isto porque, não se sabe ao certo se os ataques foram resultado de raiva espontânea de atacantes com o objectivo de se mostrarem indignados com a mudança da estátua para o cemitério militar (Clay, 2008), ou se foi algo coordenado e incentivado pelo Governo Russo. Ou seja, das informações que dispomos podemos concluir que não houve qualquer planeamento com vista ao emprego judicioso dos meios (conjunto de botnets) em locais e momentos adequados.
5) **Princípio da Manobra** – Este princípio da guerra verifica-se, pois quando se pretende dispor uma força de forma tal que o inimigo fique colocado numa situação desvantajosa, no caso da Ciberguerra e neste estudo de caso da Estónia, podemos facilmente verificar que através dos milhares de computadores infectados espalhados pelo mundo (rede de Botnets), conseguiu-se com sucesso saturar os servidores das infra-estruturas críticas da Internet da Estónia. Contribuindo para conservar a liberdade de acção, para manter a iniciativa e explorar os resultados do combate (paralisando a economia da Estónia e impedir que a disseminação de informação se fizesse para o exterior).
6) **Princípio da Unidade de Comando** – Tal como o princípio da Economia de Forças, este é um princípio da guerra que no caso da Estónia não se podem tirar conclusões precisas. Contudo, no nosso ponto de vista, este é um princípio da guerra que se revela pouco importante na Ciberguerra. Achamos necessário o desenvolvimento de ferramentas importantes, como por exemplo, no caso da OTAN, com o desenvolvimento do seu ciber-comando e de plataformas intelectuais, doutrinárias e estratégicas como foi referido no capítulo anterior, de forma a coordenar operações de Ciberguerra, contudo, achamos que o princípio da unidade de comando se iria dispersar por vários pontos de coordenação (como por exemplo auxiliar-se de Hacktivistas) para desenvolver Ciberguerras. Deverá ser estabelecido, por exemplo ligações com comunidades de Hackers que irão apoiar o desenvolvimento de ferramentas de ataque antes e durante as operações de Ciberguerra, garantindo assim a participação em massa, contudo, devemos ter em atenção que uma vez iniciado os ataques por parte dos hacktivistas, estes poderiam tomar um rumo indesejado, seguindo os seus próprios impulsos e quebrar com o princípio da unidade de comando, interferindo negativamente com as operações de Ciberguerra em curso.
7) **Princípio da Segurança** – Podemos dizer que este princípio da guerra verificou-se neste caso de Ciberguerra da Estónia, isto porque até agora apenas conseguiram condenar uma pessoa. Os autores destes ataques conseguiram garantir o seu anonimato impossibilitando a Estónia de obter informações precisas dos autores

da origem dos ataques. Este princípio da guerra foi necessário para o sucesso de todos os outros princípios na medida em que para se alcançar por exemplo o princípio da liberdade de acção, conseguiu-se negar ao inimigo a possibilidade dele obter informações sobre os ataques que estavam planeados, alcançando os objectivos pretendidos, ocultando informações sobre si próprios.

8) **Princípio da Surpresa** – Este princípio da guerra verifica-se na medida em que os ataques dirigidos contra a Estónia foram efectuados de tal forma que a Estónia não estava preparada para responder de forma eficaz, colocando a Estónia em posição desvantajosa na medida em que a "*incerteza de não conhecer o iniciador destes ataques afecta também a decisão de decidir quem será alvo de retaliação*" (Clay, 2008 p. 8). Sendo que podemos facilmente concluir que estes ataques cibernéticos podem proporcionar manobra, estimulando a ofensiva e segurança ao mesmo tempo.
9) **Princípio da Simplicidade** – Na condução destes ataques, não é exigido grande complexidade, na medida em que, os Botnets (refere-se ao conjunto de computadores infectados com códigos maliciosos, designados de computadores "*Zombis*" e controlados remotamente através de comandos enviados através da Internet) tornaram-se uma ferramenta importante para levar a cabo este tipo de operações no Ciberespaço, porque podem ser facilmente concebidos e de forma eficaz para "*interromper sistemas de computadores de diferentes formas, e porque um utilizador mal-intencionado, sem possuir grandes capacidades técnicas, pode dar inicio a esses efeitos negativos no Ciberespaço*" (Clay, 2008 p. 5), contribuindo para a eficácia e o sucesso das operações. Há ainda indicações de que estes ataques teriam sido planeados e disponibilizados na Internet para qualquer cidadão que entendesse entrar nesse movimento de revolta e atacar as infra-estruturas críticas da Internet da Estónia (Clay, 2008).

4.2.3 Considerações finais do estudo de caso da Estónia

Podemos concluir deste estudo de caso que praticamente todos os Princípios da Guerra se revelaram importantes para uma acção de Ciberguerra à excepção dos Princípio da Economia de Forças e do Princípio da Unidade de Comando, como podemos constatar no Quadro 5. O estudo de caso da Estónia, através de uma análise de conteúdo, possibilita tirar conclusões e verificar que sete dos nove princípios da guerra Clássica se revelam importantes para uma acção de Ciberguerra.

Quadro 5. Princípios da Guerra identificados no estudo de caso da Estónia

Princípios da Guerra Clássica (RC 130-1)	Estudo de caso da Estónia		
	Palavras-Chave	Indicadores (ID – Principio Identificado / ND – Principio não Identificado)	
Objectivo	Objectivo último	- Não nos é possível face à falta de informação quanto aos autores dos ataques concluir se os objectivos traçados seriam estritamente militares, contudo, podemos concluir que se o objectivo era destabilizar as acções de infra-estruturas críticas da Internet da Estónia, podemos considerar que estes objectivos poderiam ser considerados objectivos intermédios para alcançar porventura o objectivo último da guerra.	ID
	Objectivos claros	- Distribuído na Internet listas de alvos acessível a qualquer indivíduo que quisesse participar neste movimento.	
	Objectivos exequíveis	- Os meios existentes (Internet, Software adequado, Lista de alvos) para a característica da área de operações (Ciberespaço) foram adequados para o cumprimento da missão.	
Ofensiva	Pontos fracos do IN	- Foram explorados com sucesso os pontos fracos da Estónia (grande dependência da Estónia em relação às Tecnologias da Informação), remetendo a Estónia a uma posição defensiva.	ID
	Resultados decisivos	- Ao remeter a Estónia para uma posição defensiva alcançou-se o princípio da ofensiva conseguindo-se obter resultados decisivos e conservar a liberdade de acção	
Massa	Potencial superior	- Lançaram-se ataques com grandes quantidades de computadores "zombies" de modo a tornar os recursos de um sistema indisponíveis, por exemplo a capacidade de resposta de um servidor (e.g. serviços de saúde, tecnologia, bancos, comunicação social) aos utilizadores legítimos, obrigando o servidor a reiniciar ou mesmo a ficar indisponível durante algum tempo.	ID
Economia de Forças	Emprego judicioso dos meios	- Não conseguimos tirar conclusões precisas porque, apesar de haver declarações do deputado Russo (Sergei Markov) de que os ataques teriam sido incentivados e coordenados por um dos seus assistentes, não se sabe ao certo se os ataques foram o resultado de raiva espontânea de atacantes com o objectivo de se mostrarem indignados com a mudança do monumento. Ou seja, não podemos concluir se houve algum planeamento com vista ao emprego judicioso dos meios (por exemplo o conjunto de Botnets) em locais e momentos adequados	ND
Manobra	Disposição das forças	- Conseguiu-se colocar a Estónia em posição desvantajosa, na medida em que foram utilizados milhares de computadores infectados espalhados pelo mundo (rede de Botnets), saturando os servidores das infra-estruturas críticas da Internet da Estónia.	ID
	Massa e Economia de Forças, Liberdade de acção, Iniciativa	- Ao atingir com eficácia o princípio da Manobra, os autores dos ataques conseguiram conservar a sua liberdade de acção, desenvolvendo os ataques como planeado e alcançando os seus objectivos que seriam destabilizar o normal funcionamento das infra-estruturas críticas e paralisar a economia da Estónia e impedir que a disseminação de informação se fizesse para o exterior.	
Unidade de Comando	Acção coordenada	- No nosso ponto de vista este princípio da guerra também não se verifica no estudo caso da Estónia, porque nunca se veio a saber da veracidade das fontes de ataques dirigidos contra a Estónia. Portanto não se pode dizer que as acções desenvolvidas foram coordenadas de forma a convergir os seus esforços num objectivo comum, nem a existência de Doutrina e de Comando a orientarem a acção das forças.	ND
	Unidade de Doutrina e Comando		
	Autoridade única		
Segurança	Informação	- Os autores dos ataques conseguiram concretizar os seus ataques, evitando que a Estónia tivesse acesso informações precisas de quem seriam os autores destes ataques e os seus planos	ID
	Liberdade de acção	- Ao atingir o princípio da Segurança conseguiu-se obter liberdade de acção para o desenvolvimento das acções.	
Surpresa	Situações inesperadas	- Os ataques contra a Estónia foram efectuados de tal forma que a Estónia não conseguiu reagir eficazmente por não saber ao certo quem seriam os autores desses ataques.	ID
	Posição desvantajosa	- A estónia apresenta uma grande dependência face às tecnologias de informação e recursos limitados para gerir as suas infra-estruturas, colocando-a em posição desvantajosa.	
	Manobra, Ofensiva, Segurança	- Face ao anteriormente dito, fácil é concluir que a Estónia ao ser colocada numa posição desvantajosa, o Principio da Surpresa foi alcançado contribuindo para que outros princípios pudessem ser alcançados, como por exemplo o princípio da Manobra, Ofensiva e Segurança.	
Simplicidade	Plano simples	- Hoje em dia é fácil de estruturar de forma eficaz redes de Botnets para interromper ou bloquear o tráfego na Internet; - Estava acessível em salas de chat na Internet a qualquer cidadão as ferramentas (software e lista de alvos a atacar) necessárias para desencadear ataques às infra-estruturas criticas.	ID

4.3 ESTUDO DE CASO DA GEÓRGIA

"*Em Agosto de 2008, a Rússia atacou a Geórgia em uma disputa pela província georgiana da Ossétia do Sul. Enquanto os militares russos organizavam seu avanço por terra e ar, um grupo de nacionalistas russos se unia ao embate na Internet*" (McAfee, 2009 p. 7).

4.3.1 Antecedentes e Contexto dos ataques cibernéticos contra a Geórgia

No conflito armado que eclodiu a Agosto de 2008 tínhamos como intervenientes, de um lado a Geórgia (apoiada pelos E.U.A) e do outro lado a Federação Russa que, veio em apoio da Ossétia do Sul (região autónoma e desmilitarizada da Geórgia que faz fronteira com a Geórgia e a Rússia) (Tikk, 2008).

A Ossétia do Sul declarou a sua independência em 1991, durante um conflito entre Georgianos e Ossetas, apesar de perante a Comunidade Internacional a Ossétia do Sul ainda ser reconhecido como parte integrante da Geórgia (Tikk, 2008).

Com o cessar-fogo e esforços enormes para restabelecer a paz o conflito manteve-se ficando por resolver. Na tentativa de resolver o problema, foi criada uma força de paz em 1992, sob mandato da OSCE[23], constituída por forças da Geórgia, forças da Estónia e forças Russas, contudo o comando desta força que tinha por objectivo restabelecer e manter a paz estava sob o comando Russo, o que na prática, a sua actuação como força acabou por aumentar a tensão entre a Geórgia de um lado, e a Federação Russa do outro lado que apoiava as forças separatistas da Ossétia do Sul (Tikk, 2008).

A 7 de Agosto de 2008, para responder às provocações por parte das forças separatistas da Ossétia do Sul, a Geórgia lançou um ataque surpresa (Tikk, 2008).

Como forma de resposta e em auxílio da Ossétia do Sul, a 8 de Agosto de 2008, as forças Russas respondem e entram em território georgiano. Estas operações militares por parte da Rússia foram vistas como uma agressão militar contra a Geórgia (Tikk, 2008).

Em paralelo e um pouco antes das forças Russas entrarem em território georgiano, outras operações já estavam em curso. Ataques Cibernéticos já estavam a ser lançados contra um grande número de sítios governamentais e de imprensa (Tikk, 2008).

Este caso, é portanto um caso muito interessante e importante de se estudar, porque foi a primeira vez que um acontecimento político-militar terá sido acompanhado (ou mesmo

[23] **OSCE** – Organização para a Segurança e Cooperação na Europa voltada para a promoção da democracia e do liberalismo económico na Europa [http://www.osce.org/]

precedido) e coordenado com uma Ofensiva levada a cabo no Ciberespaço por um grupo de hacktivistas[24] Russos (Tikk, 2008).

Qualquer indivíduo nascido na Rússia ou não, podia ter acesso a sítios com instruções simples de como lançar ataques de negação de serviço contra a Geórgia, em que o utilizador apenas tinha de fazer o download do software e digitar o endereço Web de um alvo.

Em resultado disto, os sítios governamentais e sítios de jornais estavam impedidos de informar a população quer para dentro quer fora da Geórgia, dificultando assim gravemente as comunicações públicas do País (McAfee, 2009).

Segundo o relatório de Novembro de 2008 da CCDCOE os métodos utilizados para levar a cabo esta guerra cibernética, foram em muito idênticos aos métodos levados a cabo no caso anterior da Estónia, apenas com uma pequena diferença - os ataques efectuados à Geórgia foram mais intensos (Tikk, 2008).

Um dos métodos utilizados terá sido a desfiguração de sítios que foram dirigidas principalmente para sítios governamentais, políticos e financeiros, como por exemplo, o site do Presidente da República da Geórgia (*Mikheil Saakashvili*) assim como o site do Ministério dos Negócios Estrangeiros terão sido apagados e substituídos fotos de Adolf Hitler. O site do Banco Nacional da Geórgia foi apagado e substituído por uma galeria de fotos de ditadores do século XX.

Outro dos métodos utilizados terá sido os ataques DDoS ou ataques de negação de serviços que segundo informação recebida da CERT-EE[25] localizada na Estónia e confirmada pela embaixada Georgiana na capital da Estónia (Tallinn) os ataques que empregaram este método foram dirigidos principalmente a sítios do sector público e privado, como por exemplo sítios do Governo (Ministério da Educação e Ciência da República da Geórgia, Parlamento da República da Geórgia, Presidente da República da Geórgia, Site oficial do Governo da República Atutónoma da Abkhazia), sítios de notícias (o maior fórum da Geórgia, Associação de Imprensa, empresa privada de televisão e sítios de notícias), um site de uma instituição financeira, entre muitos outros[26]. Estes ataques tiveram duração média de 2horas e 15 minutos, sendo que o mais duradouro permaneceu por 6horas (Tikk, 2008).

Outro método utilizado terá sido a distribuição de instruções e software malicioso em blogues, fóruns e sítios que continham a informação e conteúdo necessário para que qualquer indivíduo pudesse fazer uso contra a Geórgia, ou seja, dispunham de um software que podia ser descarregado em vários sítios previamente programado para efectuarem

[24] Praticam *hacktivism* que segundo Luís Tomé, especialista em Relações Internacionais é uma junção de grupo de hackers motivados politico-ideológicamente. (Almeida, 2009)
[25] Serviço de resposta a Incidentes de Segurança Informática para a Estónia, criado no ano de 2006, responsável pela gestão de incidentes de segurança nas redes de computadores da Estónia.
[26] Como por exemplo um site de uma comunidade hacker da Geórgia [www.hacking.ge]

ataques bastando apenas o indivíduo introduzir um site à escolha. Juntamente com o programa viria em anexo um documento com uma lista de sítios que constituíam os alvos preferenciais (Tikk, 2008).

Quanto à origem dos ataques, não se consegue atribuir a responsabilidade deste ataques tal como aconteceu na Estónia. Os resultados não são conclusivos, não há provas por detrás dos ataques DDoS efectuados, existindo apenas uma suspeita de que tenham sido levadas a cabo pela Rússia. Contudo, as conclusões deixam claro que os ataques foram amplamente planeados e coordenados, não sendo apenas reacções individuais de hacktivistas (Tikk, 2008).

4.3.2 Análise dos Princípios da Guerra à luz do Estudo de Caso da Geórgia

Neste estudo de caso iremos proceder da mesma forma como foi feito no estudo de caso anterior com a Estónia, ou seja, iremos analisar cada princípio da guerra individualmente, de forma a tentar encontrar evidências que justifiquem que os princípios se revelam presentes neste estudo de caso.

1) **Princípio do Objectivo** – Aqui pode-se apontar uma diferença em relação ao caso da Estónia. Comparativamente com a Estónia, no caso da Geórgia, se os ciberataques foram executados e tolerados pela Rússia, podemos dizer que para alcançar o objectivo último da guerra, foram "traçados" objectivos intermédios (atacar sítios políticos e serviços) que uma vez alcançados iriam contribuir para o alcançar o objectivo último da guerra. De resto, em tudo é idêntico ao caso da Estónia, na medida que também foram por exemplo distribuídos na Internet objectivos claros (listas de alvos, software) acessível a qualquer cidadão.
2) **Princípio da Ofensiva** – Este princípio revela-se presente, isto porque a Rússia, fez uso de todos os meios à sua disposição, explorando todas as oportunidades, de por meio de acções ofensivas (ofensiva cibernética), obter iniciativa e alcançar resultados decisivos (impedir que a Geórgia disseminasse informação para a sua população e fora do País), impondo a sua vontade e marcando o seu ritmo, explorando os pontos fracos da Geórgia.
3) **Princípio da Massa** – À semelhança do caso anterior este princípio revela-se presente no caso da Geórgia, visto que para conseguir destabilizar as operações no Ciberespaço deste Estado, a Rússia fez uso de vários métodos (ataques de negação de serviços, alteração de conteúdos de sítios, distribuição de listas de alvos e software malicioso) para obter superioridade no Ciberespaço.
4) **Princípio da Economia de Forças** – Ao contrário do caso anterior da Estónia, em que poucas provas existiam se os ataques teriam sido coordenados com o

consentimento do governo da Rússia, acabando por concluir que este princípio não se revelava presente. Neste caso da Geórgia podemos de certa forma dizer que este princípio se revela presente, na medida em que para cada teatro de operações (terra, ar e ciberespaço) a Rússia procurou empregar judiciosamente os meios à sua disposição.

5) **Princípio da Manobra** – Não bastava já a Rússia lançar uma ofensiva por terra e ar da Rússia contra a Geórgia, que também lançou uma ofensiva cibernética coordenadamente atingindo sítios políticos (sítios governamentais e da presidência e serviços) e serviços (comunicação social, serviços bancários online), colocando a Geórgia em posição desvantajosa, permitindo à Rússia conservar a liberdade de acção, desenvolvendo os seus ataques como planeado, alcançando os seus objectivos (Tikk, 2008).
6) **Princípio da Unidade de Comando** – No nosso ponto de vista, no caso da Geórgia podemos de certa forma dizer que existiu Unidade de Comando. Ou seja, foram facultadas informações importantes a hackers (data e hora precisa marcada para as ofensivas lançadas por terra e ar) de forma a coordenarem os ataques e fazer convergir os esforços tendo em vista o mesmo objectivo. Ou seja, houve coordenação para orientar acções de forças diferentes.
7) **Princípio da Segurança** – Podemos dizer que este princípio da guerra se revelou presente no caso da Geórgia, isto porque é sempre ou quase impossível os alvos dos ataques (neste caso a Geórgia) obter informações precisas das fontes dos ataques para puder dar resposta em tempo oportuno. Ou seja, conseguiu-se negar ao inimigo a possibilidade dele obter informações sobre os ataques que estavam planeados, alcançando os objectivos pretendidos, ocultando informações sobre si próprios, permitindo por sua vez liberdade de acção para o desenvolvimento das acções no ciberespaço.
8) **Princípio da Surpresa** – Ao mesmo tempo que foram lançados ataques contra as forças separatistas da Geórgia na Ossétia do Sul, estava a ser perpetuado ataques cibernéticos em simultâneo com os ataques físicos, o que incapacitou gravemente as comunicações públicas do País, possibilitando à Rússia obter uma vitória psicológica significativa ao impedir que a Geórgia disseminasse informações dos acontecimentos para a sua população (McAfee, 2009; Tikk, 2008).
9) **Princípio da Simplicidade** – Consegue-se aplicar este princípio da guerra no caso da Geórgia na medida em que, os métodos utilizados para perpetrar os ataques (desfiguração de sítios, ataques DDoS ou ataques de negação de serviços e distribuição de instruções e software malicioso) não exigem grande complexidade, em tudo similar ao caso anterior descrito da Estónia.

4.3.3 Considerações finais do estudo de caso da Geórgia

Pode-se concluir deste estudo de caso que todos os Princípios da Guerra se revelaram presentes para uma acção de Ciberguerra no Ciberespaço, como podemos constatar no Quadro 6.

Quadro 6. Princípios da Guerra identificados no estudo de caso da Geórgia

Princípios da Guerra Clássica (RC 130-1)	Estudo de caso da Geórgia		
	Palavras-Chave	Indicadores (ID – Principio Identificado / ND – Principio não Identificado)	
Objectivo	Objectivo último	-Neste caso, vê-se claramente que os objectivos traçados para perpetrar via Internet foram definidos de modo a contribuir alcançar o objectivo último da Rússia.	ID
	Objectivos claros	- Os objectivos eram claros e disponíveis a qualquer pessoa que entendesse participar na guerra.	
	Objectivos exequíveis	- Com os meios disponíveis os objectivos eram exequíveis.	
Ofensiva	Pontos fracos do IN	- Foram explorados os pontos fracos da Geórgia (falta de capacidade para responder a estes tipos de ataques).	ID
	Resultados decisivos	- A ofensiva cibernética contribuiu para que fossem alcançados resultados decisivos (como por exemplo a ofensiva levada a cabo por terra e ar, e ainda impossibilidade da Geórgia fazer comunicações publicas à sua população).	
Massa	Potencial superior	- Rússia fez uso de vários métodos (ataques de negação de serviços, desfiguração de sítios, distribuição de listas de alvos e software malicioso) para obter superioridade no Ciberespaço, à semelhança do caso da Estónia.	ID
Economia de Forças	Emprego judicioso dos meios	- Houve uma preocupação da Rússia em empregar judiciosamente os meios à sua disposição, perante o adversário que tinha à sua frente para alcançar resultados decisivos. Ou seja, neste caso podemos dizer que este princípio se revela presente, isto porque existe uma participação activa da Rússia ao coordenar os ataques levados a cabo em terra, no ar e no ciberespaço.	ID
Manobra	Disposição das forças	- A Rússia dispôs as suas forças de modo a entrar em território Georgiano tanto por Terra, Ar e Ciberespaço colocando assim a Geórgia em posição desvantajosa.	ID
	Massa e Economia de Forças, Liberdade de acção, Iniciativa	- A Rússia ao conseguir uma boa Manobra tanto por Terra, Ar e Ciberespaço consegue a aplicação correcta da Massa, Economia de Forças, Liberdade de acção e Iniciativa.	
Unidade de Comando	Acção coordenada	- A Rússia facultou informações importantes para que grupos de Hacker's desenvolvessem os seus ataques cibernéticos; - Houve coordenação de forma a orientar acções de forças diferentes (acções por terra, ar e ciberespaço).	ID
	Unidade de Doutrina e Comando		
	Autoridade única		
Segurança	Informação	- Apesar de se saber que os ataques foram tolerados e patrocinados por parte da Rússia, não se sabe ao certo a origem dos ataques.	ID
	Liberdade de acção	- Os ataques cibernéticos até ao momento, por ser difícil ou mesmo quase impossível detectar a fontes dos ataques, garante sempre que o princípio da segurança seja alcançado, que por sua vez irá permitir alcançar liberdade de acção para o desenvolvimento das acções.	
Surpresa	Situações inesperadas	- Geórgia ficou incapacitada de fazer chegar informação à sua população via Internet.	ID
	Posição desvantajosa	- A Geórgia ao não estar em condições de responder aos ataques cibernéticos, viu-se em posição desvantajosa para puder actuar em tempo oportuno.	
	Manobra, Ofensiva, Segurança	- Os ataques às infra-estruturas críticas da Internet da Geórgia foram uma mais-valia para garantir o sucesso das operações como um todo, contribuindo como tal, para alcançar o princípio da Manobra, Ofensiva e Segurança.	
Simplicidade	Plano simples	- Métodos e planos em muito idênticos ao caso da Estónia; - Atacar infra-estruturas críticas da Internet da Geórgia	ID

4.4 BALANÇO FINAL E CONCLUSÕES DOS ESTUDOS DE CASO

Podemos concluir destes dois estudos de casos e da análise da Figura 5, que representa uma síntese do relatório de criminologia virtual de 2009 da McAfee, o seguinte:

- A grande diferença entre os dois estudos de caso encontra-se na origem dos seus ataques. No estudo de caso da Estónia existem poucas ou mesmo nenhumas evidências de envolvimento de países (eventual envolvimento da Rússia) nos ataques contra este Estado (Estónia), apenas existindo suspeitas. Já no estudo de caso da Geórgia existem provas de que estes ataques foram patrocinados e executados por países (executados pela Rússia).

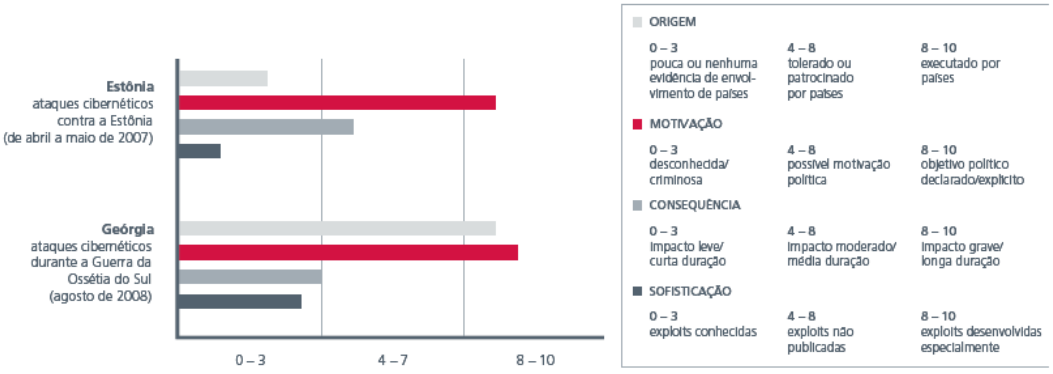


Figura 5. Avaliação dos atributos dos ataques Cibernéticos
Fonte: Adaptado de (McAfee, 2009 p. 9)

- Que o princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio segurança, princípio da surpresa e o princípio da simplicidade se revelam todos importantes para uma acção de Ciberguerra no Ciberespaço, com a excepção do princípio da economia de forças e o princípio da unidade de comando que com base na documentação analisada, não foi possível encontrar dados suficientes, que provassem a relevância destes princípios para acções de Ciberguerra. Contudo, no nosso ponto de vista, num futuro próximo, estes princípios poderão vir a revelar-se por exemplo, com a criação de centros de ciberdefesa (por exemplo a criação do “Cyber Command” nos E.U.A. e do Ciber-Comando para a cibersegurança na OTAN em Bruxelas), onde será exigido certamente o Princípio da Unidade de Comando, de forma a fazer convergir todos os esforços tendo em vista um objectivo comum, contudo deverá ter-se em conta que este princípio poderá ser quebrado com o uso de comunidades de Hackers (hacktivistas) em apoio das operações de Ciberguerra. Ou seja, o princípio da Unidade de Comando poderá ser repartido por vários pontos de decisão.

Quadro 7. Quadro resumo dos Princípios da Guerra mais relevantes na Ciberguerra

Princípios da Guerra Clássica (RC 130-1)	Estudos de Caso		Revela-se importante?
	Estónia	Geórgia	
Objectivo	ID	ID	SIM
Ofensiva	ID	ID	SIM
Massa	ID	ID	SIM
Economia de Forças	ND	ID	POUCO
Manobra	ID	ID	SIM
Unidade de Comando	ND	ID	POUCO
Segurança	ID	ID	SIM
Surpresa	ID	ID	SIM
Simplicidade	ID	ID	SIM

Legenda:

ID – Princípio Identificado

ND – Princípio não Identificado

Em suma, com a análise destes dois estudos de caso, concluímos que os Princípios da Guerra indicados no Quadro 7 podem ser aplicados à Ciberguerra. O próprio General Loureiro dos Santos reforça as conclusões do estudo apresentado quando na entrevista realizada, transmitiu a ideia de que os grandes princípios da guerra, como seja o princípio da economia de forças, do objectivo, o princípio da surpresa e o da simplicidade, se aplicam *OTAN* à guerra no ciberespaço. (Santos, 2010)

5. ENTREVISTA

Neste trabalho de investigação recorreu-se à realização do método de investigação entrevista, como instrumento de produção de informação, com o objectivo de obter respostas importantes que valorizassem o trabalho como um todo e confirmasse a análise de conteúdo realizada. Tendo sido no entanto realizada apenas uma entrevista ao General Doutor Loureiro dos Santos com conhecimentos nesta temática. Este aderiu com entusiasmo e satisfação na participação neste trabalho, respondendo prontamente a todas as questões colocadas e transmitindo todo o seu saber. A aplicação deste método de investigação a apenas um elemento da instituição militar, deve-se fundamentalmente à limitação de tempo para a realização do estudo e a inexistência de especialistas nesta área no meio militar, que possuam conceitos consolidados para a construção do puzzle da Ciberguerra. Obtivemos também algumas orientações conceptuais do Tenente-coronel Doutor Paulo Viegas Nunes.

Da entrevista realizada (Apêndice B) após a gravação da mesma e tratamento dos dados foi realizada a técnica de análise de conteúdo que se encontra no Quadro 8. O objectivo da entrevista consiste em obter uma definição de Ciberguerra; saber se existe casos de Ciberguerra; saber se o Ciberespaço pode ser considerado como novo palco de operações; obter uma definição de Ciberespaço; saber se os Princípios da Guerra Clássica podem ser aplicáveis na Ciberguerra.

Quadro 8. Análise de conteúdo da entrevista realizada ao General Loureiro dos Santos

Categorias	Subcategorias	Unidades de Registo
Ciberguerra	Definição de Ciberguerra	*"(…) a Ciberguerra é o conjunto de acções que é possível fazer no Ciberespaço, para obrigar um actor político a agir da forma que o actor que desencadeia essas acções pretende."*
	Existiram casos de Ciberguerra?	*"(…)Tem havido acções de Ciberguerra. O exemplo que se costuma utilizar e que, no meu ponto de vista, irá ser o tipo de guerra na nossa era da informação, foi a guerra dos cinco dias entre a Rússia e a Geórgia (…)"*
Ciberespaço	Definição de Ciberespaço	*"O Ciberespaço é o espaço virtual, gerado pelos elementos tecnológicos dos computadores, toda essa área da informática onde se efectuam interacções entre as pessoas, organizações ou países, de toda a natureza - interacções económicas, sociais, politicas. Um espaço virtual, sustentado, apoiado, gerado por tecnologias novas de informação e comunicação (…)"*
	Ciberespaço como no palco de operações?	*"A partir do momento que o Ciberespaço adquiriu esta importância para a vida das sociedades, para a vida moderna, para tudo, incluindo as Forças Armadas, então combate-se no Ciberespaço."*
Princípios da Guerra clássica	São os princípios da Guerra Clássica aplicáveis na Ciberguerra?	*"(…) mas agora penso que, genericamente, se aplicarão (…)"* *" Portanto a minha ideia é que os grandes princípios da guerra, o princípio da economia de forças, do objectivo, o princípio da surpresa, da simplicidade… se aplicarão à guerra no ciberespaço."*

CONCLUSÕES

Na síntese deste estudo exploratório e atendendo aos prováveis nove princípios da guerra apresentados no trabalho, torna-se necessário sistematizar os aspectos mais relevantes, de modo a responder à nossa questão derivada: Quais os princípios da guerra clássica mais relevantes na Ciberguerra, atendendo aos nove princípios da guerra clássica? e consequentemente responder à questão central: São os Princípios da Guerra clássica aplicáveis à Ciberguerra? que norteou todo o trabalho. Deste modo, conclui-se que:

- a Ciberguerra consiste num método, englobando um conjunto de acções para obrigar um actor político a agir da forma que o actor que desencadeia essas acções pretende que haja, usando como palco de operações um espaço virtual gerado pelos elementos tecnológicos dos computadores e desenvolvido pelo Homem designado de Ciberespaço;
- com este novo método ao alcance de qualquer um, é exigido obter uma capacidade tecnológica no domínio da segurança, exigindo estruturas próprias de ciberdefesa e cibersegurança, com vista a antecipar ataques desta natureza, ou mesmo e perpetrar ataques cibernéticos num conflito armado em coordenação ou não com outros teatros de operações;
- os Princípios da Guerra continuam actuais e relevantes para acções de Ciberguerra e podem ser aplicáveis e usados na acção de comando e controlo dos chefes militares;
- o Princípio do Objectivo é na Ciberguerra aplicável na medida em que é possível traçar objectivos claros e exequíveis em função da missão e meios colocados è disposição tendo em conta as características da área de operações que é o Ciberespaço;
- o Princípio da Ofensiva continua a ser um princípio importante porque é possível lançar Ofensivas neste novo espaço operacional procurando explorar os pontos fracos das tecnologias de informação em complemento ou não de acções desenvolvidas noutros teatros de operações para alcançar resultados decisivos;
- o Princípio da Massa pode ser alcançável e verifica-se na Ciberguerra, porque é possível com os meios existentes e vulnerabilidades decorrentes das tecnologias de informação obter a determinado momento em local e momento decisivo potencial de combate superior, por exemplo com o uso dos milhares de computadores ligados à Internet espalhados pelo Mundo.
- o Princípio da Economia de Forças é um dos dois princípios que, com o estudo feito, não foi possível tirar conclusões, contudo temos a percepção de que é um princípio que não deixa de ser importante porque se a Ciberguerra é algo

estritamente de cariz militar, e por consequência em todas as acções militares é exigido o emprego judicioso dos meios, este é um princípio que não pode ser posto de parte, exigindo um controlo dos meios à sua disposição.

- o Princípio da Manobra também se revelou importante para a Ciberguerra isto porque é possível dispor as forças (não fisicamente, mas virtualmente como por exemplo empregar computadores infectados de todos os cantos do Mundo) e colocar o adversário em posição desvantajosa.
- o Princípio da Unidade de Comando à semelhança do Princípio da Economia de forças não se revelou tanto até ao momento, também pelo motivo de que o virtual é ainda um espaço onde qualquer um pode ter a iniciativa e levar a cabo acções ilícitas (por exemplo Hackers desenvolverem de forma autónoma ataques a redes), o que poderá colidir e comprometer as acções militares.
- o Princípio da Segurança é um princípio que pode ser alcançado na Ciberguerra isto porque é possível conservar a liberdade de acção ao negar a possibilidade do adversário obter informações dos nossos planos.
- o Princípio da Surpresa está presente na Ciberguerra porque é possível criar situações inesperadas atacando infra-estruturas críticas da Internet e obter informações importantes.
- o Princípio da Simplicidade no nosso ponto de vista é dos princípios que se revelou presente e facilmente alcançável na medida em que com os meios disponíveis é relativamente fácil e barato e está ao alcance de qualquer um elaborar planos simples e atacar infra-estruturas críticas da Internet.

Nas principais dificuldades sentidas na elaboração deste trabalho de investigação aplicada há a destacar:

- A dificuldade em descobrir o "*Estado* da Arte" e a escolha de estudos de casos, visto que esta limitação encontra-se directamente associada ao resultado da limitação no acesso a documentos militares classificados e no caso da Indústria pela inexistência da divulgação de incidentes de segurança;
- A quase inexistência de especialistas nesta área no meio militar, que possuam conceitos consolidados para a construção do puzzle da Ciberguerra, o que nos dificultou em muito a obtenção de respostas no que diz respeito à aplicação dos princípios da guerra clássica na Ciberguerra e possíveis exemplos;

Tem-se consciência que alguns assuntos devido às limitações referidas e ao tempo disponível não são abordadas, no entanto, como possível previsão de trabalhos futuros de investigação nesta temática consideramos a possibilidade de:

- Construir uma politica de segurança da Informação para o Exército, tendo por suporte as Normas Internacionais, doutrinas e requisitos militares já existentes, para desenvolver uma cultura de segurança para as redes de informação, por exemplo, à semelhança da Agencia Europeia para a Segurança das Redes e da Informação (*ENISA*)
- A construção de jogos de Ciberguerra, à semelhança do que é praticado noutras instituições militares estrangeiras, por exemplo, à semelhança da Academia de *West Point* dos E.U.A, onde cadetes trocaram as "trincheiras por firewalls"[27].

Para finalizar, podemos concluir que a Ciberguerra constitui um novo método para desenvolver Operações Militares. Operação Militares de natureza, um pouco diferentes daquelas conhecidas até hoje, pelo facto de se desenvolver num Teatro de Operações bastante diferente dos que se conhecem, designado por Ciberespaço. Sendo que a Ciberguerra, constitui hoje, um método aceite para desenvolver operações militares, que engloba um conjunto de acções (CNA, CND e CNA) que são desenvolvidas no Ciberespaço, de modo a atingir determinado fim político.

E que as acções de Ciberguerra no Ciberespaço podem ser planeadas tendo em consideração o princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio segurança, princípio da surpresa e o princípio da simplicidade, de modo a orientar a acção de comando dos chefes militares, auxiliando-os num planeamento racional e eficiente nas suas operações de Ciberguerra.

[27] Cadetes da Academia de *West Point* tiveram que construir uma rede de computador e mantê-la activa e operacional, enquanto Hackers da Agência de Segurança Nacional dos Estados Unidos situada em *Maryland,* tentava infiltra-se dentro dessa rede através de métodos utilizados pelo Inimigo. (http://www.nytimes.com/2009/05/11/technology/11cybergames.html)

BIBLIOGRAFIA

Alexander, Keith B. 2010. United States Strategic Command. [Online] Maio de 2010. [Citação: 30 de Julho de 2010.] http://www.stratcom.mil/factsheets/cc/.

Almeida, João. 2009. Ciberguerras. [Online] 22 de Junho de 2009. [Citação: 24 de Fevereiro de 2010.] http://sic.sapo.pt/programasInformacao/scripts/videoplayer.aspx?ch=falarglobal&videoId={2856A00C-DD54-4BD2-B958-D15E907867F4}.

Alves, José Lopes. 1998. *ESTRATÉGIA - Panorama Geral da Sua Teoria.* Lisboa : Publicações Dom Quixote, Lda., 1998.

Casa Branca. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington : s.n., 2009.

CCDCOE. 2009. Cooperative Cyber Defence Cooperative Cyber Defence. [Online] 2009. [Citação: 24 de Março de 2010.] http://www.ccdcoe.org.

—. 2009. Information About Estonia. [Online] 2009. [Citação: 22 de Fevereiro de 2010.] http://www.ccdcoe.org/72.html.

Chope, M. Christopher e Kõuts, M. Tarmo. 2008. *CINQUANTE-CINQUIÈME SESSION - La guerre informatique.* 2008. A/2022.

Clausewitz, Carl. 2003. *Príncipios da Guerra.* Lisboa : Edições Sílabo, 2003.

Clay, Wilson. 2008. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Washington DC : CRS Report for Congress, 2008. RL321114.

—. 2007. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Washington DC : CRS Report for Congress, 2007. RL321114.

—. 2001. *Cyberwarfare.* Washington DC : CRS Report for Congress, 2001. RL30735.

—. 2007. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.* Washington DC : CRS Report for Congress, 2007. RL31787.

Cornish, Paul. 2009. *Cyber-Security and Politically, Socially and Religiously.* Brussels : European Parliament, 2009. PE 406.997.

Couto, Abel Cabral. 1988. *Elementos de Estratégia.* Lisboa : INSTITUTO DE ALTOS ESTUDOS MILITARES, 1988. Vol. I.

DISRF. 2000. Doctrine of the Information Security of the Russian Federation. [Online] 9 de Setembro de 2000. [Citação: 12 de Abril de 2010.] http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

Ferreira, Manuel e Serra, Fernando. 2009. *Casos de Estudo - Usar, Escrever e Estudar.* Lisboa : LIDEL, 2009.

FM3-0. 2001. *Operations.* Washington : Department of the Army, 2001.

Foch, Ferdinand. 1903. *Des Principes de la Guerre.* Paris : Berger-Levrault & Cie, Éditeurs, 1903.

Frost, Robert S. 1999. *The Growing Imperative to Adopt "Flexibility" as an American Principle of War.* s.l. : Strategic Studies Institute, 1999.

GAO. 2004. *CRITICAL INFRASTRUCTURE PROTECTION - Challenges and Efforts to Secure Control Secure Control.* s.l. : United States General Accounting Office, 2004. GAO-04-354.

Goode, W. e Hatt, P. 1969. *Métodos em pesquisa social.* 3.ª Ed. São Paulo : Cia Editora Nacional, 1969.

Hildreth, Steven A. 2001. *Cyberwarfare.* Washington DC : CRS Report for Congress, 2001. RL30735.

Hughes, Rex. 2009. *NATO and Cyber Defence - Mission Accomplished?* s.l. : NATO, 2009.

JDP 0-01. 2008. *Joint Doctrine Publication 0-01.* 3rd Edition. Swidon : s.n., 2008.

Joint Publication 3-13. 2006. *Information Operations.* 2006.

JP 1-02. 2009. *Department of Defense Dictionary of Military and Associated Terms.* 2009.

JP 2-01.3. 2000. *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.* 2000.

Krekel, Bryan. 2009. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* McLean : Northrop Grumman, 2009.

Le Livre Banc. 2008. *Défense et Sécurité nationale - LE LIVRE BLANC.* Paris : Odile Jacob, 2008.

Lemos, Manuel. 1998. *Estar na Internet: Tudo o precisa saber sobre a Internet.* Alfragide : McGRAW-HILL, 1998.

Livro Verde. 2005. *Livro Verde: Relativo a um programa Europeu de protecção das infra-estruturas críticas.* Bruxelas : s.n., 2005. COM(2005) 576 final.

McAfee. 2009. *Relatório de criminologia virtual: "Virtualmente real" - A era da guerra cibernética.* São Paulo : McAfee, 2009.

Murawiec, Laurent. 1999. AGIR - Revue Génerale de Stretégie. *Révolution de l'information, crise de Communication.* 2, 1999, La cyberguerre.

Nunes, Paulo Viegas. 2010. Pós-Graduação/Mestrado em Guerra de Informação/Competitive Intelligence. *Exercício de Gestão de Crises no Ciberespaço.* Lisboa, 4 de Junho de 2010.

OCS. 2009. *Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space.* Norwich : TSO, 2009.

Petit Robert. 2010. Le nouveau Petit Robert de la Langue Française 2010. [Online] 2010. [Citação: 14 de Maio de 2010.] http://pr2010.bvdep.com/version-1/pr1.asp.

Pravda, Komsomolskaya. 2007. Estônia comete sacrilégio ao desmantelar monumentos a soldados soviéticos. [Online] 20 de Fevereiro de 2007. [Citação: 22 de Fevereiro de 2010.] http://port.pravda.ru/mundo/15609-0/.

Quivy, Raymond e Campenhoudt, Luc Van. 1992. *Manual de investigação em Ciências Sociais.* Lisboa : Gradiva, 1992.

RC 130-1 . 1987. *Operações.* Lisboa : Estado Maior do Exército, 1987. Vol. I.

RC-OP. 2005. *Regulamento de Campanha - OPERAÇÕES.* Lisboa : Estado Maior do Exército, 2005.

Rohozinski, Rafal. 2009. *Tracking GhostNet: Investigating a Cyber Espionage Network.* Toronto : University of Toronto, 2009.

Santos, José Alberto Loureiro dos. 2009. *As Guerras que já aí estão e as que nos esperam - se os políticos não mudarem.* Mem Martins : Publicações Europa-América, 2009.

—. 2010. *Entrevista ao Exm. General Doutor Loureiro dos Santos.* Carnaxide, 14 de Junho de 2010.

Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos. 2008. *CYBERWAR - O Fenómeno, as Tecnologias e os Actores.* Lisboa : FCA, 2008.

Silva, Frederico da Costa Lopes da. 1952. *Os Princípios da Guerra: Factores da guerra, Leis da ciência, Regras da Arte.* Lisboa : Tipografia da L. C. G. G., 1952.

Tikk, Eneken. 2008. *Cyber Attacks Against Georgia: Legal Lessons Identified.* Tallinn : NATO, 2008.

TVNET. 2009. A guerra no ciberespaço. [Online] 28 de Maio de 2009. [Citação: 22 de Fevereiro de 2010.] http://tvnet.sapo.pt/noticias/video_detalhes.php?id=44111 .

Tzu, Sun. 2006. *A Arte da Guerra.* Lisboa : Edições Sílabo, 2006.

USDHS. 2009. *National Infrastructure Protection Plan - Partnering to enhance protection and resiliency.* s.l. : U.S. Department of Homeland Security, 2009.

Wilkin, Dorsey, et al. 2009. Cyberspace Policy for Critical Infrastructures. [autor do livro] Mauricio Papa e Sujeet Shenoi. *Critical Infrastructure Protection II.* s.l. : Springer Boston, 2009.

APÊNDICES

APÊNDICE A - CLÁSSICOS E PRINCÍPIOS DA GUERRA

Princípios actuais	Pensamentos	
	Pensamento de Sun Tzu	**Pensamento de Carl von Clausewitz**
Objectivo		"*A guerra consiste na combinação de muitos combates isolados… Contudo, o combate é, ele próprio, muito mais importante, de momento, uma vez que apenas a combinação de combates vitoriosos produzirá bons resultados."* (Clausewitz, 2003 p. 39) "*Nos planos que esboçamos para a batalha devemos eleger um grande objectivo*." (Clausewitz, 2003 p. 42) "*O segundo princípio é o seguinte: devemos concentrar o nosso poder tanto quanto possível naquele sector onde pretendemos desferir o ataque, mesmo que corramos o risco de ficar em desvantagem noutros pontos, para que as probabilidades de êxito aumentem nos pontos decisivos. O sucesso nestes pontos decisivos compensará quaisquer desvantagens consentidas noutros pontos*." (Clausewitz, 2003 p. 64)
Ofensiva	*"Assim, na guerra, deixa que o teu grande objectivo seja a vitória e não campanhas prolongadas."* (Tzu, 2006 p. 76) *"Acautelarmo-nos contra a derrota está nas nossas mãos, mas a oportunidade derrotar o inimigo é proporcionada pelo próprio inimigo."* (Tzu, 2006 p. 85)	*"Um princípio fundamental é nunca permanecer totalmente passivo, mas antes atacar o inimigo de frente e pelos flancos, mesmo quando ele nos está a atacar."* (Clausewitz, 2003 p. 41) *"A terceira regra consiste em não perder tempo. A menos que possamos retirar vantagens dum compasso de espera, devemos lançar mãos à obra tão depressa quanto possível…"* (Clausewitz, 2003 p. 64)
Massa	*"Se ele estiver confiante em todos os pontos, prepara-te para ele. Se ele tiver uma força superior à tua, evita-o."* (Tzu, 2006 p. 69) *"E se assim conseguirmos atacar uma força inferior com uma superior, os nossos adversários ficarão numa posição extremamente difícil."* (Tzu, 2006 p. 103)	*"Procura-se um ponto da posição do inimigo, ou seja, uma secção das suas tropas (uma divisão ou um corpo), e atacamo-lo com grande superioridade,…"* (Clausewitz, 2003 p. 44)
Economia de Forças	*"O controlo de uma grande força obedece ao mesmo principio do que o controlo de alguns homens: é apenas uma questão de os dividir."* (Tzu, 2006 p. 91)	*"Se formos muito fracos, devemos empenhar poucas das nossas forças nos outros pontos, de forma a que nos possamos apresentar o mais fortes que for possível no ponto decisivo."* (Clausewitz, 2003 p. 44)

Princípios actuais	Pensamentos	
	Pensamento de Sun Tzu	**Pensamento de Carl von Clausewitz**
	"Para que o impacto do teu exército possa ser como uma mó esmagando um ovo, deves recorrer á ciência dos pontos fracos e fortes." ' (Tzu, 2006 p. 93)	
Manobra	*"Ataca-o onde ele não está preparado, aparece onde não és esperado."* (Tzu, 2006 p. 70) *"Vencerá aquele que tiver aprendido o artifício do desvio. Esta é a arte da manobra."* (Tzu, 2006 p. 115)	
Unidade de Comando	*"Na guerra, o general recebe as suas ordens do soberano."* (Tzu, 2006 p. 109) *"Depois de ter reunido um exército e concentrado as suas forças, ele deve combinar e harmonizar os seus diferentes elementos antes de montar acampamento."* (Tzu, 2006 p. 109)	
Segurança	*"Podes avançar e ser absolutamente irresistível, se te dirigires aos pontos fracos do inimigo; podes retirar e estar a salvo de perseguição se os teus movimentos forem mais rápidos do que os do inimigo."* (Tzu, 2006 p. 102)	
Surpresa	*"Toda a guerra é baseada no engano"* (Tzu, 2006 p. 69)	*"Um dos princípios mais importantes da guerra ofensiva consiste em surpreender o inimigo. Quanto maior for o efeito de surpresa do nosso ataque, mais afortunados seremos."* (Clausewitz, 2003 p. 48)
Simplicidade	*"Por isso, o bom combatente será terrível no ataque e rápido na decisão."* (Tzu, 2006 p. 95)	

APÊNDICE B - TRANSCRIÇÃO DA ENTREVISTA DO EXMO. GENERAL DOUTOR LOUREIRO DOS SANTOS

Entrevistador: "Boa tarde meu General! Desde já agradeço a sua disponibilidade para a realização desta entrevista. A entrevista que lhe pretendo realizar enquadra-se na temática da Ciberguerra. Sendo que o tema do meu trabalho é: "A Guerra no Ciberespaço: Princípios da Guerra clássica aplicados na Ciberguerra" onde pretendo obter o seu ponto de vista em algumas das questões fundamentais para o meu estudo.

O tempo previsto para a realização da entrevista não excederá mais de 60 minutos. Solicito assim, a sua participação neste trabalho e, peço autorização para efectuar a gravação da entrevista. Os dados obtidos com a realização desta entrevista, serão exclusivamente utilizados para fins académicos.

Aceita participar neste estudo?"

Entrevistado: "Sim, aceito."

Entrevistador: "Meu General, o que é para si a Ciberguerra? Será que me pode dar uma possível definição de Ciberguerra?"

Entrevistado: "Ora bem, com o desenvolvimento tecnológico nestes últimos tempos, especialmente a partir dos anos 70/80, começando pela aplicação tecnológica da APARNET nas Forças Armadas Norte Americanas, surgiu um novo espaço de operações. Tradicionalmente, desde a antiguidade, existiam dois espaços de operações - espaços onde se desenvolviam os combates: o espaço marítimo e o espaço terrestre. Nos princípios do século XX, surgiu um novo espaço operacional, (o espaço já existia, mas não se combatia nele), o espaço aéreo. A partir dessa altura, devido ao desenvolvimento tecnológico, isto porque é sempre a tecnologia que origina isso permitindo progressos na maneira do homem dominar o material, conseguiu combater no Ar. Ou seja, surgiu um terceiro espaço, o espaço aéreo. Que já pode ser considerado actualmente como um dos espaços de operações tradicionais.

Mais tarde, no final do século XX, por volta dos anos 60/70 surge, embora ele também já existisse, o espaço exterior como novo espaço de operações - o espaço que está além do espaço aéreo, onde se encontram os satélites. Um sonho da humanidade que começou a ser concretizado na segunda metade do século XX. Aumentou de tal forma a importância desse espaço exterior, com os vários utensílios que nele giram (indispensáveis para fazer a guerra nos teatros de operações tradicionais - o GPS por exemplo), que se tornou admissível e possível fazer a guerra nesse espaço exterior. As grandes potências estão a

preparar-se para, no caso de haver uma guerra de grande intensidade, derrubar os satélites do adversário. Embora haja já alguns acordos, por exemplo um acordo patrocinado pelas Nações Unidas pelo qual é proibido colocar nele armas nucleares. Mas o espaço exterior é ainda um espaço muito em desordem: enquanto no espaço aéreo há uma série de tratados que regulam como os aviões andam e há toda uma estrutura de coordenação, no espaço exterior as coisas que ainda não estão resolvidas. A Rússia e a China têm proposto várias vezes aos EUA que avancem para negociações nesse sentido, mas os EUA não têm dado resposta. A ideia que tenho é que os EUA querem primeiro pôr no espaço aquilo que acham que precisam de lá pôr.

Nos finais do século XX, surge o Ciberespaço, que é um espaço virtual, mas indispensável para suportar o funcionamento das sociedades e, digamos assim, à circulação da informação. Quer dizer, hoje em dia, as sociedades não são imagináveis sem os computadores e o Ciberespaço para distribuir energia, água, exercer as funções de governo, finanças, etc. O que as torna muito vulneráveis.

Em todo o local útil para o Homem, em todos os espaços onde se encontram elementos que o Homem pode utilizar, há choque de interesses, portanto ocorrem conflitos, o que implica que neles se pode combater. O que é combater? Um actor combate para fazer com que os outros actores façam aquilo que ele quer que eles façam. Muitas vezes têm que utilizar a força, mas, normalmente primeiro, procuram persuadi-lo, ou seja, utilizam acções que não envolvam a violência, mas, a certa altura vê-se obrigado a utilizar mesmo a violência para que o outro faça aquilo que ele quer, que lhe interessa que ele faça - portanto há guerra.

A partir do momento que o Ciberespaço adquiriu esta importância para a vida das sociedades, para a vida moderna, para tudo, incluindo as Forças Armadas, então combate-se no Ciberespaço. Quem o utiliza para outras coisas que lhe são úteis, também o utiliza para combater. Se os combates que se fazem nesse espaço visam fins políticos, (visam impor ao outro a nossa vontade, sejamos um actor estatal ou não), podem travar-se guerras no Ciberespaço.

Assim como pode haver Crime. O Cibercrime que não chega ao patamar da guerra, porque não atinge o colectivo, não atinge um outro actor, estatal ou não estatal, um actor político. Limita-se a procurar lucros ilícitos. Logo, no Ciberespaço também há acções policiais.

Concluindo, a Ciberguerra é o conjunto de acções que é possível fazer no Ciberespaço, para obrigar um actor político a agir da forma que o actor que desencadeia essas acções pretende."

Entrevistador: "O que é para si o Ciberespaço? Será que me pode dar uma possível definição de Ciberespaço?"

Entrevistado: "O Ciberespaço é o espaço virtual, gerado pelos elementos tecnológicos dos computadores, toda essa área da informática onde se efectuam interacções entre as pessoas, organizações ou países, de toda a natureza - interacções económicas, sociais, politicas. Um espaço virtual, sustentado, apoiado, gerado por tecnologias novas de informação e comunicação.

O seu aparecimento marca o início da Era da Informação que, com todos esses ingredientes, originou uma revolução na forma de fazer a guerra.

Em qualquer desses espaços, pode haver operações próprias. Mas todas as guerras em qualquer espaço, tradicional ou não, são afectadas e ampliadas pelo espaço mediático e pelo ciberespaço. O espaço exterior apenas entra como elemento apoiante, porque, se forem derrubados os satélites que existem no Espaço, o espaço mediático quase que deixa de funcionar, além de outras consequências. De facto, estamos em presença de dois espaços virtuais. O que é curioso é que é o virtual está a dominar o real. Por exemplo, os militares israelitas, por melhor que actuem a combater os terroristas, arriscam-se a perder as guerras, por causa daquilo que se passa no espaço virtual, particularmente no espaço mediático através da gestão das percepções, numa guerra de persuasão. No fundo, tudo se baseia na gestão das percepções, para que as opiniões públicas pensem que eu é que tenho razão… e isso tem resultados estratégicos.

Tu entras nesse mundo novo… tu começas a ser militar responsável, exactamente numa época fantástica, porque é uma época que não tem exemplos do passado. Tu olhas para o passado e tens muita dificuldade em encontrar uma realidade que seja semelhante à realidade com que te vais confrontar daqui para a frente."

Entrevistador: "Meu General, temos exemplos de conflitos aos quais podemos designar de Ciberguerra? Se sim, quais?"

Entrevistado: "Sim, claro. Já há exemplos disso, já aconteceu Ciberguerra, A Ciberguerra não está ainda institucionalizada em termos de direito internacional e isso é um problema terrível e vai criar problemas terríveis. Mesmo na área da violência organizada, no uso das forças militares, há zonas ambíguas, não se sabendo se uma determinada acção é uma guerra ou não. Na área da Ciberguerra, ainda não há nada sobre isso, nem sabemos quando haverá. Mas começa a pôr-se essa questão: até que ponto um ataque maciço às infra-estruturas críticas de um Estado, obrigando-o a ajoelhar-se, neutralizando-o constitui ou não uma agressão? Uma agressão que não se pode dizer seja uma agressão armada, mas é uma agressão de outra natureza, corresponde, em termos de direito internacional, exactamente à mesma realidade do que seria uma acção conjunta das forças militares?
Tem havido acções de Ciberguerra. O exemplo que se costuma utilizar e que, no meu ponto de vista, irá ser o tipo de guerra na nossa era da informação, foi a guerra dos cinco dias

entre a Rússia e a Geórgia. As guerras mais comuns do nosso tempo serão, por um lado, guerras de insurreição, as guerras subversivas do género daquelas que se estão a passar em quase toda África, no Afeganistão, no Iraque, que são guerra assimétricas. E depois as guerras que podem ser convencionais, frequentemente dissimétricas, serão guerras normalmente limitadas no tempo e no espaço, porque, hoje em dia, as sociedades são tão frágeis que não aguentam guerras de destruição muito grande, pois ficariam completamente destruídas e paralisadas e provocariam danos terríveis, como aconteceu só com o furacão catrina no Haiti. Portanto, serão guerras muito curtas, mas precedidas por uma a barragem de ataques cibernéticos (a preparação da guerra). Na guerra convencional do passado, a preparação era feita com ataques aéreos, artilharia, morteiros, para amolecer o adversário, para fazer com que o inimigo, quando receber o choque da infantaria e da cavalaria, portanto, o choque da manobra, não esteja em grandes condições de resistir. Ora, nas guerras previsíveis, como aconteceu na Geórgia, a preparação será um ataque maciço informático. Durante esta preparação cibernética, praticamente a Geórgia ficou paralisada - os seus sistemas financeiros paralisados, o governo não tinha capacidade de trabalhar, as próprias forças armadas, todos os sistemas de comunicações. Só quando os instrumentos fundamentais da sociedade georgiana, as suas infra-estruturas críticas que são o governo, forças armadas, sistemas financeiros, de segurança, etc… distribuição de energia estavam quase paralisados então é que veio o ataque militar.

Entrevistador: “O caso da Estónia poderá ser considerado uma Ciberguerra?”

Entrevistado: “Pode ser ou não. Uma das hipóteses que se põe é que seja uma acção do exterior para fomentar um problema interno, porque como sabes, tinha havido uma reacção muito forte da minoria Russa, que é bastante grande, à mudança de uma estátua do soldado soviético de uma praça para um cemitério. E então houve uma série de problemas, como grandes manifestações, e tiveram de actuar as forças da ordem da Estónia. Claro que houve gente que disse que a minoria estava a ser acicatada pela Rússia, porque a Rússia nunca engoliu muito bem que a estónia tenha aderido à *OTAN*, porque a Estónia é um estado báltico que pertenceu à própria Rússia, portanto é natural que se possam fazer essas deduções. Agora, o curioso, é que os computadores que desencadearam os ataques sobre as infra-estruturas críticas da internet da Estónia, eram computadores dos E.U.A. porque é possível detectar de onde vieram os ataques, tendo-se chegado à conclusão que vinham de computadores americanos, isto é, alguém pôs os Botnets nos computadores americanos, em milhares de computadores americanos, e a, dada altura, deram a ordem de ataque à Estónia. Não sabemos quantos milhares de computadores em Portugal estão prontos para disparar em qualquer direcção, se algum País nos está a utilizar para isso. Isto pode acontecer. É claro que aos E.U.A ninguém acusou de serem os autores desses ataques. O

que se chegou a pensar é que seria a Rússia, mas não há provas. Estes ataques, já estavam preparados. Ou seja, uma série de milhões de computadores em todo o mundo estão mais ao menos sincronizados para, na altura própria, dispararem ataques a mando de alguém, sendo que esse alguém será, tal como foi impossível provar que foi a Rússia que lançou os ataques à Estónia. É de facto uma coisa complicada."

Entrevistador: "Estão os Estados preocupados com esta nova tipologia de Guerra? Se sim, que medidas estão a ser tomadas? Por exemplo nos Estados Unidos da América? Ao nível da OTAN? E em Portugal?"

Entrevistado: "Estão preocupados… todos o Estados estão a tentar organizar e a melhorar nesta área. Por exemplo, os Estados da *OTAN* têm regulamentos e JP's da *OTAN*, manuais que falam, que indicam, estabelecem regras para combater no ciberespaço. Há um Centro de Excelência na Estónia da *OTAN*, alias, foi criado na Estónia porque depois das acções contra o Estado na Estónia começou-se a dedicar-se e a aperfeiçoar-se nesta área e foi lá que foi criado este Centro.

Todos os países estão a apostar nisto. Os E.U.A de certa forma são aqueles, como País mais poderoso da *OTAN*, têm a iniciativa, aponta as grandes linhas de acção neste domínio, e já criaram recentemente uma organização para a Ciberguerra. Um comando para a Ciberguerra no Pentágono e uma agência para a cibersegurança na Casa Branca, o Czar. Porque não é só nas forças armadas que é necessário agir. É preciso também guardar e defender toda a área da Internet, computadores que existem no Governo, nas grandes empresas estratégicas, os Bancos, etc… todas essas organizações se devem defender por si próprias. Mas terá de haver uma direcção integradora de esforços ao nível de cada Estado. Por exemplo, cá em Portugal, a EDP é das empresas que está mais avançada nesta área da segurança, dos seus computadores, aplicações informáticas. No entanto, não pode ser só uma empresa a estar bem e as empresas ao lado estarem mal, porque, se estiver mal por exemplo a rede de transportes, um ataque à rede de transportes poderá influenciar as restantes infra-estruturas. Todos os países estão a tentar melhorar nesta área, que consideram fundamental, e será uma área chave nos conflitos que tiverem que travar.

Portugal tem tido alguma dificuldades… como sempre não é? Infelizmente, normalmente, só reagimos? Desde o Afonso Henriques, reagíamos, e bem, quando acicatados. A Ciberguerra é uma coisa que ainda não se sente. E tem havido algumas dificuldades. Nas forças armadas estamos a trabalhar nisso. No Exército, como sabes, temos cursos, como o mestrado em guerra da informação. Foi constituída uma associação, à qual eu pertenço, de que é presidente o general Coimbra (director de formação do Exército neste momento), que já tem uma certa capacidade de intervenção. É uma associação que está ligada a esses assuntos. As empresas por si só estão a trabalhar, por

exemplo a EDP, que é das mais avançadas. Mas nos bancos, nas redes de transportes, enfim em todas as grandes empresas existem meios de segurança. Falta criar uma estrutura de controlo. O TCor Paulo Viegas Nunes já apresentou uma proposta neste sentido. A sua proposta parece-me correcta, mas tenho afirmado que, antes de implantar essa estrutura, para ganhar tempo, até para sensibilizar todos os responsáveis para esta questão, porque isso só será implementado, quando os responsáveis políticos tiverem consciência da sua necessidade. É preciso sensibilizá-los. Para isso, seria conveniente criar qualquer coisa para o fazer. da minha proposta avança em dar às forças armadas a responsabilidade de "pilotar" o arranque, com a coordenação do Governo e com as diversas áreas do Estado interessadas, as empresas etc… para assim caminharmos para a tal estrutura, em que o elemento central de coordenação terá de estar no governo, com as várias estruturas críticas coordenadas, embora cada uma delas com as suas estruturas próprias."

Entrevistador: "Que tipos de actores é que poderão ser alvo destes ataques de Ciberguerra?

Entrevistado: "Em termos de Ciberguerra, só são há guerra quando estão em acção actores políticos. Quando há fins políticos. Portanto, os actores que podem ser alvo são os Estados. Os actores que podem desencadear podem ser estados e actores não estatais. É perfeitamente possível que um conjunto de hackers pode visar certos objectivos. Os estados têm maior capacidade para, por si só, organizar uma espécie de um ataque coordenado. Todos os países estão a dar uma grande importância a esta nova forma de fazer a guerra.

Quando nós estamos a falar em guerra, estamos a falar em Estados; só há guerra quando participam um ou muitos Estados. Se não participar nenhum Estado não há guerra, há sim outro tipo de confronto. Crimes, há ataques, mas que não fazem parte da Guerra. Do ponto de vista do Direito Internacional não são guerras.

O desenvolvimento tecnológico e o funcionamento da sociedade, que é mais fácil, mais cómodo, mais eficiente quando apoiado neste tipo de tecnologia, cria uma vulnerabilidade. A sua sustentação online pode ser atacada, ameaçando o seu funcionamento. Mas se houver um ataque intencional, por parte de um Estado ou outro actor político (actores não Estatais, por exemplo Al-Qaeda), com objectivos políticos, estamos na Guerra. Se não for, por exemplo cidadãos que o façam para alcançar objectivos ilícitos, estaremos perante um crime, e o crime está tipificado."

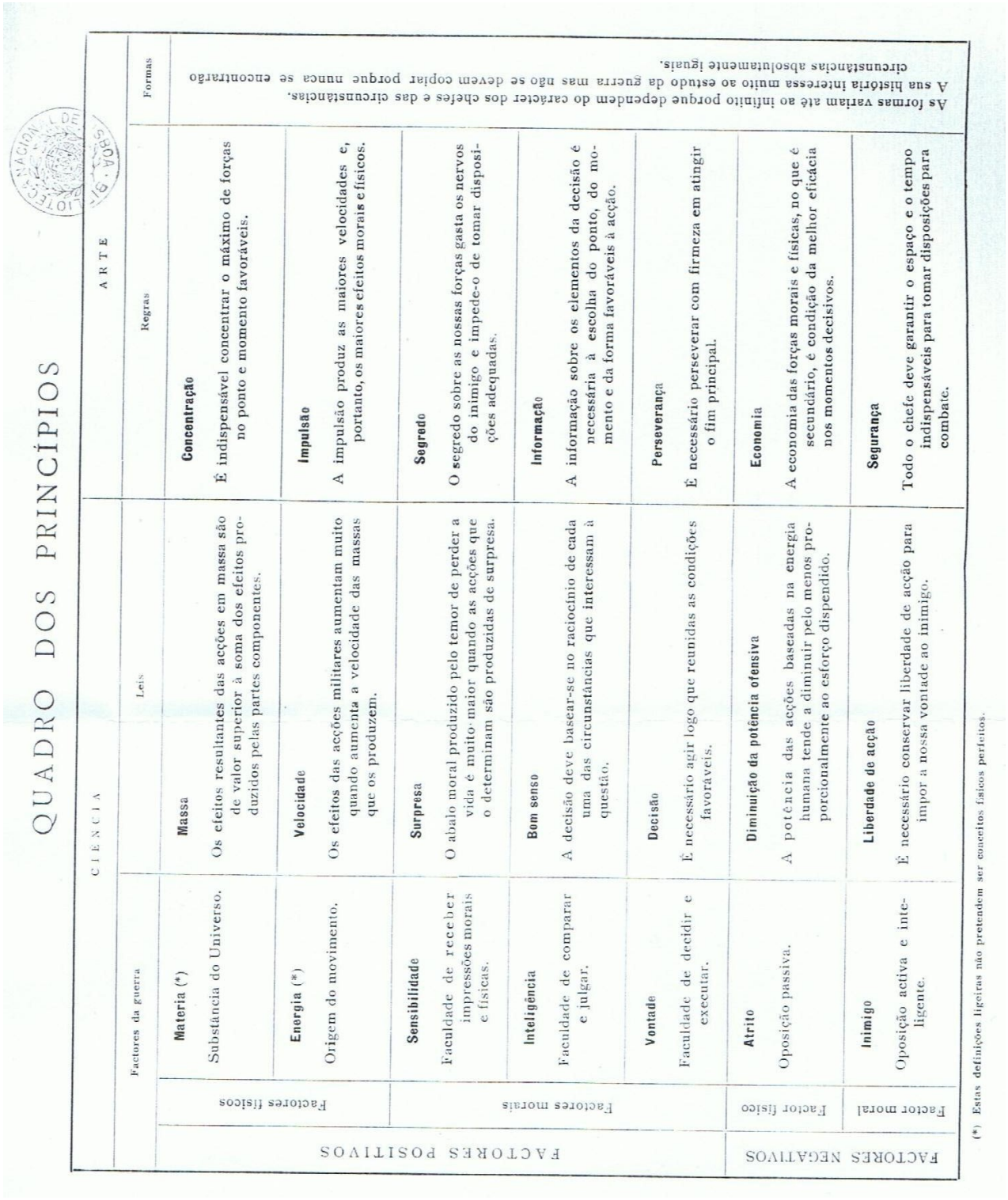
Entrevistador: "No seu ponto de vista os 9 Princípios da Guerra continuam actuais e deverão ser tido em conta para os Comandantes no planeamento, porventura numa acção de Ciberguerra?"

Entrevistado: “Acho, que a resposta a essa pergunta tem que se dada por um especialista, mas agora penso que, genericamente, se aplicarão.

O princípio da simplicidade aplica-se a tudo, não se aplica só à guerra. Quer dizer, as coisas quanto mais simples forem para produzir determinado tipo de resultados, mais eficiência terão. O princípio do objectivo também se aplica a tudo. Quando queremos fazer qualquer coisa, temos que eleger um objectivo; como sabes, as empresas foram buscar aos nossos manuais, nomeadamente os que abordam os princípios da guerra, para os aplicarem na gestão e actuação empresarial. Já há manuais que falam sobre isso, sobre a estratégia militar aplicada às empresas. Portanto a minha ideia é que os grandes princípios da guerra, o princípio da economia de forças, do objectivo, o princípio da surpresa, da simplicidade… se aplicarão à guerra no ciberespaço. Parece evidente que, se conseguirmos criar a surpresa num ataque no Ciberespaço, desequilibraremos o adversário. Portanto, se for possível desencadear um ataque surpreendendo o adversário, um ataque com que ele nunca contaria, conseguiremos uma vantagem mais nítida do que se o adversário estivesse a contar com ele.”

ANEXOS

ANEXO A - QUADRO DOS PRINCÍPIOS DO EXMO. GENERAL LOPES DA SILVA



QUADRO DOS PRINCÍPIOS

	Factores da guerra	CIÊNCIA — Leis	ARTE — Regras	Formas
FACTORES POSITIVOS — Factores físicos	**Materia (*)** Substância do Universo.	Os efeitos resultantes das acções em massa são de valor superior à soma dos efeitos produzidos pelas partes componentes.	**Concentração** É indispensável concentrar o máximo de forças no ponto e momento favoráveis.	As formas variam até ao infinito porque dependem do carácter dos chefes e das circunstâncias. A sua história interessa muito ao estudo da guerra mas não se devem copiar porque nunca se encontrarão circunstâncias absolutamente iguais.
	Energia (*) Origem do movimento.	Os efeitos das acções militares aumentam muito quando aumenta a velocidade das massas que os produzem.	**Impulsão** A impulsão produz as maiores velocidades e, portanto, os maiores efeitos morais e físicos.	
FACTORES POSITIVOS — Factores morais	**Sensibilidade** Faculdade de receber impressões morais e físicas.	O abalo moral produzido pelo temor de perder a vida é muito maior quando as acções que o determinam são produzidas de surpresa.	**Surpresa** **Segredo** O segredo sobre as nossas forças gasta os nervos do inimigo e impede-o de tomar disposições adequadas.	
	Inteligência Faculdade de comparar e julgar.	A decisão deve basear-se no raciocínio de cada uma das circunstâncias que interessam à questão.	**Bom senso** **Informação** A informação sobre os elementos da decisão é necessária à escolha do ponto, do momento e da forma favoráveis à acção.	
	Vontade Faculdade de decidir e executar.	É necessário agir logo que reunidas as condições favoráveis.	**Decisão** **Perseverança** É necessário perseverar com firmeza em atingir o fim principal.	
FACTORES NEGATIVOS — Factor físico	**Atrito** Oposição passiva.	A potência das acções baseadas na energia humana tende a diminuir pelo menos proporcionalmente ao esforço dispendido.	**Diminuição da potência ofensiva** **Economia** A economia das forças morais e físicas, no que é secundário, é condição da melhor eficácia nos momentos decisivos.	
FACTORES NEGATIVOS — Factor moral	**Inimigo** Oposição activa e inteligente.	É necessário conservar liberdade de acção para impor a nossa vontade ao inimigo.	**Liberdade de acção** **Segurança** Todo o chefe deve garantir o espaço e o tempo indispensáveis para tomar disposições para combate.	

(*) Estas definições ligeiras não pretendem ser conceitos físicos perfeitos.

Fonte: (Silva, 1952)

ANEXO B - PRINCÍPIOS DA GUERRA EM PORTUGAL

CAPITULO 3

PRINCIPIOS DA GUERRA E POTENCIAL DE COMBATE

SECÇÃO I - PRINCÍPIOS DA GUERRA

301. **Generalidades**

a. Os Princípios da Guerra são normas de acção fundamentais que devem ser respeitadas na conduta da guerra para permitir e facilitar o êxito na prossecução da mesma. A sua adequada aplicação é essencial ao exercício do comando e à condução, com sucesso, das operações militares. Os princípios da guerra estão relacionados entre si e, conforme o caso, podem tender para mutuamente se reforçarem ou se oporem. Consequentemente, o grau de aplicação de um determinado princípio variará com a situação.

b. Os Princípios da Guerra considerados na doutrina nacional são os seguintes:

- Objectivo
- Ofensiva
- Massa
- Economia de forças
- Manobra
- Unidade de comando
- Segurança
- Surpresa
- Simplicidade.

302. **Principio do Objectivo**

O objectivo militar último da guerra é o aniquilamento das forças armadas do adversário e da sua vontade de combater.

O objectivo de toda e qualquer operação militar deverá contri-

buir para o obtenção daquele objectivo último. Para que assim aconteça são normalmente atribuídos às forças militares objectivos intermédios cuja consecução simultânea ou sucessiva consubstancia a obtenção do objectivo da operação militar.
Os objectivos atribuídos às forças militares devem ser definidos de uma forma clara e inequívoca. Devem ser suficientemente importantes para, por si só, contribuírem para a consecução do objectivo do escalão imediatamente superior. E devem ser exequíveis, isto é, susceptíveis de serem alcançados pelas forças e com os meios a elas destinados.
A escolha de um objectivo deve ser feita em função da missão, dos meios disponíveis, do inimigo e das características da área de operações. Se o objectivo for correctamente definido, de acordo com os parâmetros atrás indicados, o Comandante deverá orientar toda a sua acção para o atingir, não se afastando nunca da sua consecução **permanência no objectivo**.

303. **Principio da Ofensiva**

A acção ofensiva é necessária para se obterem resultados decisivos e para conservar ou reconquistar a liberdade de acção. Permite ao Comandante tomar a iniciativa, impor a sua vontade ao inimigo, marcar o ritmo e influenciar o curso da batalha e explorar os pontos fracos do inimigo.
Um Comandante pode ser obrigado pelo inimigo e remeter-se a uma atitude defensiva ou pode adoptá-la deliberadamente, quer para ganhar tempo a fim de reorganizar as suas forças e aguardar uma oportunidade mais favorável para passar à ofensiva, quer para economizar forças num determinado local da frente onde não se procura obter a decisão. Porém, mesmo nestes casos, o Comandante deve explorar todas as oportunidades de, por meio de acções ofensivas, obter a iniciativa e alcançar resultados decisivos.

304. **Principio da Massa**

A fim de alcançar o sucesso, deve empregar-se um potencial de combate superior ao do inimigo no local e no momento decisivo.
Essa superioridade obtém-se combinando apropriadamente os vários meios disponíveis.
A aplicação correcta do **Principio da Massa**, em conjugação com outros princípios, pode permitir que forças numericamente inferiores no seu conjunto, obtenham uma superioridade local e momentânea, decisiva para o desenrolar das operações.

305. **Principio da Economia de Forças**

O princípio da **Economia de Forças**, é um corolário do princípio da massa. Para se concentrar, num local, um elevado potencial de combate, deverá conseguir-se a economia de forças noutros locais. Por-

tanto, o Comandante deverá procurar cumprir a sua missão através ,do emprego judicioso dos meios à sua disposição, reduzindo ao mínimo o desgaste desses meios e procurando empregá-los de forma decisiva no local e momento mais adequados.
Tal não implica uma atribuição sistematicamente parcimoniosa dos meios mas, antes, uma distribuição judiciosa do potencial de combate disponível pela acção principal e pelas acções secundárias, a fim de se obter um potencial de combate adequado no ponto onde se procura a decisão.

306. **Princípio da Manobra**

A finalidade da **Manobra** consiste em dispor uma força de forma tal que o inimigo fique colocado numa situação desvantajosa e assim conseguirem-se resultados que, de outra forma, exigiriam um maior dispêndio de homens e de material.
A manobra permite a correcta aplicação dos princípios da massa e da economia de forças, concentrando num ponto forças disponíveis doutros locais e reduzindo assim a vulnerabilidade do diapositivo nos locais e momentos decisivos. Contribui para conservar a liberdade de acção, para manter a iniciativa e para explorar os resultados do combate.

307. **Princípio da Unidade de Comando**

A aplicação decisiva do **Potencial de Combate** disponível, através da manobra e visando a conjunção dos princípios da economia de forças e da massa, exige uma acção coordenada de todas as forças por forma a fazerem convergir os seus esforços tendo em vista um objectivo comum. Essa coordenação só é possível se existir unidade de doutrina e de comando a orientarem a acção das diferentes forças:
A forma de melhor garantir essa **Unidade de Comando**, aconselha a investir num único. Comandante a autoridade necessária.

308. **Princípio da Segurança**

A **Segurança** é essencial à conservação do potencial de combate, bem como à exploração; com sucesso, da capacidade de manobra das forças por forma a. concentrá-las no local e momento adequados.
Através da segurança garante-se a conservação da liberdade de acção, nega-se ao inimigo a possibilidade de obter informações sobre as forças amigas e os seus planos e evita-se ser surpreendido, pelo adversário.
A aplicação do princípio da segurança não exclui a necessidade de se correrem riscos calculados, característicos da guerra. Não é, portanto, incompatível com a adopção do princípio da ofensiva, o qual, visando a iniciativa, limita ao inimigo a capacidade de interferir nas nossas acções.

309. **Princípio da Surpresa**

A **Surpresa** consiste em criar uma situação inesperada, para a qual o inimigo não esteja em condições de reagir eficazmente em tempo oportuno. Visa retirar ou limitar a liberdade de acção do adversário, impedindo-o de manter a iniciativa e colocando-o, sempre que possível, em posição de desvantagem. Pode, por si só, modificar decisivamente o Potencial Relativo de Combate, permitindo obter êxitos altamente compensadores, relativamente aos esforços despendidos.
Entre outros factores, contribuem para a surpresa: a velocidade, a decepção, a concentração inesperada de forças num dado local e momento, uma informação e contra-informação eficientes e a variação de processos tácticos e dos métodos de actuação.
A surpresa facilita a manobra, estimula a ofensiva e favorece a segurança.

310. **Princípio da Simplicidade**

Os planos devem ser simples e os objectivos e as ordens claras e concisas, a fim de se reduzirem as dificuldades de interpretação e as possibilidades de confusão.
Uma demasiada complexidade da manobra pode contribuir para lhe retirar eficácia, conduzindo mesmo, eventualmente, ao insucesso.

Fonte: (RC 130-1 , 1987)

ANEXO C - LISTA DE INFRA-ESTRUTURAS CRITÍCAS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

Fonte: (Livro Verde, 2005 p. 25)