DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

MESTRADO EM ESTUDOS DA PAZ E DA GUERRA NAS NOVAS RELAÇÕES INTERNACIONAIS

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

A CIBERNÉTICA NA DEFESA DA INTEGRIDADE DOS ESTADOS. AS POSSIBILIDADES PORTUGUESAS, NO SEIO DA OTAN, NO DOMÍNIO DA CIBERDEFESA

Dissertação para a obtenção do grau de Mestre em Estudos da Paz e da Guerra nas Novas Relações Internacionais

Autor: Carlos Manuel Ferreira de Passos

Orientadores: Professor Doutor Luís José Rodrigues Leitão Tomé

Professor Doutor Luís Manuel Alves de Fraga

Número do candidato: 20160852

Fevereiro de 2020

Lisboa

Dedicatória

Procuro a excelência que vejo em
vocês os três, Inês, Fábio e André

Agradecimentos

Esta dissertação foi um objetivo de há muito, concluída hoje. Tendo sido um trabalho de um, teve aqui e ali, um incentivo, um apoio, uma colaboração, uma ajuda, de muitos a quem quero agradecer.

Em primeiro lugar agradecer ao meu orientador, Professor Doutor Luís Alves Fraga, que desde o projeto até à dissertação sempre me orientou, corrigindo sem me desmotivar, apoiando e motivando sempre. Ao meu coorientador, Professor Doutor Luís Leitão Tomé, que com o seu rigor me obrigou a dar sempre mais.

A todos os meus colegas de Mestrado pelo apoio e amizade, em especial ao Pedro Bernardino pela disponibilidade e colaboração. Ao TCOR José Dinis, pelas horas de discussão sobre a temática, pela disponibilidade sempre presente e pelos seus conselhos e ensinamentos. Ao Major Nuno Goes, pelo apoio e pelas afinações facultadas que tão úteis foram. Quero igualmente agradecer a toda a minha equipa da Direção dos Sistemas de Informação, da Defesa Nacional, e em especial aos meus colaboradores diretos que me ajudaram a ganhar tempo, liderando e gerindo os difíceis projetos que tínhamos em execução "dando-me tempo" e libertando-me para a consecução deste objetivo. Sem vós, teria sido muito mais difícil.

Quero também agradecer à minha família e amigos pelo apoio incondicional que me deram ao longo deste caminho.

Acabo com três agradecimentos especiais: à minha irmã Paula, a alegria e o orgulho que manifestas, por me veres atingir este estágio, faz-me sentir um privilegiado e personificas tudo aquilo que os nossos pais sentiriam nesta ocasião; aos meus filhos Fábio e André, a vossa excelência como estudantes e o sucesso que têm atingindo nas vossas carreiras são um alento para que eu nunca pare de tentar chegar sempre mais longe; à minha mulher Inês, o teu patamar de excelência como pessoa é algo que muitos almejam, mas que poucos conseguem atingir. O meu profundo obrigado pelo teu amor, partilha, companheirismo e apoio incondicional. Tem sido um enormíssimo prazer percorrer a estrada da vida ao teu lado.

A todos O meu Obrigado

Resumo

Embora Portugal não seja um key player na Organização do Tratado do Atlântico Norte (OTAN), face às suas carências armamentistas, tem uma oportunidade única de qualificar melhor as suas estruturas e pessoal militar, no domínio da defesa cibernética, promovendo uma cultura de excelência, neste domínio, assegurando uma posição de destaque no seio da Aliança.

A capacidade armamentista portuguesa é reduzida, e no seio da OTAN, Portugal ocupa o modesto 19.º lugar entre os 27. Mesmo comparado com países congéneres, como a Bélgica, a Holanda e a Dinamarca, países de média dimensão europeia, fundadores da OTAN e membros da União Europeia (UE) e da Organização das Nações Unidas (ONU), Portugal continua a não ter uma posição de destaque.

Entretanto existe um novo domínio no teatro de operações militares – o ciberespaço, que se caracteriza como o sistema do caos, com um carácter de desterritorialização e omnipresente, sendo tão crítico para a defesa nacional e internacional quanto os domínios clássicos da terra, do mar, do ar e do espaço sendo por isso apelidado como o quinto domínio das operações militares.

Assim, a juntar à imensa massa crítica e conhecimento que existe em Portugal sobre o ciberespaço e alavancado com a relocalização da NATO Communications and Information Systems School, de Latina (Itália) para Oeiras com a nova designação NATO Communications, Information and Cyber Academy, e fortalecido com a liderança do programa Smart Defence - Multinational Cyber Defence Education and Training Project, que prevê a criação de um currículo de Defesa Cibernética, que estabelecerá os fundamentos conceituais, doutrinais e didáticos do futuro trabalho da Academia, Portugal tem uma oportunidade única para construir um Centro de Excelência Nacional na área da Educação, Formação e Treino nos domínios da Cibersegurança e Ciberdefesa. Este polo, funcionando como Knowledge Hub, desenvolverá uma estreita ligação com a Academia, Indústria e outros espaços de inovação nacionais e internacionais.

A investigação que conduziu à elaboração da dissertação, analisa como Portugal é um bom exemplo de como um pequeno país pode ter um papel importante na OTAN ao liderar uma área.

Palavras-chave: ciberdefesa; domínio da defesa cibernética; educação, formação e treino; quinto domínio.

Abstract

Although Portugal is not a key player in the North Atlantic Treaty Organization (NATO), given its armament shortage, it has a unique opportunity to improve its structures and military personnel in the field of cyber defence, promoting a culture of excellence in this field ensuring a prominent position within the Alliance.

The Portuguese armament capacity is reduced and within NATO, Portugal occupies a modest 19th place among the 27. Even compared to similar countries, such as Belgium, the Netherlands and Denmark, countries of medium European dimension, NATO founders and members of the European Union (EU) and the United Nations (UN), Portugal still does not have a prominent position.

However, there is a new domain in the theatre of military operations - cyberspace, which is characterized as the system of chaos, with a deterritorialization and omnipresent character, being as critical for national and international defence, as the classic domains of land, sea, air and space and is therefore called the fifth domain of military operations.

Thus, in addition to the immense critical mass and cyberspace knowledge that exists in Portugal, and leveraged with the relocation of NATO Communications and Information Systems School, from Latina (Italy) to Oeiras with the new name NATO Communications, Information and Cyber Academy, and strengthened by the leadership of the Smart Defence program - Multinational Cyber Defence Education and Training Project, which provides for the creation of a Cyber Defence curriculum, which will establish the conceptual, doctrinal and didactic foundations of the future work of the Academy, Portugal has a unique opportunity to build a Center of National Excellence in the area of Education, Formation and Training in the fields of Cybersecurity and Cyber Defence. This hub, acting as a Knowledge Hub, will develop a close link with the Academia, Industry and other national and international innovation spaces.

The research that led to the writing of this dissertation examines how Portugal is a good example of how a small country can play an important role in NATO in leading an area.

Keywords: cyber defence; domain of cyber defence; education, formation and training; fifth domain.

Índice

Lista de Quadros e Gráficos

Lista de Abreviaturas, Acrónimos e Siglas

BBC British Broadcasting Corporation

CCD Comando Cibernético de Defesa

CD TEXP Cyber Defence Training and Exercise Coordination Platform

CDP Capability Defence Plan

CEDN Conceito Estratégico de Defesa Nacional

CEE Comunidade Económica Europeia

CERN Laboratório Europeu de Física de Partículas

CFCS Center for Cyber Security

CNCS Centro Nacional de Cibersegurança

CNN Cable News Network

CPLP Comunidade dos Países de Língua Portuguesa

CSIRT Computer Security Incident Response Teams

Cybercom Cyber Command

CyOC Cyberspace Operations Center

DDGHM Destroyer/with AShM/with hangar/with SAM

DDoS Distributed Denial of Service

DGRDN Direção-Geral de Recursos da Defesa Nacional

DOD Departament of Defence

EMGFA Estado-Maior Genereal das Forças Armadas

EPO Escritório Europeu de Patentes

ESA Agência Espacial Europeia

EUA Estados Unidos da América

EUMTG EU Military Training Group

FBI Federal Bureau of Investigation

FFGHM Fire-fighting/frigate/with AShM (anti-ship missile) with hangar/with SAM (surface-to-air missile)

FMI Fundo Monetário Internacional

GCHQ Government Communications Headquarters

GFP Global Firepower

GNR Guarda Nacional Republicana

HTF/EUMTG Headline Gold Task Force/EU Military Training Group

IESD Índice de Economia e Sociedade Digital

IISS The International Institute for Strategic Studies

IoT Internet das Coisas

IRNA Islamic Republic News Agency

ISR Intelligence, Surveillance and Reconnaissance

LPM Lei da programação militar

MDN Ministério da Defesa Nacional

MFMS Manpower Fit-for-Military-Service

MISP Malware Information Sharing Platform

MIT Massachusetts Institute of Technology

MNCD2 Multinational Cyber Defence Capability Development

MNCDE&T Multinational Cyber Defence Education and Training

NATO North Atlantic Treaty Organization

NCISS Nato Communications and Information System School

NDPP NATO Defence Planning Process

NORDEFCO Nordic Defence Cooperation

NSA Agência de Segurança Nacional

OCCDCE OTAN Cooperative Cyber Defence Centre of Excellence

ONU Organização das Nações Unidas

OTAN Organização do Tratado do Atlântico Norte

P&D Pesquisa e desenvolvimento

PIB Produto Interno Bruto

PME Pequenas e médias empresas

PPS Purchasing Power Standard

RAF Royal Air Force

RCM Resolução do Conselho de Ministros

SEGNAC4 Normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática

SPIIN Sistema de Proteção da Infraestrutura de Informação Nacional

SSK Attack submarine with ASW (anti-submarine warefare) capability (hunter-Killer)

TERMA Fabricante dinamarquês de defesa aeroespacial

TIC Tecnologias da informação e comunicação

TOW Tube launched, Optically tracked and Wire command - link guied weapon system

UAV Unmanned Aerial Vehicle

UE	União Europeia
UE-FMI	União Europeia e Fundo Monetário Internacional
UK	United Kingdom
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol

1. Introdução

O facto de o mundo se tornar cada vez mais interconectado e globalizado, torna-o cada vez mais "pequeno" em que tudo, ou quase tudo, interessa a todos, ou a quase todos e, por isso, ciberespaço, ciberdefesa, cibersegurança, ciberguerra e ciberataque são assuntos na ordem do dia e praticamente ninguém fica indiferente quando deles falamos.

O interesse em pesquisar e debater as possibilidades de Portugal no domínio da Ciberdefesa, no seio da OTAN, surgiu desde muito cedo, muito provavelmente devido ao currículo académico e militar, do autor, assim como, ao "normal" interesse sobre estes assuntos da cibernética. No entanto, a juntar a todo este interesse existe o orgulho patriótico, quase exacerbado, e à forte convicção, de que Portugal é um país de enormes potencialidades e que quando motivado e imbuído de um espirito nacionalista, é imparável e excelente entre os melhores.

Eis-nos então, perante o problema principal desta dissertação à qual procuraremos dar resposta, i.e., haverá condições para Portugal suprir as suas carências armamentistas do presente através do desenvolvimento cibernético?

De forma adjacente surgem outras questões para as quais pretendemos dar resposta durante esta dissertação. Assim, terá Portugal uma posição de relevo, na OTAN, no que à capacidade armamentista diz respeito? Será a Ciberdefesa um instrumento na área do armamento? Poderá Portugal criar condições, de cariz cibernético, para ser considerado um país indispensável em operações combinadas e conjuntas na OTAN?

Estes problemas conduzem-nos a um objetivo principal, tornando-o no nosso guia da investigação. Assim, iremos tentar demonstrar que, embora Portugal não seja um *key player*[1] na Organização do Tratado do Atlântico Norte (OTAN), face às suas carências armamentistas, pode ganhar relevância nessa organização criando doutrina e cultura estratégica de defesa cibernética e concomitantemente qualificar as suas estruturas e pessoal militar nesse domínio, de modo a se tornar um polo relevante e estratégico na rede de centros de excelência cibernéticos da OTAN.

Para isso e fazendo recurso ao método de abordagem dedutivo como metodologia de pesquisa para desenvolvimento da dissertação e utilizando o procedimento comparativo através de estudo de caso iremos dividir esta dissertação em três capítulos no seguimento desta introdução, seguidos das conclusões a que chegámos.

[1] Pessoa ou organização considerada importante em determinada área.

No capítulo imediatamente a seguir iremos tentar responder ao primeiro objetivo específico que consiste em avaliar e comparar a capacidade armamentista portuguesa face a alguns congéneres no âmbito da Aliança. Para esta comparação escolhemos a Bélgica, a Holanda e a Dinamarca, países de média dimensão europeia, fundadores da OTAN e membros da União Europeia (EU) e da Organização das Nações Unidas (ONU).

Por conseguinte e para uma melhor compreensão, iremos caracterizar genericamente os países em estudo, segundo determinados fatores, culminando naquele que é o mais importante para este trabalho – a sua capacidade militar. Para a consecução deste objetivo iremos utilizar 4 fontes principais, a *Global Firepower (GFP)*[2], *The World Factbook - Central Intelligence Agency*[3], *The International Institute for Strategic Studies (IISS)*[4] e *The Encyclopedia of the Nations*[5]. Ainda que pontualmente possamos fazer recurso a outras fontes, estas foram aquelas que em muita da bibliografia lida, no levantamento do estado da arte, eram referenciadas como basilares e por isso serem as fontes principais neste capítulo.

Enquanto *The World Factbook* e *The Encyclopedia of the Nations* nos ajudarão a caracterizar fatores como a geografia, economia, comunicações e ciência e tecnologia, no que aos valores militares diz respeito, as fontes principais serão a *GFP* e *The Military Balance* (2019) do *IISS*. A *GFP* avalia os valores individuais de cada país e, fazendo recurso a uma fórmula interna para gerar a pontuação, denominada *PwrIndx* (*PowerIndex*), estabelece as classificações *GFP* num determinado ano (o ano em referência será o de 2019) e o *The Military Balance* é uma avaliação oficial do *The International Institute for Strategic Studies* em relação às capacidades militares e da economia da defesa em todo o mundo.

Em seguida, e em outro capítulo, iremos tentar responder ao segundo objetivo específico que consiste em demonstrar que o ciberespaço, como sistema do caos, com um caráter de desterritorialização e omnipresença, é tão crítico para a defesa nacional e internacional quanto os domínios clássicos da terra, do mar, do ar e do espaço sendo por isso apelidado como o

[2] ***Global Firepower (GFP)*** é um site baseado em estatísticas, atualizado anualmente, que rastreia informações relacionadas com a defesa de 137 países e existe como um recurso totalmente independente.
[3] ***The World Factbook*** é organizado pela Agência Central de Inteligência (CIA) dos EUA. Os dados são recolhidos e coordenados tendo por base uma grande variedade de agências do governo dos EUA, bem como de centenas de fontes publicadas.
[4] ***The International Institute for Strategic Studies (IISS)*** produz dados independentes e relevantes para a política sobre conflitos. Este Instituto recolhe, analisa e valida continuamente dados de defesa de 173 países. O banco de dados digital, *Military Balance Plus,* permite aos utilizadores produzir gráficos à medida e empregar ferramentas analíticas avançadas para entender as tendências de defesa. Estão a desenvolver uma metodologia para medir o poder cibernético.
[5] ***The Encyclopedia of the Nations*** é uma fonte completa de informações detalhadas sobre cento e noventa e três países do mundo, tendo ainda informações sobre as Nações Unidas e as agências associadas e Líderes Mundiais.

quinto domínio das operações militares. Ao mesmo tempo, representa um desafio aos conceitos militares tradicionais em todos os níveis da guerra: estratégica, operacional e tática.

Hoje em dia, poucos são aqueles que são capazes de refutar a importância crescente do ciberespaço no mundo atual, quer seja nos negócios, nas telecomunicações, nas empresas, nas organizações públicas e privadas, na comunicação entre as pessoas, na cultura, na economia, em suma, em toda atividade em que estamos envolvidos diariamente o ciberespaço está presente.

Segundo *The Rt Hon Francis Maude MP Minister for the Cabinet Office and Paymaster General*, na introdução da publicação "Estratégia de Segurança Cibernética do Reino Unido", em 2012, "O crescimento da internet foi a maior mudança social e tecnológica da minha vida. É uma força enorme para o bem no mundo, na maneira como promove o crescimento, reduz as barreiras ao comércio e permite que pessoas de todo o mundo se comuniquem e cooperem. Como vimos nesta primavera no mundo árabe, pôde ajudar a dar voz ao inédito e responsabilizar os governos. Terá um papel enorme a desempenhar no apoio ao desenvolvimento sustentável nos países mais pobres. Ao mesmo tempo, a nossa crescente dependência do ciberespaço trouxe novos riscos, riscos que dados e sistemas importantes nos quais agora confiamos possam ser comprometidos ou danificados, de maneiras difíceis de detetar ou defender."[6]

Face a esta nova realidade, os ataques cibernéticos ganham espaço nesta "nova maneira de fazer guerra" muitas das vezes, ou quase sempre, sem rosto. "Todavia, a revolução tecnológica e digital em marcha desde finais do século passado está, indiscutivelmente, a transformar a economia, a sociedade e a maneira de fazer a guerra. Tanto quanto é possível avaliar hoje, a tendência é para que o ciberespaço – entendido como a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores – se transforme, também, numa nova dimensão dos conflitos internacionais. Apesar das dificuldades de avaliação das reais consequências de uma genuína ciberguerra, é de recear que estas possam ser bem destrutivas para o normal funcionamento de sociedades complexas."[7]

---

[6] GOV.UK. ***The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.*** Introduction by the Rt Hon Francis Maude MP, Minister for the Cabinet Office [Em linha]. 2011. [Consult. 03 nov. 2019]. Disponível em https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. (Tradução livre do autor)

[7] José Pedro Teixeira Fernandes. ***A ciberguerra como nova dimensão dos conflitos do século xxi.*** [Em linha]. 2012 [Consult. 24 nov. 2019]. Disponível em http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri33/n33a05.pdf

O primeiro grande ataque cibernético (ciberataque) foi em 2007 e teve a Estónia como alvo.

A relocalização da escultura do Soldado de Bronze, com a cabeça arriada, punho cerrado e vestindo o uniforme do Exército Vermelho, da Segunda Guerra Mundial, do centro de *Tallinn* para um canto silencioso de um cemitério nos arredores, ficou famosa, e acabaria por dar sequência ao primeiro ataque cibernético contra um país.

Decorria o dia 27 de abril de 2007 quando a Estónia começou a "sofrer" inúmeros ciberataques a diversos servidores da sua infraestrutura nacional de internet tendo como consequência a colocação de vários sítios governamentais fora de serviço.

A arma utilizada para estes ataques foi o *DDoS* (*Distributed Denial of Service*)[8] que se materializa em um computador *master* ter sob seu comando milhares de outros computadores e força esses computadores a executarem vários pedidos de serviço, a uma mesma hora, a um determinado servidor fazendo com que este colapse por incapacidade de atender a todos os pedidos. Estes ataques, para além de indisponibilizarem os sítios por um período de tempo, não causam danos permanentes. No entanto, expõem a vulnerabilidade que os sistemas ligados à Internet têm.

Este ataque serviu de aviso a todos os países, com serviços idênticos, pois poderiam vir a ser futuros alvos deste tipo de ataques cibernéticos.

Em consequência desse brutal ataque cibernético, os estónios não conseguiram usar os serviços financeiros de uso diário, como multibanco e serviços bancários online. Em termos estatais, houve ataques ao serviço do correio eletrónico e os funcionários do estado não puderam comunicar por *email*. Os jornais e os media, de repente, viram-se incapazes de transmitir as notícias. *Liisa Past,* editora da página de opinião de um jornal da Estónia, na época, lembra como repentinamente os jornalistas não podiam enviar os seus artigos para o sistema de edição para posterior impressão.

Este acontecimento de 2007, foi um alerta para os estónios e ajudou-os a identificarem *in loco* as suas vulnerabilidades. Em consequência, podiam ter uma de duas atitudes – ficar furiosos e lastimar ou aprender com a situação. Optaram pela aprendizagem e colocaram em prática o saber da palavra crise em chinês como o fez *John F. Kennedy* no seu discurso em *Indianápolis,* a 12 de abril de 1959.

[8] Redes de computadores - conhecidas como *botnets* - enviam enormes quantidades de mensagens indesejadas (*spam*) e pedidos on-line automáticos para saturar os servidores.

"When written in Chinese, the word "crisis" is composed of two characters - one represents danger and one represents opportunity."[9]

A Estónia sofreu com esta situação, mas face à oportunidade, tornaram-se especialistas em defesa cibernética**.**

"Foi um ótimo teste de segurança. Não sabemos para quem enviar o cheque", disse *Tanel Sepp*, especialista em segurança cibernética do Ministério da Defesa da Estónia.

"Os ataques cibernéticos do Soldado de Bronze foram os primeiros ataques a serem suspeitos de terem sido lançados por uma nação contra outra."[10]

Cerca de um ano mais tarde, ocorreu um novo ataque e teve um cariz mais militar. Este foi o primeiro caso em que um ciberataque ocorreu de um modo síncrono com um ataque convencional – conflito que opôs a Geórgia à Rússia. Se dúvidas restavam, este acontecimento esclareceu que havia um novo espaço para o conflito armado – o ciberespaço.

Decorria o mês de agosto de 2008, quando as forças georgianas lançaram um ataque surpresa contra as forças separatistas da Ossétia do Sul numa tentativa de recuperar o território, afirmando que estavam a responder aos ataques efetuados contra as suas forças de paz, e que a Rússia estava a deslocar unidades não pertencentes à manutenção da paz para o país. A 8 de agosto, a Rússia respondeu ao ataque efetuando operações militares em território georgiano.

No entanto, um dia antes da invasão russa, diversos ataques cibernéticos coordenados acompanharam a campanha militar. "Essa foi a primeira vez que uma operação de ataque contra uma rede de computadores em grande escala foi executada em conjunto com importantes operações de combate terrestre. O ataque não teve ligação direta com o governo russo, mas exerceu importante impacto psicológico e de informação na Geórgia, isolando-a do resto do mundo."[11]

Como já referido, este foi o primeiro caso em que um conflito internacional político e militar foi acompanhado, ou mesmo precedido, por uma ofensiva no domínio cibernético e parece ter sido bem-sucedido, pois ao mesmo tempo que era lançado um ataque cibernético

---

[9] ***John F. Kennedy – Presidential Library and Museum*** [Em linha]. 1959. [Consult. 24 nov. 2019]. Disponível em https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/indianapolis-in-19590412

[10] McGUINNESS, Damien. ***Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*** [Em linha]. 2012. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/mundo/noticias-39800133 (Tradução livre do autor)

[11] SHAKARIAN, Paulo Cpt. ***Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008*** – MILITARY REVIEW [Em linha]. Novembro-Dezembro 2011, p.6. [Consult. 2 out. 2019]. Disponível em https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20111231_art011POR.pdf

apontando para o controlo do ciberespaço, criando o pânico e desinformação, foi efetuada uma invasão militar utilizando os domínios terrestre, aéreo e marítimo.

O terceiro ataque atingiu o maior grau de sofisticação. Em 2010, as centrifugadoras de *Natanz*, usadas no programa nuclear do Irão, foram atacadas com o *malware* (software malicioso) *Stuxnet* que fez com que as centrifugadoras, usadas para enriquecer urânio, começassem a funcionar erraticamente, até se autodestruírem, apesar de os instrumentos de monitorização indicarem estar tudo bem.

"A importância deste evento, foi o facto de ter sido o primeiro incidente documentado em que uma arma cibernética real foi implantada, e cuja intenção era negar, degradar, interromper e destruir a operacionalidade de um determinado sistema."[12]

Em setembro desse mesmo ano a *BBC*, com base em informações da agência de notícias oficial *IRNA*[13], fazia uma reportagem intitulada "*Worm Stuxnet* atinge computadores da equipa da central nuclear do Irão" dizendo que um complexo *worm*[14] tinha infetado os computadores internos da primeira central nuclear do Irão.

Suspeitas de que os Estados Unidos e Israel tinham sido os possíveis autores deste ato, foram reforçadas, mas não confirmadas, em 2012, aquando um funcionário (sob anonimato) dos EUA reconheceu o envolvimento deste país como fazendo parte do programa *Operation Olympic Games,*[15] iniciado por Presidente *George W. Bush* e continuado pelo Presidente *Barack Obama.* A Administração Americana não fez nenhum pronunciamento oficial sobre o assunto.

No último capítulo, imediatamente antes da conclusão, iremos tentar responder ao terceiro objetivo específico que consiste em demonstrar que Portugal, membro fundador da OTAN, deverá estar comprometido com a inovação e a transformação que a Aliança está a protagonizar sobre o tema ciberespaço, tornando-se num polo relevante e estratégico.

Neste capítulo iremos investigar o que se concretizou, em Portugal e na Organização do Tratado do Atlântico Norte, em termos de produção normativa de política e estratégia para a ciberdefesa.

---

[12] ZETTER, Kim. ***An Unprecedented Look at Stuxnet, the World's First Digital Weapon*** **[Em linha]**. 2014. [Consult. 24 nov. 2019]. Disponível em https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (Tradução livre do autor)

[13] ***Agência de Notícias da República Islâmica***, conhecida internacionalmente como **IRNA** (de sua denominação em inglês: ***Islamic Republic News Agency***) é uma agência de notícias oficial da República Islâmica do Irão, mantida com recursos públicos e controlada pelo Ministério da Cultura e da Orientação Islâmica.

[14] ***Worm*** – Vírus de computador de replicação rápida infetando o sistema.

[15] ***Operation Olympic Games*** foi uma campanha secreta e ainda não reconhecida, de sabotagem por meio de interrupção cibernética, dirigida às instalações nucleares iranianas pelos Estados Unidos e provavelmente por Israel. É a primeira utilização conhecida de armas cibernéticas ofensivas. Iniciada sob a administração de George W. Bush em 2006, esta operação foi acelerada sob a presidência de Barack Obama

Como é óbvio, com o passar dos anos e face à escalada de interesse mundial pelo tema ciberespaço, muito se tem escrito e legislado sobre o assunto. No entanto, iremos dar especialmente atenção àqueles que nos pareceram ser mais relevantes para o nosso trabalho e que irão apoiar a nossa linha de raciocínio.

Muita da produção normativa que iremos abordar tem uma interdependência dos dois "ramos" do ciberespaço – segurança e defesa. No sítio da Defesa Nacional, no espaço reservado à ciberdefesa, é referido que "As atividades de ciberdefesa constituem uma nova área operacional da defesa nacional e um contributo fundamental para a cibersegurança do país.".

É nesse sentido que, Paulo Viegas Nunes, no contributo que deu para a estratégia Nacional de Ciberdefesa, nos diz que "assim como existe uma estreita ligação entre a Segurança e a Defesa Nacional, também a cibersegurança se revela indissociável da ciberdefesa do Estado. Na prática, isto significa que não será possível garantir a cibersegurança sem o levantamento de uma capacidade de ciberdefesa."[16]

Assim, em nosso entender, Portugal é um bom exemplo de como um pequeno país pode ter um papel importante na OTAN, ao liderar uma área, como a ciberdefesa. Com o acolhimento da Academia de Comunicações e Informação da OTAN, com o *Cyber Academia and Innovation Hub*, com a formação (pós-graduação) na Academia Militar em ciberdefesa, com o Instituto Universitário Militar a desenvolver formação também nesta área, em parceria com as universidades do país, com o reforço de verbas na recente lei de programação militar triplicando o investimento em ciberdefesa (51 milhões de euros, para o período 2019-2030), com a liderança nestes últimos quatro anos dos programas "*Smart Defense*" a criar operadores informáticos mais qualificados e a contribuir para a criação de novas competências, Portugal tem demonstrado que não é preciso ser grande para se ser líder no seio da Aliança.

Em conclusão, tentaremos demonstrar que existe uma janela de oportunidade para Portugal, no seio da Aliança do Atlântico Norte, para se tornar num polo relevante e estratégico na rede de centros de excelência cibernéticos no domínio da ciberdefesa.

Para isso, a juntar à imensa massa crítica e conhecimento que existe em Portugal sobre este assunto, e alavancado com a relocalização da *NATO Communications and Information Systems School,* de Latina (Itália), para Oeiras com a nova designação *NATO Communications, Information and Cyber Academy*, e fortalecido com a liderança do programa *Smart Defence - Multinational Cyber Defence Education and Training Project*, que prevê a criação de um currículo de Defesa Cibernética, que estabelecerá os fundamentos conceituais, doutrinais e

[16] ***Contributos para uma estratégia Nacional de Ciberdefesa***, IDN Cadernos, nº28, 2018, p. 64

didáticos do futuro trabalho da Academia, Portugal tem uma oportunidade única de qualificar melhor as suas estruturas e pessoal militar no domínio da defesa cibernética e promover uma nova cultura de excelência neste domínio, assegurando uma posição de destaque no seio da Aliança.

2. Capacidade militar portuguesa face a alguns parceiros da OTAN

> *"Portugal nasceu e consolidou-se pela força de vontade dos primeiros reis e pelos braços armados dos seus homens. Lanças, piques, espadas, adagas, fundas, maças, arcos, bestas, machados, paus ferrados e até instrumentos agrícolas tiveram um papel importante, senão fundamental, na conquista e defesa do território."*[17]

Portugal, como muitos outros países, foi edificado a "ferro e fogo", recorrendo à ação armada, de modo a alcançar os seus objetivos político-estratégicos. Nesse sentido, e como consequência natural, foi construindo e consolidando a sua capacidade militar.

Neste capítulo, pretendemos caracterizar genericamente Portugal, Bélgica, Holanda e Dinamarca, segundo determinados fatores, culminando naquele que é o mais importante para este trabalho – a capacidade militar. Assim, e no sentido de alcançarmos tal desiderato, iremos ao longo deste capítulo, utilizar 4 fontes fundamentais, a *Global Firepower (GFP)*, o *World Factbook* da *Central Intelligence Agency (CIA)*, o *Military Balance* do *International Institute for Strategic Studies (IISS)* e o *Encyclopedia of the Nations*.

Ainda que pontualmente possamos fazer recurso a outras fontes, estas foram aquelas, que em muita da bibliografia lida, eram dadas como referência, facto que pesou aquando da escolha das fontes principais para a elaboração deste capítulo.

Enquanto o *World Factbook* da *CIA* e *The Encyclopedia of the Nations* nos irão ajudar a caracterizar fatores como geografia, economia, comunicações e ciência e tecnologia, no que aos valores militares diz respeito, as fontes principais irão ser a *GFP* e o *The Military Balance* de 2019 do *IISS*.

Como referido anteriormente, iremos aferir a capacidade militar dos quatro países em análise e, em nosso auxílio, iremos fazer uso de uma caraterística que a *GFP* utiliza – o *PwrIndx* (*PowerIndex*). Para calcular este *index*, a *GFP*, avalia os valores individuais de cada país e, fazendo recurso a uma fórmula interna, para gerar a pontuação, estabelece as classificações *GFP* num determinado ano (o ano utilizado será o de 2019). No entanto, alguns dos valores são estimados enquanto os números oficiais não estão disponíveis.

"O *PowerIndex* que a *GFP* utiliza para classificar os países, é um produto de vários fatores que vai desde do uso da tecnologia, fator cada vez mais predominante e decisivo nas guerras, até à "mão de obra" disponível, muitas vezes fator preponderante para a vitória. Este

[17] PINTO, Renato Fernando Marques – As indústrias militares e as armas de fogo portáteis no Exército Português. **Revista Militar** [Em linha]. Nº 2495 (2009), pp 1543-1634. [Consult. 15 set. 2019]. Disponível em https://www.revistamilitar.pt/artigo/528.

último fator é crucial no ranking da *GFP*, pois representa a parte de uma determinada população que está (teoricamente) disponível para ajudar num esforço de guerra. Isso pressupõe pessoas saudáveis, aptas para a luta e com possibilidade de se verem envolvidas numa longa campanha. O *Manpower Fit-for-Military-Service* (MFMS) é usado pelo ranking final da *GFP* para refinar ainda mais a força militar geral de uma nação. Em consequência, as nações com populações globais inerentemente grandes serão, de uma maneira óbvia, capazes de oferecer mais pessoal adequado ao serviço militar."[18]

2.1. Caracterização de Portugal e sua capacidade militar

> *Portugal foi considerada uma potência marítima mundial durante os séculos XV e XVI tendo, no entanto, começado a perder a sua riqueza e estatuto com a destruição de Lisboa (terramoto de 1755), com as incursões militares das tropas francesas sobre o território (invasões francesas no início do século XIX) e "atingiu o seu perigeu" em 1822 com a independência da sua colónia mais rica, o Brasil. No início do século XX uma revolução organizada pelo Partido Republicano Português destituiu a monarquia constitucional vigente e implantou um regime republicano que durante a maior parte das seis décadas seguintes governaram o País com governos repressores. Mais recentemente, em 1974, um golpe militar acomodou amplas reformas democráticas, e no ano seguinte, Portugal concedeu a independência a todas as colónias africanas. Portugal é membro fundador da Organização do Tratado do Atlântico Norte (OTAN) em 1949 e entrou na Comunidade Económica Europeia (CEE), agora União Europeia (UE) em 1986.*[19]

Segundo a *GlobalFirepower*, no que à capacidade militar diz respeito, Portugal ocupa o 67.º lugar ao nível mundial (entre 137 países considerados pela *GFP* na avaliação da capacidade militar), o 18.º lugar (de 25)[20] na União Europeia e no seio da OTAN ocupa a 19.ª posição (entre 27)[21].

2.1.1. Caracterização de Portugal

Portugal tem uma área aproximada de 92.000 Km^2 e a sua geografia é definida por um "triângulo estratégico", que tem como vértices o território continental e os arquipélagos dos

[18] ***Global Firepower*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.globalfirepower.com (Tradução livre do autor)
[19] ***The World Factbook. Central Intelligence Agency*** [Em linha]. 2019 [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html (Tradução livre do autor)
[20] Chipre, Luxemburgo e Malta não estão incluídos nesta lista devido a condições e mínimos não atendidos pela *GFP*.
[21] A Islândia e o Luxemburgo não estão incluídos nesta lista devido a condições e mínimos não atendidos pela *GFP*.

Açores e da Madeira, ambos situados no Atlântico Norte, que tornam este espaço euro-atlântico como uma área geográfica de interesse estratégico permanente[22].

"O seu clima é temperado com variações sazonais e regionais. A norte, predomina um clima oceânico com verões frescos e invernos chuvosos assistindo-se a fortuitas quedas de neve. O centro tem verões quentes e invernos frios e chuvosos e a sul o clima é muito seco, com chuvas em quantidade diminuta ao longo da costa. A temperatura média anual em Portugal é de 16 ° C."[23]

Os seus principais recursos naturais são a pesca, cortiça, minério de ferro, cobre, zinco, estanho, tungstênio, prata, ouro, urânio, mármore, argila, gesso, sal, terra arável e energia hidroelétrica[24].

Desde que ingressou na Comunidade Económica Europeia (CEE), Portugal alterou a sua economia tornando-a mais diversificada e baseada em serviços. Nas duas décadas seguintes, sucessivos governos privatizaram muitas empresas controladas pelo Estado e liberalizaram áreas-chave da economia, incluindo as áreas financeira e setores de telecomunicações. O País aderiu à União Económica e Monetária em 1999 e o euro começou a circular em Portugal em 1 de janeiro de 2002, juntamente com outros 11 estados-membros da UE[25].

Durante grande parte dos anos 90 a economia portuguesa cresceu mais do que a média da UE, mas a taxa de crescimento diminuiu em 2001-08 e após a crise financeira global em 2008, a economia de Portugal contraiu-se e entrou em recessão durante 3 anos, no período de 2011 a 2013. Durante estes anos o governo implementou enormes cortes orçamentais e aumentos de impostos para atender às condições de um pacote de resgate financeiro patrocinado pelo "consórcio" União Europeia e Fundo Monetário Internacional (UE-FMI), assinado em maio de 2011[26].

Como diz o ditado popular "*Depois da tempestade, vem a bonança*" e Portugal saiu com êxito do programa UE-FMI, em maio de 2014, e a sua recuperação económica ganhou força no ano de 2015 devido às fortes exportações e à recuperação do consumo privado. O crescimento do Produto Interno Bruto (PIB) acelerou em 2016 e atingiu os 2,5% em 2017. O desemprego

[22] **Conceito Estratégico de Defesa Nacional** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.idn.gov.pt/conteudos/documentos/CEDN_2013.pdf
[23] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Portugal-CLIMATE.html (tradução livre do autor).
[24] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html
[25] ***Idem.***
[26] ***Idem.***

permaneceu alto, com uma percentagem de 9,7%, em 2017, mas tem vindo a melhorar de uma forma constante, desde do pico de 18% em 2013[27].

Após as eleições legislativas em 2015, o governo socialista, com acordo parlamentar à esquerda, acabou com algumas medidas impopulares de austeridade, conseguindo, no entanto, permanecer dentro da maioria das metas fiscais da UE. "O deficit orçamental caiu de 11,2% do PIB, em 2010, para 1,8%, em 2017, o mais baixo do País desde que a democracia foi restaurada em 1974 superando as projeções da UE e do FMI de 3%. Portugal saiu do procedimento de deficit excessivo da UE em meados de 2017,"[28]

Portugal tem um valor de PIB *per capita* (PPS)[29] de 23.396,8 relativamente abaixo da média europeia que se encontra nos 30.967,2[30].

Em termos de comunicações, o sistema telefónico de Portugal possui uma rede de ponta com capacidade de banda larga e alta velocidade, encontrando-se atualmente a desenvolver capacidade de 5G. Os telefones de linha fixa têm um rácio de 45:100 (45 telefones por 100 pessoas) e no que diz respeito a telefones de rede móvel o rácio aumenta substancialmente ficando nos 109:100 (dados de 2018)[31].

Portugal tem um papel muito importante na rede mundial de cabos submarinos, pois a sua localização geoestratégica aliada à sua capacidade de inovação têm sido elementos essenciais para que o País seja um ponto de amarração de sistemas internacionais, promovendo e facilitando o tráfego entre os continentes.

---

[27] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html (Tradução livre do autor).
[28] ***Idem.***
[29] ***PPS*** é a sigla de *Purchasing Power Standard*, uma moeda fictícia que significa «paridade de poder de compra padrão» em português. Serve para comparar os níveis de bem-estar e de despesa entre países, anulando a diferença dos níveis de preços.
[30] ***PORDATA, Base de dados Portugal contemporâneo*** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.pordata.pt/Europa/PIB+per+capita+(PPS)-1778
[31] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html

Principais cabos submarinos como *Ella Link*[32], *EIG*[33], *SAT-3 / WASC*[34], *SeaMeWe-3*[35], *Atlantis2*[36] e *Columbus-III*[37] fornecem conectividade para a Europa, África, Médio Oriente, Ásia, Sudeste Asiático, Austrália, América do Sul e EUA.[38]

No que diz respeito a atividades de investigação científica e tecnológica em Portugal, estas são conduzidas, principalmente, no âmbito de uma rede de unidades de investigação e desenvolvimento (I&D) que estão integradas em universidades públicas e estatais de gestão autónoma de investigação.

Portugal tem acordos com várias organizações científicas, europeias e norte-americanas, de modo a desenvolver e aumentar a eficácia do ensino superior e de investigação. Nas organizações anteriormente referidas podemos incluir, como exemplo, na Europa a Agência Espacial Europeia (ESA) e o Laboratório Europeu de Física de Partículas (CERN) e nos Estados Unidos a conceituada universidade privada *Massachusetts Institute of Technology* (MIT).

"A ciência, a tecnologia e a inovação são parte de quase todos os aspetos das nossas vidas quotidianas, mas também podem ajudar a enfrentar alguns dos principais desafios da sociedade. Elas potencialmente contribuem para resolver ameaças ambientais ou de segurança internacional, garantir alimentos mais seguros ou levar ao desenvolvimento de novos medicamentos para prevenir e combater doenças e para responder a questões relacionadas ao envelhecimento da população. Ciência, tecnologia e inovação também são consideradas uma das forças motrizes impulsionando o crescimento e a criação de empregos."[39]

---

[32] ***EllaLink*** é um cabo submarino que liga Brasil e Portugal (Sines) e prevê uma ligação a 100Gbps; a atual ligação é de apenas 10Gbps. [Em linha]. [Consult. 17 set. 2019]. Disponível em https://pt.wikipedia.org/wiki/EllaLink

[33] ***Europe India Gateway (EIG)*** é um cabo submarino que tem cerca de 15.000 quilómetros de comprimento e liga o Reino Unido à Índia e tem um ponto de acesso em Portugal (Sesimbra). É capaz de fornecer até 3.84 terabits por segundo [Em linha]. [Consult. 17 set. 2019]. Disponível em https://en.wikipedia.org/wiki/Europe_India_Gateway

[34] ***SAT-3 / WASC* ou *South Atlantic 3/West Africa Submarine Cable*** é um cabo de comunicação submarino que liga Portugal e Espanha à África do Sul, com ligações a vários países da África Ocidental ao longo de todo o seu percurso [Em linha]. [Consult. 17 set. 2019]. Disponível em https://en.wikipedia.org/wiki/SAT-3/WASC

[35] ***SEA-ME-WE3*** or ***South-East Asia - Middle East - Western Europe 3*** é um cabo submarino com 39.000 quilómetros de comprimento que liga a Alemanha ao Japão passando pela Austrália e tem um ponto de acesso em Portugal (Sesimbra) [Em linha]. [Consult. 17 set. 2019]. Disponível em https://en.wikipedia.org/wiki/SEA-ME-WE_3

[36] ***ATLANTIS-2*** é um cabo submarino transatlântico de fibra ótica ligando a Argentina a Portugal passando pelo Brasil, Senegal, Cabo Verde e Ilhas Canárias [Em linha]. [Consult. 17 set. 2019]. Disponível em https://pt.wikipedia.org/wiki/Atlantis-2

[37] ***COLUMBUS III*** é um cabo de telecomunicações transatlântico de 9900 km com 2 pares de fibras e uma capacidade de projeto de 20 Gbps que liga Miami (EUA) à Sicilia (Itália) passando por Portugal [Em linha]. [Consult. 17 set. 2019]. Disponível em https://en.wikipedia.org/wiki/Columbus_III

[38] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html

[39] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/web/science-technology-innovation (Tradução livre do autor)

Os dados seguidamente apresentados têm como fonte a reputada Instituição Europeia – *Eurostat*[40] e entre os inúmeros indicadores existentes escolhemos 5 para nos dar uma panorâmica do estado da ciência e tecnologia no País. Assim, os escolhidos foram os seguintes:

- Despesas em pesquisa e desenvolvimento (P&D);
- Recursos Humanos em Ciência e Tecnologia;
- Doutorandos nas áreas de Ciência e Tecnologia;
- Pedidos de patentes de alta tecnologia submetidos ao Instituto Europeu, e;
- Exportações de alta tecnologia.

"A pesquisa e o desenvolvimento experimental, compreendem o trabalho criativo realizado de forma sistemática a fim de aumentar o capital de conhecimento, incluindo o conhecimento do homem, da cultura e da sociedade de forma a criar novas aplicações. As despesas de P&D, consideradas, incluem todas as despesas governamentais de P&D e as realizadas pelo sector empresarial no território nacional durante um determinado período, independentemente da fonte de recursos. As despesas de P&D são mostradas como uma percentagem do *PIB* e em Portugal essas despesas foram (em 2018) de 1,35% do *PIB*, distante da média Europeia que se encontram nos 2,11%," [41]

No que diz respeito aos Recursos Humanos em Ciência e Tecnologia, considerámos a população ativa na faixa etária de 25 a 64 anos (ou seja, tendo concluído com êxito uma educação no terceiro nível ou sendo empregada em ciência e tecnologia). Neste indicador, Portugal está aquém da média europeia (47,5% da população ativa) ficando-se pelos 37,5%[42].

"Quanto aos doutorandos, nas áreas de Ciência e Tecnologia, este indicador considera todos os que participam no segundo estágio do ensino superior nas áreas de ciência e tecnologia, em percentagem da população com idade entre os 20 e os 29 anos. Este indicador, com um valor de 0,6% em Portugal (uma décima acima da média europeia), inclui o número total de

[40] ***Eurostat*** é a Instituição de estatística da União Europeia com a sua sede no Luxemburgo. A sua missão é fornecer estatísticas de alta qualidade para a Europa. No cumprimento da sua missão, o Eurostat promove os seguintes valores: respeito e confiança, promoção da excelência, promoção da inovação, orientação para serviços, independência profissional. Procurando maneiras de melhorar continuamente seus produtos e serviços, o Eurostat ganhou o reconhecimento da Fundação Europeia para a Gestão da Qualidade "Comprometida com a Excelência" em novembro de 2016.

[41] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00001/default/table?lang=en (Tradução livre do autor)

[42] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00025/default/table?lang=en

estudantes em programas de ensino superior que leva a uma qualificação avançada em pesquisa, nos campos educacionais da Ciência, Matemáticas, Computação e Engenharias."[43]

Os dados sobre as patentes de alta tecnologia referem a proporção de pedidos feitos diretamente ao Escritório Europeu de Patentes (EPO) ou via Tratado de Cooperação de Patentes, por milhão de habitantes de um país. A definição de patentes de alta tecnologia utiliza subclasses específicas da Classificação Internacional de Patentes. Portugal tem uma percentagem de 1,54%, desmesuradamente abaixo da média europeia que é 15,77%[44].

O último indicador, exportações de alta tecnologia, tem como resultado uma percentagem referente à participação das exportações de todos os produtos de alta tecnologia no cômputo geral das exportações. "Consideramos como produtos de alta tecnologia a soma dos seguintes produtos: aeroespacial, máquinas para escritório, computadores, eletrónica-telecomunicações, farmácia, instrumentos científicos, maquinaria elétrica, química, maquinaria não elétrica e armamento. Neste indicador, uma vez mais, fica enfatizado a distância de Portugal ante a média europeia 4,0% e 17,9% respetivamente."[45].

Por fim, quanto ao desempenho digital, Portugal encontra-se na 19.º posição entre os 28 da EU, segundo o Índice de Economia e Sociedade Digital (IESD)[46] que resume indicadores relevantes sobre o desempenho digital da Europa e acompanha a evolução dos estados membros da UE em competitividade digital observando 5 fatores, a saber:

- Conectividade - Evolução do mercado de banda larga;
- Capital Humano - Inclusão Digital e Habilidades;
- Uso de serviços de Internet;
- Integração da tecnologia digital.
- Serviços Públicos Digitais.

Em relação ao IESD de referir que no último ano todos os países da UE melhoraram o seu desempenho digital, tendo a Finlândia, Suécia, Holanda e Dinamarca obtido as maiores pontuações em 2019 encontrando-se entre os líderes globais em digitalização. Esses países são seguidos pelo Reino Unido, Luxemburgo, Irlanda, Estónia e Bélgica. Os restantes países ainda

[43] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00028/default/table?lang=en (Tradução livre do autor)
[44] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00010/default/table?lang=en
[45] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tin00140/default/table?lang=en (Tradução livre do autor)
[46] ***European Commission*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/digital-single-market/en/desi

têm um longo caminho a percorrer, e a UE, como um todo, precisa de melhorias para poder competir no cenário global[47].

2.1.2. Capacidade militar Portuguesa

As Forças Armadas Portuguesas são constituídas pela Marinha Portuguesa (inclui o Corpo de Fuzileiros Navais), o Exército Português e a Força Aérea Portuguesa. Tem ainda um órgão paramilitar denominado Guarda Nacional Republicana (GNR)[48].

"A idade para serviço militar voluntário ou contratado encontra-se entre os 18-30 anos de idade não havendo nenhum serviço militar obrigatório. O recrutamento é possível se houver voluntários insuficientes. As mulheres servem nas forças armadas, em navios da marinha desde 1992, mas são proibidas de servir em algumas especialidades de combate. O serviço contratado dura um período inicial de dois a seis anos e pode ser estendido até um máximo de 20 anos de serviço. A reserva é obrigatória até à idade de 35 anos. O orçamento para a defesa, no ano de 2018, foi de 1,43% do *PIB*."[49]

Segundo o *Military Balance*, as principais tarefas das forças armadas de Portugal são a defesa da pátria, a segurança marítima, as operações multinacionais e responder em caso de desastres humanitários. A revisão estratégica de 2013 estabeleceu tarefas-chave de defesa e previa uma redução na força do Exército associada a uma mudança organizacional, dividindo os serviços em forças de reação rápida, forças de defesa permanentes e forças modulares. Os planos de investimento traçados apoiam a ambição de Portugal no campo da reação rápida e na capacidade de vigilância marítima, assim como, nas operações multinacionais. Em dezembro de 2018, o governo aprovou uma nova lei da programação militar (LPM) para os anos de 2019-30 que posteriormente foi aprovada pelo parlamento em abril de 2019[50].

Ainda segundo aquele relatório do *IISS*, a proposta da LPM irá impulsionar a indústria de defesa nacional, levando à aquisição de cinco aeronaves *KC-390*, seis embarcações de patrulha oceânica e um navio-tanque de reabastecimento, assim como, um navio logístico multiuso.

[47] ***Idem***.
[48] **GNR** é uma força nacional de gendarmaria composta por militares com funções de aplicação da lei, segurança interna, defesa civil, resposta a desastres e guarda costeira. Depende do Ministro da Administração Interna. Em caso de guerra ou crise, pode ser colocado sob ordens do Chefe do Estado Maior Geral das Forças Armadas.
[49] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html (Tradução livre do autor)
[50] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 138

Haverá novos investimentos em segurança cibernética (a nova academia de cibersegurança da OTAN foi construída em Oeiras) e em tecnologias de uso duplo.[51]

No que diz respeito ao Exército, este Ramo das Forças Armadas planeia melhorar a sua capacidade de guerra eletrónica e efetuar a atualização aos seus carros de combate, os *Leopard* 2A6s. Por sua vez a Marinha, pretende atualizar as fragatas e os submarinos e proceder à aquisição de embarcações de patrulha e de um navio de apoio logístico. Em relação à Força Aérea, este Ramo planeia efetuar a modernização dos F-16 (aeronave de ataque) que ainda se encontram na versão anterior, assim como, dos P-3C (aeronave de patrulha marítima).[52]

Portugal tem uma indústria de defesa presente e ativa e segundo o sítio da Defesa Nacional gera um volume de negócios de 100 mil milhões de euros por ano, empregando direta ou indiretamente, cerca de 1,4 milhões de pessoas altamente qualificadas potenciando o desenvolvimento da economia nacional e reforçando as exportações.

Em 2013, Portugal estabeleceu uma estrutura nacional de defesa cibernética, e passados dois anos produziu a primeira Estratégia Nacional de Segurança do Ciberespaço. O Centro de Ciberdefesa encontra-se em operação, desde de 2017, sob o comando do Chefe do Estado-Maior General das Forças Armadas, deixando a responsabilidade dos aspetos estratégicos-militares da defesa cibernética ao Conselho de Chefes de Estado-Maior. Os três ramos das forças armadas possuem unidades de defesa cibernética sendo responsáveis por responder a ataques cibernéticos[53].

Portugal tem, segundo a *GFP*, uma população de 10.355.493 pessoas e uma população disponível para ajudar em esforço de guerra de 4.804.949 (46,4%) e um *MFMS* de 3.953.253 (38.2%). Anualmente 118.058 pessoas (1,1%) atingem a "idade militar" e atualmente existem 245.500 pessoas (2,3%) com capacidade militar, sendo que 30.500 (0.3%) estão no ativo[54].

Portugal em termos militares conta com 41 ativos navais sendo parte integrante desses ativos os submarinos *SSK*[55] da classe Tridente, as fragatas *FFGHM*[56], como principais combatentes de superfície com capacidade de helicópteros a bordo e por último as corvetas para combate costeiro. A esta capacidade junta-se ainda os navios de logística e suporte. Dos 41 ativos navais, destacam-se os 2 submarinos, as 5 fragatas e os 19 navios de patrulha.

[51] ***Idem.***
[52] ***Idem.***
[53] ***Idem.*** p. 139
[54] ***Global Firepower*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=portugal
[55] ***SSK*** *– Attack submarine with ASW (anti-submarine warefare) capability (hunter-Killer)*
[56] ***FFGHM*** *– Fire-fighting/frigate/with AShM (anti-ship missile) with hangar/with SAM (surface-to-air missile)*

No que diz respeito ao Exército, este ramo das Forças Armadas tem como capacidade principal as viaturas blindadas *Leopard* 2A6, *Chaimite* e *Pandur* II. Como armamento pesado possui os canhões de 84mm *Carl Gustav* e os M40A1 de 106mm, assim como, os morteiros *Tampella* de 120mm e o M30 de 107mm. Em termos de capacidade de armas antiaérea possui os sistemas de mísseis *Chaparral* e *Stinger* e ainda o sistema de armas *TOW*[57].

Em termos numéricos destacam-se 186 tanques de combate, 700 veículos de combate e as 33 peças de artilharia.

A Força Aérea Portuguesa é dos três ramos o mais recente e foi criada como ramo independente em 1952. Possui atualmente cinco bases aéreas, dois aeródromos de manobra, um aeródromo de trânsito e quatro estações de radar.

A sua força é composta por 87 aeronaves distribuídas por 2 esquadras de ataque, com a aeronave *F-16*, 1 esquadra de patrulha marítima, com o *P-3C Orion*, 1 esquadra de *ISR*,[58] com os *C295M*, 1 esquadra de busca e salvamento, com o helicóptero *AW101 Merlin*, 2 esquadras de transporte, com os *C-130H/C-130H-30 Hercules* e *Falcon 50* e por fim 2 esquadras de treino, com as aeronaves *Alouette* III e *TB-30 Epsilon*. De toda esta força destacam-se os 24 aviões de ataque, os 11 de transporte e por fim 25 helicópteros, mas nenhum é de ataque.

[57] ***TOW*** (***T****ube launched,* ***O****ptically tracked and* ***W****ire command - link guied weapon system*)
[58] ***ISR*** – ***I****ntelligence,* ***S****urveillance and* ***R****econnaissance*

2.2. Caracterização da Bélgica e sua capacidade militar

"A Bélgica tornou-se independente da Holanda em 1830, tendo sido ocupada pela Alemanha durante as I e II Guerras Mundiais. O país prosperou no último meio século como um estado europeu moderno e tecnologicamente avançado e é atualmente membro da OTAN e da UE. Nos últimos anos, as divisões políticas entre os flamengos, de língua holandesa do Norte, e os valões, de língua francesa do Sul, levaram a emendas constitucionais que concedem a estas regiões o reconhecimento e autonomia formais. A capital, Bruxelas, acolhe inúmeras organizações internacionais, incluindo a UE e a OTAN."[59]

Segundo o *GlobalFirepower*, no que a capacidade militar diz respeito, a Bélgica ocupa o 68.º lugar (entre 137 países considerados pela *GFP* na avaliação da capacidade militar) ao nível mundial, o 19.º lugar (de 25)[60] na União Europeia e no seio da OTAN ocupa a 20.ª posição (entre 27)[61].

2.2.1. Caracterização da Bélgica

A Bélgica tem uma área aproximada de 30.528 Km2 e está localizada na Europa Ocidental, na fronteira com o Mar do Norte, entre a França e a Holanda. A maioria das capitais da Europa Ocidental fica a 1.000 km de Bruxelas.[62]

"O seu clima é temperado com invernos amenos e verões frescos. No entanto quando nos lembramos da Bélgica vem sempre à ideia um clima chuvoso, húmido e nublado."[63]

Os principais recursos naturais são materiais de construção, areia de sílica, carbonatos e terras aráveis[64].

"A localização geográfica central da Bélgica e a rede de transportes altamente desenvolvida ajudaram a fortalecer uma economia bem diversificada, com uma combinação entre transportes, serviços, indústria e alta tecnologia. As áreas de serviços e alta tecnologia

[59] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/be.html (Tradução livre do autor)
[60] Chipre, Luxemburgo e Malta não estão incluídos nesta lista devido a condições e mínimos não atendidos pela *GFP*.
[61] A Islândia e o Luxemburgo não estão incluídos nesta lista devido a condições e mínimos não atendidos pela *GFP*.
[62] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/be.html
[63] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Belgium-CLIMATE.html (Tradução livre do autor)
[64] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/be.html

estão concentradas na região norte da Flandres, enquanto a região sul da Valónia abriga indústrias como a produção do carvão e do aço. A Bélgica é completamente dependente de países estrangeiros no que diz respeito a combustíveis fósseis, e o facto de o governo belga ter aprovado um novo pacto energético, que fará com que o país elimine gradualmente a energia atómica entre 2022 e 2025, faz com que sete centrais nucleares encerrem entre as datas referidas mas como consequência irá aumentar a sua dependência de energia estrangeira."[65]

> *Assumindo um papel preponderante como centro logístico regional, a economia da Bélgica é vulnerável a variações da procura externa, principalmente com os parceiros comerciais da UE. Aproximadamente três quartos do comércio da Bélgica é com os países da União e quase metade do comércio do porto de Zeebrugge tem como destino o Reino Unido, deixando a economia belga vulnerável ao resultado das negociações sobre a saída do Reino Unido da UE. O PIB da Bélgica cresceu 1,7% em 2017, e o deficit orçamental foi de 1,5% do PIB. O desemprego situou-se nos 7,3%, no entanto, a taxa de desemprego, devido às diferenças industriais entre as regiões, é menor na região da Flandres do que na Valónia, 4,4% e 9,4% respetivamente. Devido aos ataques terroristas de março de 2016, a região de Bruxelas sofreu um forte impacto no sector do turismo, no entanto a economia tem vindo a recuperar com o governo de centro-direita do primeiro-ministro Charles MICHEL a prometer reduzir ainda mais o deficit, em resposta à pressão da UE para diminuir a alta dívida pública da Bélgica que se encontra em 104% do PIB, mas em contraponto esses esforços também reduziriam o crescimento económico.*[66]

De modo a melhorar a competitividade, o governo belga prometeu encontrar um programa de reformas incluindo, nesse programa, mudanças nas regras do mercado de trabalho e benefícios sociais. Em 2017, a Bélgica aprovou um plano de reforma tributária, de modo a reduzir as taxas empresariais de 33% para 29%, em 2018, e reduzir até 25% em 2020. O plano de reforma tributária também incluía benefícios para a inovação e para as pequenas e médias empresas (PME), destinadas a estimular a competitividade e o investimento privado[67].

[65] ***Idem.*** (Tradução livre do autor)
[66] ***Idem.*** (Tradução livre do autor)
[67] ***Idem.***

A Bélgica tem um valor do *PIB per capita* (PPS) de 35.637,3 substancialmente acima da média europeia que se encontra nos 30.967,2[68].

Em termos de comunicações, as instalações de telefone e telégrafo nacionais e internacionais são altamente desenvolvidas, tecnologicamente avançadas e completamente automatizadas. Existem continuados investimentos no desenvolvimento de aplicativos e serviços para a rede 5G e os telefones de linha fixa têm um rácio de 37:100 (37 telefones por 100) pessoas e no que diz respeito a telefones de rede móvel o rácio aumenta substancialmente para 104:100 pessoas (dados de 2018).

Quanto a pontos de amarração de cabos submarinos que fornecem links para Europa, Oriente Médio, Austrália e Ásia encontram-se entre os mais importantes o que liga o Reino Unido-Bélgica (um dos cabos mais antigos do mundo) e o *SeaMeWe-3* (*South-East Asia - Middle East - Western Europe 3*)[69].

No que diz respeito a atividades de investigação científica e tecnológica encontram-se na Bélgica das mais distintas instituições europeias e mundiais. Entre essas instituições estão o Centro para o Estudo da Energia Nuclear em *Mol* (fundado em 1952), o Jardim Botânico Nacional da Bélgica em *Meise* (fundado em 1870), o Instituto de Pesquisa Química em *Tervuren* (fundado em 1928) e o Instituto *Von Karman* de Dinâmica de Fluidos em *Rhode-St-Genese* (fundado em 1956) e apoiado pela OTAN[70].

Os dados seguidamente apresentados têm como fonte a reputada Instituição Europeia – *Eurostat*, e à imagem e semelhança como fizemos com Portugal, iremos manter exatamente os mesmos 5 indicadores dando uma panorâmica do estado da ciência e tecnologia no País. Recordando, os 5 indicadores escolhidos foram:

- Despesas em pesquisa e desenvolvimento (P&D);
- Recursos Humanos em Ciência e Tecnologia;
- Doutorandos nas áreas de Ciência e Tecnologia;
- Pedidos de patentes de alta tecnologia submetidos ao Instituto Europeu, e;
- Exportações de alta tecnologia.

[68] ***PORDATA, Base de dados Portugal contemporâneo*** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.pordata.pt/Europa/PIB+per+capita+(PPS)-1778

[69] ***Idem.***

[70]***The Encyclopedia of the Nations*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Belgium-SCIENCE-AND-TECHNOLOGY.html

As despesas de P&D são mostradas como uma percentagem do PIB e na Bélgica essas despesas foram (em 2018) de 2,76% do *PIB*, um pouco acima da média Europeia que se encontra nos 2,11% [71].

No que diz respeito aos Recursos Humanos, em Ciência e Tecnologia, considerámos a população ativa na faixa etária de 25 a 64 anos (ou seja, tendo concluído com êxito uma educação no terceiro nível ou sendo empregada em ciência e tecnologia). Neste indicador a Bélgica tem um valor de 54,4% da população ativa face aos 47,5% da UE[72].

"Quanto aos doutorandos nas áreas de Ciência e Tecnologia este indicador considera todos os que participam no segundo estágio do ensino superior nas áreas de ciência e tecnologia, em percentagem da população com idade entre os 20 e os 29 anos. Este indicador, com um valor de 0,4% na Bélgica (uma décima abaixo da média europeia), inclui o número total de estudantes em programas de ensino superior que leva a uma qualificação avançada em pesquisa, nos campos educacionais Ciência, Matemáticas, Computação e Engenharias."[73]

Os dados sobre as patentes de alta tecnologia referem a proporção de pedidos feitos diretamente ao Escritório Europeu de Patentes (EPO) ou via Tratado de Cooperação de Patentes, por milhão de habitantes de um país. A definição de patentes de alta tecnologia utiliza subclasses específicas da Classificação Internacional de Patentes. A Bélgica tem uma percentagem de 28,80% bem acima da média europeia que é 15,77%[74].

Como último indicador, temos o que nos dá a participação das exportações de todos os produtos de alta tecnologia no total das exportações. "Consideramos como produtos de alta tecnologia a soma dos seguintes produtos: aeroespacial, máquinas para escritório, computadores, eletrónica-telecomunicações, farmácia, instrumentos científicos, maquinaria elétrica, química, maquinaria não elétrica e armamento. A Bélgica ainda tem que caminhar pois ainda se encontra a uma certa distância da média da EU 10,3% e 17,9% respetivamente."[75]

Em relação, ao desempenho digital, a Bélgica encontra-se na 9º posição entre os 28 da EU segundo o Índice de Economia e Sociedade Digital (IESD)[76] que resume indicadores

[71] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00001/default/table?lang=en

[72] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00025/default/table?lang=en

[73] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00028/default/table?lang=en (Tradução livre do autor)

[74] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00010/default/table?lang=en

[75] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tin00140/default/table?lang=en (Tradução livre do autor)

[76] ***European Commission*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/digital-single-market/en/desi

relevantes sobre o desempenho digital da Europa e acompanha a evolução dos estados membros da UE em competitividade digital observando 5 fatores, a saber:

- Conectividade - Evolução do mercado de banda larga;
- Capital Humano - Inclusão Digital e Habilidades;
- Uso de serviços de Internet;
- Integração da tecnologia digital.
- Serviços Públicos Digitais.

Segundo as pontuações do IESD 2019, no que a desempenho digital, diz respeito, a Bélgica segue num segundo grupo de países.[77]

2.2.2. Capacidade militar Belga

As Forças Armadas Belgas são compostas pelas três habituais componentes: terrestre, naval e aérea. O orçamento para a defesa no ano de 2018 foi de 0,93% do *PIB*[78].

A idade para o serviço militar voluntário, masculino e feminino, é de 18 anos tendo sido abolido o recrutamento em 1994.

Em julho de 2016, o governo belga publicou a sua visão estratégica para a Defesa até o ano de 2030, pretendendo estabilizar o esforço que tem vindo a ser efetuado até 2020 e propiciar de seguida, até 2030, um crescimento. Tem igualmente como objetivo um componente de pessoal reduzido com cerca 25.000 elementos. No entanto, prevê-se um grande número de passagens à reserva, facto que poderá implicar um aumento gradual no recrutamento para que o número referido anteriormente, seja mantido. A Bélgica, tem como objetivo, nesta visão estratégica para a Defesa, a procura de altos níveis de prontidão e a capacidade de destacar forças, principalmente no âmbito da EU e da OTAN[79].

Devido ao seu tamanho e capacidade limitada, a Bélgica frequentemente colabora com os seus vizinhos tendo-se comprometido, com a Dinamarca e a com a Holanda, a formar um comando de operações especiais combinadas[80].

Em relação a material militar, o governo está a investir em aeronaves, equipamentos pessoais e veículos para forças terrestres como parte do plano de defesa. Para isso prevê o

[77] ***Idem***.
[78] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/be.html
[79] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 89
[80] ***Idem.***

lançamento de cinco projetos de investimento que engloba aviões de caça (a Força Aérea selecionou o F-35 *Lightning* II para substituir seus F-16), fragatas, navios draga-minas, *Unmanned Aerial Vehicle* (*UAV)* e veículos de combate terrestre[81].

A Bélgica possui uma indústria de defesa avançada, focada na exportação, componentes e subcontratação, embora a *FN Herstal*[82] seja um dos maiores fabricantes mundiais de armas pequenas.

Em 2014, o Ministério da Defesa, lançou a estratégia belga para a Ciberdefesa, descrevendo três pilares para a capacidade de segurança cibernética: defesa cibernética, inteligência cibernética e contraofensiva cibernética, com "total capacidade operacional" até 2020. Esta estratégia, incluindo não apenas a defesa e inteligência, mas também a capacidade ofensiva, deve, por um lado, garantir um nível adequado de segurança cibernética para armas e sistemas de comunicação, e por outro, deve ser capaz de identificar, manipular ou distorcer as redes e sistemas de um oponente. Assim, para operar essa capacidade, o Ministério da Defesa está a desenvolver o centro de operações de segurança cibernética[83].

A Bélgica tem, segundo a *GFP*, uma população de 11.570.762 pessoas e uma população disponível para ajudar num esforço de guerra de 4.833.107 (41,8%) contando com um *MFMS* de 3.841.305 (33.2%). Anualmente 115.239 pessoas (1,0%) atingem a idade de recrutamento militar, tendo atualmente 35.000 pessoas (0,3%) como capacidade militar sendo 30.000 (0.3%) no ativo 5.000 na reserva[84].

A Bélgica, em termos militares, conta com um dispositivo de 17 ativos navais distribuídos por 2 fragatas *FFGHM* [85] como principais combatentes de superfície, 2 navios de patrulhamento costeiro e 5 navios draga-minas.

No que ao Exército diz respeito, a Bélgica tem como capacidade principal as viaturas blindadas *Piranha III-C DF90* e os *Pandur* e como armamento pesado os morteiros *LG1 MKII* de 105mm. Mas é na Força Aérea que a Bélgica tem a sua pujança, contendo 158 aeronaves distribuídas por 4 esquadras de ataque, com as aeronaves *F-16*, 1 esquadra de busca e salvamento, com os *Sea King MK48*, 2 esquadras de transporte, composta com as aeronaves

---

[81] ***Idem.***

[82] ***Fabrique Nationale d'Herstal*** , auto identificado como **FN Herstal** e frequentemente referida como **Fabrique Nationale** ou simplesmente **FN**, é uma empresa belga líder na fabricação de armas de fogo, localizada em Herstal, na província de Liége, na região de Valónia, e é propriedade da holding Herstal Group, que pertence ao governo regional da Valónia. É atualmente a maior exportadora de armas militares curtas na Europa.

[83] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 91

[84]***Global Firepower*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=belgium

[85] FFGHM – Fire-fighting/frigate/with AShM (anti-ship missile) with hangar/with SAM (surface-to-air missile)

A321, *Falcon 900B* e *C-130H*, 4 esquadras de treino, com diversas aeronaves (e.g. *F-16* e *Alpha Jet*), 1 esquadra de helicópteros de transporte e por último 1 esquadra de *UAV*[86].

De toda esta capacidade destaca-se 43 aviões de ataque, 14 de transporte e 32 helicópteros sem que nenhum seja de ataque.

[86] ***Unmanned Aerial Vehicle*** (UAV) ou veículo aéreo não tripulado comumente conhecido como *drone* é uma aeronave sem piloto humano a bordo. Os UAVs incluem o a aeronave, um controlador em terra e um sistema de comunicação entre os dois e geralmente são operados remotamente por um operador humano ou autonomamente por computadores de bordo.

2.3. Caracterização da Holanda e sua capacidade militar

"As Províncias Unidas Holandesas declararam independência da Espanha em 1579 e durante o século XVII tornaram-se uma potência marítima e comercial com colónias em todo o mundo. Após uma ocupação francesa de 20 anos foi criado o Reino da Holanda, em 1815, e quinze anos mais tarde a Bélgica formou um reino separado separando-se do Reino da Holanda. Durante a Primeira Guerra Mundial a Holanda permaneceu neutral, no entanto, foi invadida e ocupada na Segunda Guerra Mundial pelos alemães. Hoje, a Holanda é uma nação moderna e industrializada e grande exportador de produtos agrícolas. O país foi membro fundador da OTAN e da CEE (atualmente UE) e participou na introdução do euro em 1999."[87]

Em outubro de 2010, as antigas Antilhas Holandesas foram dissolvidas e as três menores ilhas - *Bonaire*, *São Eustáquio* e *Saba* - tornaram-se municípios especiais na estrutura administrativa da Holanda. As ilhas maiores de *São Martinho* e *Curação* juntaram-se aos Países Baixos e Aruba como países constituintes que formam o Reino dos Países Baixos[88].

Segundo o *GlobalFirepower* (*GFP*), no que a capacidade militar diz respeito, a Holanda ocupa o 35.º lugar (entre 137 países considerados pela *GFP* na avaliação da capacidade militar) ao nível mundial, o 10.º lugar (de 25)[89] na União Europeia e no seio da OTAN ocupa a 12.ª posição (entre 27)[90].

2.3.1. Caracterização da Holanda

A Holanda tem uma área aproximada de 41.500 Km^2 e encontra-se na Europa Ocidental, fazendo fronteira com o Mar do Norte, Bélgica e a Alemanha. Localizada na foz dos três principais rios europeus (*Reno*, *Maas* ou *Meuse* e *Schelde*), cerca de um quarto do país fica abaixo do nível do mar e apenas metade da terra excede um metro acima do nível do mar[91].

---

[87] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html (Tradução livre do autor)
[88] ***Idem.*** (Tradução livre do autor)
[89] Chipre, Luxemburgo e Malta não estão incluídos nesta lista devido a condições e mínimos não atendidos pela GFW.
[90] A Islândia e o Luxemburgo não estão incluídos nesta lista devido a condições e mínimos não atendidos pela GFW.
[91] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html

O seu clima é marítimo com verões frescos e invernos amenos[92]. Os seus principais recursos naturais são o gás natural, petróleo, turfa, pedra calcária, sal, areia e cascalho, terras aráveis[93].

"A Holanda é a sexta maior economia da União Europeia, desempenhando um papel importante como centro logístico europeu, aliando um alto excedente comercial a um baixo desemprego. A indústria concentra-se no processamento de alimentos, produtos químicos, refinaria de petróleo e máquinas elétricas. A Holanda possui um setor agrícola altamente mecanizado empregando apenas 2% da força de trabalho, mas fornece grandes excedentes para o processamento de alimentos e sustenta o *status* do país como o segundo maior exportador agrícola do mundo."[94]

A Holanda faz parte da "zona euro" e, como tal, a sua política monetária é controlada pelo Banco Central Europeu. "O setor financeiro é altamente concentrado, com quatro bancos comerciais congregando mais de 80% dos ativos bancários e é quatro vezes o tamanho do *PIB* holandês."[95]

Em 2008, durante a crise financeira, o deficit orçamental da Holanda atingiu 5,3% do *PIB* iniciando uma recessão que se prolongou até 2013. O seu crescimento económico começou a avançar em 2014, mas a recessão deixou marcas profundas. A taxa de desemprego tinha sido dobrada e encontrava-se na marca de 7,4% e o consumo das famílias tinha diminuído em quatro anos consecutivos. Desde 2010, o governo do primeiro-ministro *Mark Rutte* implementou medidas de austeridade significativas para melhorar as finanças públicas e instituiu amplas reformas estruturais nas principais áreas da política, incluindo o mercado de trabalho, o sector habitacional, o mercado da energia e o sistema de pensões. Em 2017, o orçamento do governo retornou a um superavit de 0,7% do *PIB*, com crescimento económico de 3,2%, e o *PIB per capita* finalmente superou os níveis pré-crise.

Durante os anos de 2018 a 2021, a política fiscal anunciada, pelo novo governo, é suportada no aumento do investimento público, assim como, no consumo e investimento das famílias. Este novo governo, ainda com liderança de *Mark Rutte*, planeia também aumentar o número de trabalhadores nos setores público e privado, prevendo um novo declínio na taxa de desemprego, que atingiu 4,8% em 2017.

---

[92] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Netherlands-CLIMATE.html

[93] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html

[94] ***Idem.*** (Tradução livre do autor)

[95] ***Idem.*** (Tradução livre do autor)

A Holanda tem um valor do PIB *per capita* (PPS) de 39.893,8 substancialmente acima da média europeia que se encontra nos 30.967,2[96].

Em termos de comunicações, estas encontram-se altamente desenvolvidas e bem conservadas. Na Holanda o mercado de voz de linha fixa está em declínio, no entanto as plataformas *VoIP*[97] e móveis avançam a bom ritmo. Com uma das maiores taxas de penetração de banda larga fixa do mundo, a Holanda prepara-se para desligar a rede 3G em 2022 e encontram-se a efetuar preparativos e testes para a rede 5G[98].

Os telefones de linha fixa têm um rácio 38:100 (38 telefones por 100 pessoas) enquanto os telefones de rede móvel o rácio é de 120:100 (dados de 2018)[99].

A Holanda, à imagem e semelhança de Portugal tem um papel muito importante na rede mundial de cabos submarinos. Dos cabos que têm a Holanda como ponto de amarração destacam-se o *Farland North*[100], *TAT-14*[101], *Concerto*[102] e o *AC-1*[103] que fornecem links para os EUA e Europa[104].

"A pesquisa e o desenvolvimento científico avançado deram o ímpeto tecnológico para a recuperação económica da Holanda desde a Segunda Guerra Mundial. As universidades holandesas tradicionalmente realizam pesquisas científicas fundamentais, e o governo promove atividades de pesquisa com o patrocínio da Organização Holandesa de Pesquisa Científica, criada em 1988, e da Organização Holandesa de Pesquisa Científica Aplicada, criada em 1930. A Holanda também apoia organizações científicas como a Fundação de Pesquisa Energética, a

[96] ***PORDATA, Base de dados Portugal contemporâneo*** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.pordata.pt/Europa/PIB+per+capita+(PPS)-1778

[97]**VoIP** (*Voice over Internet Protocol*), também chamada de **Voz sobre IP** é o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.

[98] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html

[99] Idem

[100] ***Farland North*** consiste num cabo de fibra ótica com 150 quilômetros de extensão liga o Reino Unido e Holanda e ficou operacional por volta de 1989.

[101] ***TAT-14*** é um cabo de telecomunicações transatlântico, em operação desde 2001, que utiliza multiplexação por divisão de comprimento de onda. O TAT-14 liga os Estados Unidos e a União Europeia (Reino Unido, França, Holanda, Alemanha e Dinamarca) numa topologia em anel.

[102] ***Concerto*** é um sistema de cabo de telecomunicações submarino no Mar do Norte que liga o Reino Unido, Holanda e Bélgica. O Concerto 1 foi construído em 1999 pela Alcatel.

[103] ***AC-1 (Atlantic Crossing 1)*** é um sistema de cabo de telecomunicações submarino ótico com 14.000 Km que liga os Estados Unidos e três países europeus. Ele transporta o tráfego de voz e dados entre os EUA, o Reino Unido, a Holanda e a Alemanha.

[104] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html

Agência de Desenvolvimento Aeroespacial, o Laboratório Aeroespacial Nacional e o Instituto Marítimo da Holanda."[105]

"A indústria eletrotécnica holandesa é altamente desenvolvida concebendo computadores, sistemas de telecomunicações, equipamentos de medição e controlo eletrónico, comutadores e transformadores elétricos e instrumentos médicos e científicos. As empresas holandesas projetaram e construíram os satélites da Holanda e desempenham um papel importante na Agência Espacial Europeia. A importante indústria aeroespacial é liderada pela empresa mundialmente famosa *Fokker*[106], que produziu os aviões de passageiros mais vendidos na Europa, o *F-27 Friendship*[107], e atuou no consórcio que desenvolveu o *Airbus* europeu."[108]

Os dados seguidamente apresentados têm como fonte a reputada Instituição Europeia – Eurostat[109] à imagem e semelhança como fizemos com Portugal e a Bélgica. Aliás, iremos manter exatamente os mesmos 5 indicadores analisados nos dois Países anteriores. Assim, os escolhidos foram os seguintes:

- Despesas em pesquisa e desenvolvimento (P&D);
- Recursos Humanos em Ciência e Tecnologia;
- Doutorandos nas áreas de Ciência e Tecnologia;
- Pedidos de patentes de alta tecnologia submetidos ao Instituto Europeu, e;
- Exportações de alta tecnologia.

[105] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 28 dez. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Netherlands-SCIENCE-AND-TECHNOLOGY.html (Tradução livre do autor)

[106] ***Fokker*** foi uma empresa de construção de aviões da Holanda fundada em 1912 por Anthony Fokker, um empresário político que se tornou fornecedor de aeronaves de guerra durante a 1ª Guerra Mundial, foi uma das empresas pioneiras na fabricação de séries de aviões militares e comerciais. A empresa entrou em falência em 1996 e em 1 de Janeiro de 2006, ela foi adquirida pela EADS-Space Transportation

[107] ***Fokker F27 Friendship*** é um avião turboélice desenvolvido e fabricado pelo fabricante holandês de aeronaves *Fokker*. É o mais numeroso avião pós-guerra fabricado na Holanda e também foi um dos aviões comerciais europeus mais bem sucedidos da sua época.

[108] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 28 dez. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Netherlands-SCIENCE-AND-TECHNOLOGY.html (Tradução livre do autor)

[109] ***Eurostat*** é a Instituição de estatística da União Europeia com a sua sede no Luxemburgo. A sua missão é fornecer estatísticas de alta qualidade para a Europa. No cumprimento da sua missão, o Eurostat promove os seguintes valores: respeito e confiança, promoção da excelência, promoção da inovação, orientação para serviços, independência profissional. Procurando maneiras de melhorar continuamente seus produtos e serviços, o Eurostat ganhou o reconhecimento da Fundação Europeia para a Gestão da Qualidade "Comprometida com a Excelência" em novembro de 2016.

As despesas de P&D são mostradas como uma percentagem do *PIB* e na Holanda essas despesas foram, em 2018, de 2,16% do *PIB*, em média com a União Europeia que se encontra nos 2,11% [110].

No que diz respeito aos Recursos Humanos em Ciência e Tecnologia considerámos a população ativa na faixa etária de 25 a 64 anos (ou seja, tendo concluído com êxito uma educação no terceiro nível ou sendo empregada em ciência e tecnologia). Neste indicador a Holanda tem um valor de 56,9% da população ativa face aos 47,5% da UE[111].

"Quanto aos doutorandos nas áreas de Ciência e Tecnologia este indicador considera todos os que participam no segundo estágio do ensino superior nas áreas de ciência e tecnologia, em percentagem da população com idade entre os 20 e os 29 anos. Este indicador, com um valor de 0,2%, duas décimas abaixo da média europeia, inclui o número total de estudantes em programas de ensino superior que leva a uma qualificação avançada em pesquisa, nos campos educacionais Ciência, Matemáticas, Computação e Engenharias."[112]

Os dados sobre as patentes de alta tecnologia referem a proporção de pedidos feitos diretamente ao Escritório Europeu de Patentes (EPO) ou via Tratado de Cooperação de Patentes, por milhão de habitantes de um país. A definição de patentes de alta tecnologia utiliza subclasses específicas da Classificação Internacional de Patentes. A Holanda tem uma percentagem de 34,28% bem acima da média europeia que é 15,77%[113].

Como último indicador, temos a participação das exportações de todos os produtos de alta tecnologia no total das exportações. "Consideramos como produtos de alta tecnologia a soma dos seguintes produtos: aeroespacial, máquinas para escritório, computadores, eletrónica-telecomunicações, farmácia, instrumentos científicos, maquinaria elétrica, química, maquinaria não elétrica e armamento. Aqui a Holanda mostra a sua força e distancia-se da média da EU 21,3% e 17,9% respetivamente."[114]

Por fim, quanto ao desempenho digital, a Holanda encontra-se na honrosa 3.ª posição entre os 28 da EU, segundo o Índice de Economia e Sociedade Digital (IESD)[115] que resume

[110] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00001/default/table?lang=en
[111] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00025/default/table?lang=en
[112] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00028/default/table?lang=en
[113] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00010/default/table?lang=en
[114] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tin00140/default/table?lang=en (Tradução livre do autor)
[115] ***European Commission*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/digital-single-market/en/desi

indicadores relevantes sobre o desempenho digital da Europa e acompanha a evolução dos estados membros da UE em competitividade digital observando 5 fatores, a saber:

- Conectividade - Evolução do mercado de banda larga;
- Capital Humano - Inclusão Digital e Habilidades;
- Uso de serviços de Internet;
- Integração da tecnologia digital.
- Serviços Públicos Digitais.

Segundo as pontuações do IESD 2019, no que a desempenho digital, diz respeito, a Holanda segue no pelotão da frente ao contrário de Portugal e da Bélgica[116].

2.3.2. Capacidade militar Holandesa

A componente militar holandesa é constituída pelo real exército holandês, pela real marinha holandesa (inclui serviço aéreo naval e corpo de fuzileiros navais), pela real força aérea holandesa e finalmente pela real *Marechaussee* (polícia militar). A idade para aderir, voluntariamente, às forças armadas é aos 17 anos de idade e o valor do orçamento para a defesa, em 2018, foi de 1,21% do *PIB*[117].

"A revisão em 2018, da estratégia da defesa, encarrega as forças armadas de medidas territoriais de defesa e apoio às autoridades civis nacionais na aplicação da lei e a ajuda em desastres e assistência humanitária. As forças holandesas estão cada vez mais integradas com os seus aliados da OTAN, particularmente com o seu vizinho alemão. A testemunhar essa integração atesta o batalhão de tanques holandês-alemão existente no Exército, assim como, uma cooperação e integração com as forças armadas alemãs nos domínios aéreo e naval."[118]

A Holanda possui acordos de policiamento aéreo com a França, Bélgica e Luxemburgo e é membro da *UK-led Joint Expeditionary,*[119] liderada pelo Reino Unido. A par com a Bélgica e com a Dinamarca comprometeu-se a formar um comando de operações especiais conjunto.

---

[116] ***Idem.***

[117] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html

[118] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 130

[119] ***UK-led Joint Expeditionary*** (Força Expedicionária Conjunta do Reino Unido (JEF)) é uma força expedicionária liderada pelo Reino Unido que pode agregar, conforme necessário, Dinamarca, Finlândia, Estônia, Letônia, Lituânia, Holanda, Suécia e Noruega

As forças holandesas são totalmente profissionais, bem treinadas e podem estabelecer e suportar, no exterior e por um período prolongado, uma força de média escala fazendo significativas contribuições para as operações militares da OTAN e da UE em todo o mundo.

O país possui equipamento militar moderno, de origem europeia e americana, e irá adquirir para a Marinha, em parceria com a Bélgica, novas fragatas e navios draga-minas e para a Força Aérea a aeronave de combate *F-35 Lightning II.*[120]

"O país tem uma avançada indústria de defesa com foco nos veículos blindados, navios e sistemas de defesa aérea, mas também abriga uma variedade de subsidiárias da empresa *Damen Schelde Naval Shipbuilding* que exporta fragatas, corvetas e embarcações de ataque rápido, enquanto a *DutchAero* fabrica componentes de motor para o *F-35*. A Holanda também colabora com a Alemanha na construção de veículos blindados *Boxer* e *Fennek."*[121]

Em 2014, a Holanda iniciou a edificação do Comando Cibernético de Defesa (CCD) tendo entrado em operação no início de 2017, fornecendo integração nas operações militares, assim como, capacidade cibernética ofensiva. Este Comando está instalado no Exército, mas inclui pessoal de todas as forças armadas, e em julho de 2018 ficou sob o comando direto do comandante das forças armadas.

Segundo o *Military Balance*, as forças armadas podem atacar, manipular e desativar os sistemas digitais dos oponentes, sendo esses potenciais oponentes outros estados, terroristas ou outras organizações ou *hackers*. Em novembro de 2018, foi publicada uma atualização da estratégia cibernética[122].

A Holanda tem, segundo a *GFP*, uma população de 17.151.228 pessoas e uma população disponível para ajudar num esforço de guerra de 7.820.960 (45.6%) e um *MFMS* de 6.334.978 (36.9%). Anualmente 196.384 pessoas (1,1%) atingem a idade de recrutamento militar tendo atualmente 40.500 (0,2%) de pessoas como capacidade militar sendo 35.500 (0.2%) no ativo e 5.000 na reserva.

A Holanda em termos militares conta com 56 ativos navais, fazendo parte integrante desses ativos os submarinos *SSK* da classe *Walrus*[123], os contratorpedeiros *DDGHM* e as fragatas *FFGHM* como principais combatentes de superfície com capacidade de helicópteros a

[120] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 130 e 131
[121] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 131 (Tradução livre do autor)
[122] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 132
[123] Os submarinos da classe ***Walrus*** são invisíveis quando submersos, silenciosos e, portanto, difíceis de serem detetados por navios, aviões e outros submarinos quando se escondem. Estes submarinos foram projetados especificamente para "caçar" submarinos russos durante a Guerra Fria.

bordo. A esta capacidade junta-se os navios patrulha e os draga-minas. Destes 56 ativos navais há a destacar 4 submarinos, 4 contratorpedeiros, 2 fragatas e 6 draga-minas.

No que ao Exército diz respeito, a Holanda tem como capacidade principal as viaturas blindadas *Fennek, CV9035NL, Bushmaster IMV* e os *Boxer*. Como armamento pesado possui os carros de combates *PzH 2000* e os morteiros *L16/M1* de 81 mm e os *Brandt* de 120mm. Em termos de capacidade antiaérea possuí os sistemas de mísseis *Patriot, NASAMS II* e *Stinger*. Nesta capacidade militar do Exército destacam-se os 18 carros de combate, os 1014 veículos blindados e as 57 peças de artilharia auto propulsada.

A Força Aérea é composta por 161 aeronaves distribuídas por 3 esquadras de ataque, com a aeronave *F-16,* 1 esquadra de busca e salvamento, com os helicópteros *NH90,* 2 esquadras de transporte, com as aeronaves *C-130* e *KDC-10,* 1 esquadra de helicópteros de ataque, com os AH-*64D Apache* e 3 esquadras de treino, com diversas aeronaves. Destas 161 aeronaves destacam-se os 60 aviões de ataque, 4 de transporte e por fim 95 helicópteros sendo 28 de ataque.

2.4. Caracterização da Dinamarca e sua capacidade militar

"Outrora sede de invasores vikings e mais tarde uma grande potência do norte da Europa, a Dinamarca evoluiu para uma nação moderna e próspera que participa da integração política e económica geral da Europa. Juntou-se à OTAN em 1949 e à CEE (agora UE) em 1973. No entanto, o país não optou por certos elementos do Tratado de Maastricht da UE, incluindo a União Económica e Monetária Europeia, a cooperação europeia em defesa e questões relativas a certas questões de justiça e assuntos internos."[124]

Segundo a *GlobalFirepower*, no que a capacidade militar diz respeito, a Dinamarca ocupa o 51.º lugar (entre 137 países considerados pela *GFP* na avaliação da capacidade militar) ao nível mundial, o 13.º lugar (de 25)[125] na União Europeia e no seio da OTAN ocupa a 16.ª posição (entre 27)[126].

2.4.1. Caracterização da Dinamarca

A Dinamarca tem uma área aproximada de 43.100 Km2 e encontra-se situada a sul da Escandinávia. O Reino da Dinamarca consiste na própria Dinamarca, nas Ilhas Faroé e na Groenlândia. "A Dinamarca propriamente dita, compreende a península da Jutlândia (*Jylland*) e 406 ilhas (97 delas habitadas). Exceto pela fronteira sul com a Alemanha, o país é cercado por água e o comprimento total da fronteira da Dinamarca é de 7.382 km, dos quais apenas 68 km são fronteira terrestre com a Alemanha."[127]

A capital da Dinamarca, Copenhague, está localizada na extremidade leste do país, na ilha de *Sjaelland*.

"O clima é temperado, húmido e nublado com invernos amenos e ventosos e verões frescos. Os seus recursos naturais são petróleo, gás natural, peixe, terras aráveis, sal, calcário, giz, pedra, cascalho e areia."[128]

---

[124] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/da.html (Tradução livre do autor)

[125] Chipre, Luxemburgo e Malta não estão incluídos nesta lista devido a condições e mínimos não atendidos pela *GFP*.

[126] A Islândia e o Luxemburgo não estão incluídos nesta lista devido a condições e mínimos não atendidos pela *GFP*.

[127] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 28 dez. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Denmark-LOCATION-SIZE-AND-EXTENT.html (Tradução livre do autor)

[128] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/da.html (Tradução livre do autor)

A Dinamarca possuí uma economia de mercado completamente moderna, apresentando uma indústria avançada com empresas líderes mundiais em produtos farmacêuticos, transporte marítimo e energia renovável. O setor agrícola dinamarquês é bastante desenvolvido e emprega alta tecnologia. Os dinamarqueses desfrutam de um alto padrão de vida, e a sua economia é caracterizada por extensas medidas de bem-estar do governo e uma distribuição equitativa da receita[129].

Considerada como forte exportador de alimentos, petróleo e gás, a Dinamarca, desfruta de um confortável excedente na balança de pagamentos, sendo, no entanto, dependente da importação de matérias-primas para o setor da indústria[130].

A Dinamarca é membro da UE, mas não adotou o euro. Apesar de cumprir previamente os critérios de adesão à União Económica e Monetária Europeia, a Dinamarca negociou uma opção de exclusão com a UE e não é obrigada a adotar o euro[131].

A Dinamarca está a passar por uma modesta expansão económica com taxas a rondar os 2%, em 2017. Com a taxa do desemprego a cifrar-se nos 5,5%, e com as empresas a enfrentar algumas dificuldades em encontrar trabalhadores qualificados para preencher posições, o governo dinamarquês, para colmatar essa carência, iniciou amplos programas para treinar pessoas desempregadas para trabalhar em setores que precisam desses trabalhadores qualificados.

Em termos orçamentais, a Dinamarca manteve um superavit saudável no orçamento por muitos anos até 2008. No entanto, a crise financeira global transformou esse saldo orçamental em deficit e desde de 2014 que o saldo tem comutado entre superavit e deficit. Este estado foi-se mantendo até 2019, ano em que o governo projetou um deficit de 0,7% e um valor de 34,8% do PIB para a dívida pública, que tem vindo a diminuir, pois em 2018 registava um valor de 35,6% do PIB.[132]

A Dinamarca tem um valor de *PIB per capita* (PPS) de 39.054,0 substancialmente acima da média europeia que se encontra nos 30.967,2[133].

Em termos de comunicações, a Dinamarca conta com excelentes serviços telefónicos e de Internet e o competitivo mercado de telecomunicações dinamarquês levou o país a ter a segunda maior taxa de penetração de banda larga na Europa. O setor de telefone fixo continua

[129] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/da.html
[130] ***Idem.***
[131] ***Idem.***
[132] ***Idem.***
[133] ***PORDATA, Base de dados Portugal contemporâneo*** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.pordata.pt/Europa/PIB+per+capita+(PPS)-1778

em declínio, em termos de receita, entretanto o *VoIP* (*Voice over Internet Protocol*) e as alternativas móveis têm tido um crescimento substancial. Os telefones de rede fixa têm um rácio de 26:100 (26 telefones por 100 pessoas) enquanto o telefone de rede móvel tem um rácio de 124:100 (dados de 2018)[134]. A Dinamarca também é um forte ponto de amarração de cabos submarinos como o *CANTAT-3*[135] e o *Havfrue/AEC-2*[136] que fazem parte das 34 séries de cabos submarinos de fibra ótica que ligam a Dinamarca ao Canadá, Ilhas Faroé, Alemanha, Islândia, Holanda, Noruega, Polónia, Rússia, Suécia, EUA e Reino Unido.

Em termos de ciência e tecnologia, a Dinamarca possui 29 sociedades especializadas de ensino nas áreas da ciência agrícola e veterinária, medicina, ciências naturais e tecnologia tendo como principal sociedade instruída a Academia Real Dinamarquesa de Ciências e Letras (fundada em 1742)[137]. Entre as principais instituições públicas de pesquisa estão diversas universidades como a Universidade de Copenhaga, considerada como uma das principais universidades europeias, a Universidade de *Aarhus* e a Universidade Técnica da Dinamarca que está na vanguarda das instituições de engenharia em todo o continente europeu, depois de se ter fundindo com outros cinco centros de pesquisa em 2007.

Os dados seguidamente apresentados à imagem e semelhança dos três anteriores países analisados (Portugal, Bélgica e Holanda) têm como fonte a reputada Instituição Europeia – *Eurostat*[138] e entre os inúmeros indicadores existentes escolhemos 5 para nos dar uma panorâmica do estado da ciência e tecnologia no País. Assim, os escolhidos foram os seguintes:

- Despesas em pesquisa e desenvolvimento (P&D);
- Recursos Humanos em Ciência e Tecnologia;
- Doutorandos nas áreas de Ciência e Tecnologia;
- Pedidos de patentes de alta tecnologia submetidos ao Instituto Europeu, e;
- Exportações de alta tecnologia.

---

[134] ***Idem.***

[135] ***CANTAT-3*** foi o terceiro cabo de telecomunicações transatlântico canadiense, em operação de 1994 a 2010, transportando inicialmente 3 x 2,5 Gbit / s entre o Canadá e a Europa. Ramifica à Islândia e às Ilhas Faroé.

[136] ***HAVFRUE*** é um cabo submarino que atravessa o Atlântico Norte e liga o norte da Europa continental aos EUA, com uma capacidade de 108Tbps ligando Nova Jersey, EUA, à Península da Jutlândia da Dinamarca.

[137] ***The Encyclopedia of the Nations*** [Em linha]. [Consult. 28 dez. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Denmark-SCIENCE-AND-TECHNOLOGY.html

[138] ***Eurostat*** é a Instituição de estatística da União Europeia com a sua sede no Luxemburgo. A sua missão é fornecer estatísticas de alta qualidade para a Europa. No cumprimento da sua missão, o Eurostat promove os seguintes valores: respeito e confiança, promoção da excelência, promoção da inovação, orientação para serviços, independência profissional. Procurando maneiras de melhorar continuamente seus produtos e serviços, o Eurostat ganhou o reconhecimento da Fundação Europeia para a Gestão da Qualidade "Comprometida com a Excelência" em novembro de 2016.

As despesas de P&D, consideradas, incluem todas as despesas governamentais de P&D e as realizadas pelo sector empresarial no território nacional durante um determinado período, independentemente da fonte de recursos. As despesas de P&D são mostradas como uma percentagem do PIB e na Dinamarca essas despesas foram (em 2018) de 3,03% do *PIB*, distante, positivamente, da média Europeia que se encontra nos 2,11% [139].

No que diz respeito aos Recursos Humanos em Ciência e Tecnologia considerámos a população ativa na faixa etária de 25 a 64 anos (ou seja, tendo concluído com êxito uma educação no terceiro nível ou sendo empregada em ciência e tecnologia). Neste indicador a Dinamarca está bem acima da média europeia (47,5% da população ativa) alcançando os 57,6%[140].

"Quanto aos doutorandos nas áreas de Ciência e Tecnologia este indicador considera todos os que participam no segundo estágio do ensino superior nas áreas de ciência e tecnologia, em percentagem da população com idade entre os 20 e os 29 anos. Este indicador, com um valor de 0,5% na Dinamarca igual à média europeia, inclui o número total de estudantes em programas de ensino superior que leva a uma qualificação avançada em pesquisa, nos campos educacionais Ciência, Matemáticas, Computação e Engenharias."[141]

Os dados sobre as patentes de alta tecnologia referem a proporção de pedidos feitos diretamente ao Escritório Europeu de Patentes (EPO) ou via Tratado de Cooperação de Patentes, por milhão de habitantes de um país. A definição de patentes de alta tecnologia utiliza subclasses específicas da Classificação Internacional de Patentes. A Dinamarca tem uma percentagem de 40,751%, desmesuradamente acima da média europeia que é 15,775%[142].

Como último indicador foi considerado aquele que nos dá a participação das exportações de todos os produtos de alta tecnologia no total das exportações. "Considerámos como produtos de alta tecnologia a soma dos seguintes produtos: aeroespacial, máquinas para escritório, computadores, eletrónica-telecomunicações, farmácia, instrumentos científicos, maquinaria elétrica, química, maquinaria não elétrica e armamento. Neste indicador uma vez mais fica claro a distância da Dinamarca ante a média europeia 4,0% e 9,4% respetivamente."[143]

---

[139] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00001/default/table?lang=en

[140] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00025/default/table?lang=en

[141] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00028/default/table?lang=en (Tradução livre do autor)

[142] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00010/default/table?lang=en

[143] ***Eurostat*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tin00140/default/table?lang=en (Tradução livre do autor)

Por fim, quanto ao desempenho digital, a Dinamarca encontra-se na 4.ª posição entre os 28 da EU segundo o Índice de Economia e Sociedade Digital (IESD)[144] que resume indicadores relevantes sobre o desempenho digital da Europa e acompanha a evolução dos estados membros da UE em competitividade digital observando 5 fatores, a saber:

- Conectividade - Evolução do mercado de banda larga;
- Capital Humano - Inclusão Digital e Habilidades;
- Uso de serviços de Internet;
- Integração da tecnologia digital.
- Serviços Públicos Digitais.

A Finlândia, a Suécia, a Holanda e a Dinamarca obtiveram as maiores pontuações no IESD 2019 e estão entre os líderes globais em digitalização[145].

2.4.2. Capacidade militar Dinamarquesa

As Forças Armadas Dinamarquesas são constituídas pelo Exército Real dinamarquês, pela Marinha Real dinamarquesa, pela Força Aérea Real dinamarquesa e a Guarda Nacional dinamarquesa (Reservas). O orçamento para a defesa, no ano de 2018, foi de 1,30% do PIB[146].

A idade mínima para integrar o serviço militar obrigatório e voluntário é aos 18 anos de idade e os recrutas cumprem um período de treino inicial que varia entre 4 a 12 meses, de acordo com a especialização. As mulheres são elegíveis para serem voluntárias no serviço militar. Para além do emprego de tempo integral, todos os ramos oferecem contratos de reserva[147].

As capacidades militares dinamarquesas permanecem compactas, mas eficazes, apesar de pressões sobre os orçamentos. Em janeiro de 2018, o governo emitiu um novo acordo de defesa para 2018–2023, prevendo um aumento dos gastos com a defesa para lidar com a deterioração do ambiente da segurança. Em particular, pretende-se reforçar a dissuasão, defesa cibernética e o papel da Dinamarca em operações internacionais, bem como, com a capacidade das forças armadas de apoiar as autoridades civis em tarefas de segurança nacional.

A Dinamarca, planeia montar uma brigada pesada, com capacidade de defesa aérea terrestre, e um batalhão de infantaria para assumir missões de patrulha e guarda em apoio à

[144] ***European Commission*** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/digital-single-market/en/desi
[145] ***Idem***.
[146] ***The World Factbook. Central Intelligence Agency*** [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/da.html
[147] ***Idem.***

polícia. Também estão nos planos dinamarqueses o fortalecimento da defesa aérea naval, bem como recursos antiguerra submarina.[148]

As ligações à *OTAN*, *NORDEFCO*[149] e a outros vizinhos regionais têm vindo a aumentar. Sendo disso exemplo o acordo de defesa, assinado em abril de 2015, com outros estados nórdicos, destinado a dissuadir a Rússia. A Dinamarca é membro da UE, mas não optou pela cooperação militar no âmbito da Segurança Comum e Política de Defesa. O novo acordo de defesa dinamarquesa prevê que o serviço nacional seja mantido e que a incorporação anual de recrutas deva aumentar[150].

As alterações e modernizações também chegaram à Força Aérea Real dinamarquesa, com a aquisição do *F-35A* para substituir os antigos *F-16.* Esta modernização foi confirmada em junho de 2016 quando o Ministério da Defesa dinamarquês declarou que a Dinamarca iria adquirir 27 *F-35A* e que iriam entrar em operação na Força Aérea a partir de 2026.

O suporte industrial que a *TERMA*[151], a maior empresa de defesa da Dinamarca, providencia a esta aeronave pode ter sido importante para a decisão de aquisição do *F-35A*, pois alguns subcomponentes são produzidos pela *TERMA* que é considerada como uma das principais fornecedoras globais do *F-35A*. No entanto, esta transição para esta nova plataforma, pode reduzir, temporariamente, a contribuição da Dinamarca para tarefas de policiamento aéreo da OTAN. A Dinamarca tem na industria de defesa um contribuinte importante nas exportações de eletrónicos de defesa e fabrico de componentes e subsistemas, tendo como destino prioritário a Europa e a América do Norte[152].

No que diz respeito ao ciberespaço, foi lançada, em dezembro de 2014, uma estratégia nacional para informação e segurança cibernética, de modo a que a Dinamarca para além da capacidade existente de defesa cibernética, adquirisse igualmente uma capacidade de conduzir operações militares defensivas e ofensivas no ciberespaço, ficando totalmente operacional em 2019. Para consecução desses objetivos foi criado o *Center for Cyber Security* (*CFCS*) que ficou integrado no Departamento de Inteligência de Defesa da Dinamarca e é a autoridade nacional de segurança para a tecnologia de informação e comunicações (*TIC*). O *CFCS* tem como três principais responsabilidades: contribuir para a proteção da Dinamarca contra ameaças cibernéticas; ajudar a garantir uma infraestrutura *TIC* robusta; e avisar, proteger e

[148] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 99
[149] ***NORDEFCO*** é uma cooperação que consiste na colaboração entre os países nórdicos no âmbito da defesa. Os seus são Dinamarca, Finlândia, Islândia, Noruega e Suécia.
[150] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 99
[151] ***TERMA*** – Empresa dinamarquesa que opera no sector aeroespacial, de defesa e da segurança. Com mais de 1.400 funcionários fabrica cerca de 70 peças para o F-35.
[152] ***The International Institute for Strategic Studies (IISS)*** - *The Military Balance 2019*. p 100

combater ataques cibernéticos. Todas estas responsabilidades, levaram a que o acordo para a Defesa 2018–23 já contemplasse um aumento significativo de recursos para o *CFCS*.

A Dinamarca tem, segundo a *GFP*, uma população de 5.809.502 pessoas e uma população disponível para ajudar em esforço de guerra de 2.590.457 (44.6%) e um *MFMS* de 2.093.089 (36.0%). Anualmente 77.444 pessoas (1,3%) atingem a idade militar e atualmente existem 61.500 pessoas (1.1%) com capacidade militar sendo 16.000 (0.3%) no ativo e 45.500 (0,8%) na reserva.

A Dinamarca, em termos militares, conta com 90 ativos navais distribuídos por fragatas como principais combatentes de superfície com capacidade de helicópteros a bordo, navios de patrulha, draga minas e navios de logística e suporte. Destes 90 ativos navais destacam-se 6 fragatas, 13 navios de patrulha e 12 draga minas.

Em relação ao Exército, este Ramo das Forças Armadas tem como capacidade principal as viaturas blindadas *Leopard 2A5* e os *CV9035 MkIII*. Como armamento pesado possui os canhões *Carl Gustav* de 84 mm e os *M109A3* de 155 mm e em termos de capacidade de arma antiaérea, possui o sistema de mísseis *Stinger*.

De todo este armamento do Exército destacamos os 57 carros de combate, os 1.068 veículos blindados, 18 peças de artilharia auto propulsada e 33 de reboque.

Quanto à capacidade aérea, a Dinamarca possui no total 113 aeronaves. Estas aeronaves estão distribuídas por 2 esquadras de ataque, com a aeronave *F-16*, 1 esquadra de guerra antissubmarina, com a aeronave *Super Lynx Mk90B*, 2 esquadras de busca e salvamento, com as aeronaves *AW101 Merlin* e *AS550 Fennec*, 1 esquadra de transporte, com a aeronave *C-130j-30* e a *CL-604 Challenger* e por fim uma esquadra de treino, com a aeronave *MFI-17 Supporter*. De toda esta força destacam-se os 33 aviões de ataque, os 4 de transporte e os 35 helicópteros sem que nenhum seja de ataque.

2.5. Síntese comparativa e conclusões

Uma comparação entre atores distintos no cenário internacional é sempre discutível e arriscada, especialmente quando essa comparação compreende apenas um pequeno grupo de parâmetros podendo desvalorizar outros, que em outro entender, possam ser determinantes para a análise que acabámos de efetuar.

No entanto, depois de um estudo e investigação achámos que utilizar alguns dos critérios aplicados na caraterização dos países no *The World Factbook* da *CIA* seria um bom ponto de partida para essa comparação, coadjuvados e alimentados por mais três ou quatro fontes importantes e conceituadas, de modo a que a nossa conclusão neste capítulo, chegasse a um desfecho consensual e que principalmente contribuísse para a demonstração de parte do nosso objetivo principal e o primeiro objetivo específico "que Portugal não é um *key player* na *OTAN* face às suas carências armamentistas" e que mesmo comparando com países congéneres essa capacidade é limitada.

Para este desiderato, escolhemos, a par com Portugal, a Bélgica, a Holanda e a Dinamarca, países de média dimensão europeia, fundadores da *OTAN* e membros de pleno direito da *EU* e da *Organização das Nações Unidas (ONU),* com responsabilidades europeias e mundiais ao nível da segurança e com consideráveis presenças em missões internacionais de Apoio à Paz em convénio com organizações como a *EU*, *OTAN* e *ONU*.

Assim, analisámos os países supracitados tendo por base dois vetores. O primeiro, generalista, agregando parâmetros como geografia, economia, comunicações e ciência e tecnologia e o segundo orientado e focado para a essência deste capítulo, a capacidade militar.

De acordo com os dados analisados, Portugal é o maior país dos quatro sendo três vezes maior do que a Bélgica e duas vezes maior do que a Holanda e Dinamarca, mas em termos populacionais encontra-se em terceiro lugar tendo praticamente o dobro da população da Dinamarca, mas somente 60% da população da Holanda e com uma diferença em cerca 1 milhão e duzentas mil de pessoas, a menos, para a Bélgica. O rácio militar, por habitante, é muito idêntico em Portugal, Bélgica e Dinamarca com 1:339, 1:385 e 1:363 respetivamente, mas tem um incremento na Holanda com um rácio de 1:483.

Em termos económicos os países "mais a norte da Europa" revelam uma maior capacidade económica do que Portugal, comprovado nos dados apresentados durante este capítulo. O *PIB per capita* (*PPS*) dos três países (Bélgica, Holanda e Dinamarca) encontra-se 15% a 30% superior à média europeia enquanto Portugal regista um valor de cerca 25% abaixo da média europeia.

Por último, ainda em relação ao primeiro vetor, nos parâmetros comunicações e ciência e tecnologia, Portugal encurta distâncias e disputa posições com os restantes três países, no que a comunicações diz respeito, mas em termos de ciência e tecnologia, com 4 dos 5 indicadores abaixo da média europeia, ainda tem um longo caminho a percorrer face aos 3 indicadores acima da média europeia da Bélgica e Dinamarca e os 4 indicadores acima da média europeia da Holanda, sendo curioso o único indicador em que Portugal tem um valor positivo (acima da média europeia) batendo os restantes países – Doutorandos nas áreas de Ciência e Tecnologia.

Em termos de estratégia nacional para a defesa, conforme consta nos seus documentos orientadores, os quatro países em análise e comparação não têm uma abordagem muito díspar, contribuindo para esse alinhamento o facto de todos serem membros da OTAN e a EU.

Portugal face à revisão estratégica de 2013 estabeleceu como tarefa uma redução na força do Exército, associando uma mudança organizacional, dividindo os serviços em forças de reação rápida, forças de defesa permanentes e forças modulares, de modo a melhor responder aos novos teatros de operações. A lei de programação militar, recentemente aprovada, patrocina a ambição de Portugal no campo da reação rápida, capacidade de vigilância marítima e nas operações multinacionais, indo ao encontro das principais tarefas, consagradas na revisão estratégica, a defesa da pátria, a segurança marítima, as operações multinacionais e a resposta a desastres humanitários.

Em julho de 2016, o governo belga publicou a sua visão estratégica para a Defesa até o ano de 2030 onde propõe uma consolidação até 2020 e um crescimento até 2030. O objetivo é a procura de altos níveis de prontidão e a capacidade de destacar forças principalmente no âmbito da *EU* e da *OTAN*. Em termos de pessoal tenciona reduzir para cerca de 25.000 elementos.

A Bélgica, devido ao seu tamanho e capacidade limitada, colabora frequentemente com os seus vizinhos e comprometeu-se com a Dinamarca e a Holanda a formar um comando de operações especiais combinadas.

A Holanda para além do comando combinado referido anteriormente, possui acordos de policiamento aéreo com a França, Bélgica e Luxemburgo e é membro da *UK-led Joint Expeditionay* liderada pelo Reino Unido. Em 2018, a nova estratégia da defesa encarrega as forças armadas de medidas territoriais de defesa e apoio às autoridades civis nacionais na aplicação da lei e a ajuda em desastres e assistência humanitária.

A Dinamarca é membro da *UE*, mas não optou pela cooperação militar no âmbito da Segurança Comum e Política de Defesa, no entanto, tem vindo a celebrar acordos de defesa, com outros estados nórdicos, com o objetivo de dissuadir a Rússia de qualquer ato.

Em janeiro de 2018, o governo dinamarquês emitiu um novo acordo de defesa para 2018–2023, prevendo um aumento dos gastos com a defesa para reforçar a dissuasão, defesa cibernética e aumentar o papel da Dinamarca em operações internacionais, nunca descurando a capacidade das forças armadas em apoiar as autoridades civis em tarefas de segurança nacional. A Dinamarca planeia fortalecer a capacidade de defesa aérea terrestre, defesa aérea naval e recursos antiguerra submarina, assim como, o patrulhamento e guarda em apoio à polícia.

O novo acordo de defesa prevê que o serviço nacional é mantido e que a incorporação anual de recrutas deve aumentar.

O nível de ambição dos diferentes países analisados em relação à sua estrutura militar, equipamento e sistema de forças é muito fruto e proporcional aos recursos financeiros postos à disposição da Defesa. Assim, embora a percentagem em relação ao *PIB* não seja muito díspar 0,93% para a Bélgica, 1,21% para a Holanda, 1,30% para a Dinamarca e 1,43% para Portugal quando analisamos em termos de valor (em euros), essas diferenças são exponenciadas em consequência da riqueza desse país. Enquanto Portugal é o país que mais esforço faz em relação à sua riqueza já a Bélgica está em completo contraste 1,43% e 0,93%, respetivamente. Mas em valor, segundo o *Military Balance* (2019) a diferença entre os valores que foram postos à disposição da Defesa em 2018 foi de cerca de dois mil milhões de euros, 2,18 mil milhões de euros para Portugal e 4,20 mil milhões de euros para a Bélgica.

Esta diferença é agudizada quando falamos da Holanda e da Dinamarca e à imagem e semelhança da Bélgica o valor em euros distancia-se do português. Assim são postos à disposição da Defesa na Holanda 9,53 mil milhões e 3,82 mil milhões[153] para a Dinamarca (conversão de dólar para euro ao câmbio do dia 12jan2020).

Para podermos concluir, resta-nos analisar a capacidade militar dos quatro países fazendo recurso a uma tabela que exibe alguns dos dados apresentados no decorrer deste capítulo com recurso a uma única fonte para que essa comparação seja a mais fidedigna possível. Essa fonte é a *GFP* que avalia os valores individuais de cada País e, fazendo recurso a uma fórmula interna para gerar a pontuação, denominada *PwrIndx* (*PowerIndex*), estabelece as classificações *GFP* num determinado ano (neste caso o ano de 2019).

[153] ***Banco de Portugal*** **Conversor de moeda do Banco de Portugal.** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.bportugal.pt/conversor-moeda?from=USD&to=EUR&date=1578787200&value=4250000000

GlobalFirepower				
Comparison Results of World Military Strengths				
Subjects	Portugal	Bélgica	Holanda	Dinamarca
GFP Rank	67 (of 137)	68 (of 137)	35 (of 137)	51 (of 137)
**Value of 0.0000 Being Ideal*	0.9611	0.9633	0.6063	0.7767
Total Population	10 355 493	11 570 762	17 151 228	5 809 502
Manpower Available	4 804 949	4 833 107	7 820 960	2 590 457
Fit-for-Service	3 953 253	3 841 305	6 334 978	2 093 089
Reaching Military Age	118 058	115 239	196 384	77 444
Active Personnel	30 500	30 000	35 500	16 000
Reserve Components	212 000	5 000	5 000	45 500
Total Military Personnel	242 500	35 000	40 500	61 500
Total Aircraft	87	158	161	113
Fighters / Interceptors	24	43	60	33
Attack Aircraft	24	43	60	33
Transports	11	14	4	4
Trainers	18	69	21	37
Helicopters	25	32	95	35
Attack Helicopters	0	0	28	0
Serviceable Airports	64	41	29	80
Tank Strength	186	0	18	57
Armored Fighting Vehicles	700	984	1 014	1 068
Self-Propelled Artillery	0	0	57	18
Towed Artillery	33	0	0	33
Rocket Projectors	0	0	0	0
Total Naval Assets	41	17	56	90
Aircraft Carriers	0	0	0	0
Submarines	2	0	4	0
Frigates	5	2	2	6
Destroyers	0	0	4	0
Corvettes	0	0	0	0
Patrol Craft	19	2	4	13
Mine Warfare Craft	0	5	6	12
Merchant Marine Strength	466	185	1 244	654
Major Ports & Terminals	4	6	6	7
Coastline Coverage (km)	1 793	67	451	7 314
Shared Borders (km)	1 224	1 297	1 053	140
Square Land Area (km)	92 090	30 528	41 543	43 094

Tabela 1 Resultado de comparação das Forças Militares Mundiais

Fonte: Sítio *GlobalFirepower*

Em termos de capacidade militar Portugal ocupa o 67.º lugar ao nível mundial (entre 137 países considerados pela *GFP* na avaliação da capacidade militar), o que significa que se encontra no limiar do meio da tabela sendo reflexo da sua débil capacidade militar. Em comparação com os restantes três países só a Bélgica se encontra ainda abaixo de Portugal, no 68.º lugar. Holanda e Dinamarca encontram-se alguns lugares acima, embora a Holanda se encontre substancialmente acima com os 35.º e 61.º lugares respetivamente.

Deixando a perspetiva mundial e passando para uma perspetiva europeia, os valores pioram para Portugal pois deixa de estar a meio da tabela e passa para uns lugares abaixo desse patamar ocupando o 18.º lugar (de 25). A Bélgica continua um lugar abaixo e a Holanda e a Dinamarca continuam com a mesma preponderância manifestada a nível mundial, ocupando os 10.º e 13.º lugares entre os 25 países da EU, abrangidos na análise da *GFP*.

O cenário não muda de figura quando analisamos a *OTAN*. Portugal e Bélgica separados por um lugar, ocupam a segunda parte da tabela com os lugares 19.º e 20.º e a Holanda e a Dinamarca ocupam a primeira parte da tabela com a Holanda em lugar de destaque, no 12.º lugar, enquanto Dinamarca ocupa a 16.ª posição.

Em termos de armamento Portugal tem uma boa posição em termos de Marinha, mas perde nos outros dois Ramos (Exército e Força Aérea).

Em jeito de conclusão e segundo o ranking da *GFP*, Portugal encontra-se em 3.º lugar entre os quatro países em análise e comparação, ficando somente à frente da Bélgica. Os dados são contundentes e chegámos, em nossa opinião, a um desfecho consensual demonstrando parte do nosso objetivo principal e o primeiro objetivo específico "que Portugal não é um *key player* na OTAN face às suas carências armamentistas" e que mesmo comparado com países congéneres essa capacidade é limitada.

Durante a evolução deste capítulo, na análise da capacidade militar dos países em geral e destes quatro em particular, houve algo que começou a surgir na literatura com grande assiduidade, passando até a ser corriqueiro e consensual, que é o facto de a cibernética fazer parte da capacidade militar. Prova dessa escalada é a menção e o espaço que uma das literaturas de referência da capacidade militar, *The Military Balance* do *The International Institute for Strategic Studies* reserva ao *Cyber*, já muito próximo daquilo que dedica aos outros domínios da guerra.

Por outro lado, é uma constatação de que todos os países que analisámos neste capítulo tem, já hoje, uma estratégia de ciberdefesa.

Assim sendo, a pergunta impõe-se: será que o ciberespaço a par da terra, água, ar e espaço é um novo domínio da guerra? É o que iremos analisar no capítulo seguinte.

3. O Ciberespaço – o quinto domínio das operações militares

> *"AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, "was the most monumental non-nuclear explosion and fire ever seen from space."*[154]

Esta foi uma das primeiras demonstrações do poder de uma "bomba lógica".

Três décadas depois, com mais e mais sistemas vitais conectados à Internet, os inimigos poderiam usar bombas lógicas para, por exemplo, desligar a eletricidade do outro lado do mundo? Poderiam terroristas ou *hackers* causar caos financeiro ao adulterar os sistemas de negociação computadorizados de *Wall Street*? E, como os *chips* e *softwares* de computador são produzidos globalmente, uma potência estrangeira poderia infetar equipamentos militares de alta tecnologia com *bugs* de computador? *"It scares me to death"*, diz uma fonte militar sénior do Exército americano. *"The destructive potential is so great."*[155]

Após terra, mar, ar e espaço, a guerra entrou no quinto domínio: ciberespaço. O presidente *Barack Obama* declarou a infraestrutura digital da América como um "ativo estratégico nacional" e nomeou *Howard Schmidt*, ex-chefe de segurança da *Microsoft*, como seu *czar* de segurança cibernética. Em maio de 2010, o Pentágono instalou o seu novo *Cyber Command* (*Cybercom*), liderado pelo general *Keith Alexander*, diretor da Agência de Segurança Nacional (*NSA*)[156].

> *His mandate is to conduct "full-spectrum" operations — to defend American military networks and attack other countries' systems. Precisely how, and by what rules, is secret*[157].

[154]Economist. ***War in the fifth domain*** [Em linha]. 2010. [Consult. 22 dez. 2019]. Disponível em https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.
[155] ***Idem.***
[156] ***Idem.***
[157] ***Idem.***

A Grã-Bretanha também criou uma política de cibersegurança e um "centro de operações" baseado no *GCHQ*[158], o equivalente britânico da agência americana *NSA*[159].

A estratégia nacional de segurança cibernética britânica, para 2016-2021, tem uma abordagem ambiciosa e deliberadamente intervencionista, apoiada por um investimento de 1.9 bilhões de libras, para fortalecer a segurança cibernética e a resiliência, de modo a que o Reino Unido seja líder mundial em segurança cibernética.

> *"In the three years since its inception, the National Cyber Security Strategy has transformed the UK's fight against cyber threats. Through an ambitious, deliberately interventionist approach, backed by an investment of £1.9 billion, it has put in place many of the building blocks to strengthen our cyber security and resilience for the future. It has also helped to establish the UK as a world-leader in cyber security, with other countries looking to our Strategy – and our pioneering National Cyber Security Centre – as a model for a comprehensive, forward-looking approach."*[160]

A China fala em "vencer guerras informadas em meados do século 21".

> *"Efforts should be made to build our country into a network powerhouse."*[161]
> *Xi Jinping* [162]

Muitos outros países, entre eles a Rússia, Israel e a Coreia do Norte, estão a organizar-se para a guerra cibernética. O Irão afirma, orgulhosamente, de ter o segundo maior exército cibernético do mundo.

Como será a guerra neste quinto domínio?

Richard Clarke, ex-funcionário da Casa Branca encarregado do combate ao terrorismo e cibersegurança prevê, no seu novo livro, um colapso catastrófico em 15 minutos, "Defeitos nos programas deixam militares sem acesso a sistemas de email; refinarias de petróleo e oleodutos explodem; sistemas de controle de tráfego aéreo colapsam; comboios de carga e metro

---

[158] ***Government Communications Headquarters***, conhecido como GCHQ, é uma organização de inteligência e segurança responsável por fornecer inteligência e garantir informações ao governo e às forças armadas do Reino Unido.

[159] ***National Security Agency,*** conhecida como NSA é a agência de segurança dos Estados Unidos, criada em 4 de novembro de 1952 com funções relacionadas com a inteligência, incluindo intercetação e criptoanálise.

[160] Progress Report. ***Chancellor of the Duchy of Lancaster National Cyber Security Strategy 2016 – 2021*** [Em linha]. 2019. [Consult. 22 dez. 2019]. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf.

[161] Economist. ***War in the fifth domain*** [Em linha]. 2010. [Consult. 22 dez. 2019]. Disponível em https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

[162] ***Xi Jinping*** é atualmente o principal membro do Secretariado do Partido Comunista Chinês, o presidente da China, o diretor da Escola Central do Partido Comunista da China, e o mais importante membro do Comitê Permanente do Politburo.

descarrilam; dados financeiros são modificados; a rede elétrica cai no leste dos Estados Unidos; satélites em órbita ficam fora de controle. Logo que os alimentos se tornem escassos a sociedade quebra e o dinheiro acaba. O pior de tudo é que a identidade do atacante pode permanecer um mistério."[163]

Como acabámos de observar, os principais países do mundo estão a preparar-se, de uma forma ou de outra, para aquilo que já hoje é uma realidade – o quinto domínio da guerra.

Neste capitulo, tentaremos demonstrar o nosso segundo objetivo específico "Demonstrar que o ciberespaço como sistema do caos, com um caráter de desterritorialização e omnipresença, é tão crítico para a defesa nacional e internacional, quanto os domínios clássicos da terra, do mar, do ar e do espaço, sendo por isso apelidado como o quinto domínio das operações militares. Ao mesmo tempo, representa um desafio aos conceitos militares tradicionais em todos os níveis da guerra: estratégica, operacional e tática."

O ciberespaço toca praticamente tudo e todos, fornecendo uma plataforma para inovação e prosperidade e os meios para melhorar o bem-estar geral em todo o mundo. Porém, a constatação de que a infraestrutura digital é fraca e pouco regulamentada pode gerar grandes vulnerabilidades, ameaçando nações, empresas privadas e direitos individuais.

Segundo o sítio oficial do *Department of Homeland Security*, dos Estados Unidos da América, o governo tem a responsabilidade de lidar com essas vulnerabilidades estratégicas para garantir que os Estados Unidos e seus cidadãos, juntamente com a maior comunidade de nações, possam realizar e potenciar uma revolução da tecnologia da informação[164].

Mas afinal o que é o ciberespaço?

Existem muitas definições do que é o ciberespaço. Deixamos aqui algumas, umas mais abrangentes do que outras, mas todas elas referenciadas na revisão bibliográfica.

O CNCS[165] , utilizando como fonte a Associação para a Promoção e Desenvolvimento da Sociedade de Informação, diz-nos que o ciberespaço é uma metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar de diferentes maneiras, por exemplo, através de mensagens eletrónicas, em salas de conversa ou em fóruns de discussão.

---

[163] Economist. ***War in the fifth domain*** [Em linha]. 2010. [Consult. 22 dez. 2019]. Disponível em https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

[164] CISA. ***2009 Cyberspace Policy Review*** [Em linha]. 2009. [Consult. 15 dez. 2019]. Disponível em https://www.cisa.gov/publication/2009-cyberspace-policy-review.

[165] ***CNCS – Centro Nacional de Cibersegurança*** atua como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de Infraestruturas Críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático.

Por sua vez, o Departamento de Defesa dos Estados Undos da América, no seu *Dictionary of Military and Associated Terms (DOD),* diz-nos que:

> ***"Cyberspace** — A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*."

Do Reino Unido, no *UK National Cyber Security Strategy 2016-2021*:

> ***"Cyberspace** is the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept."*

Preparado pelo grupo internacional de especialistas a convite do centro de excelência em defesa cibernética da OTAN, a publicação *Tallinn Manual on the internacional law applicable to cyber warefare*, (Tallinn, 2013, p. 212), diz-nos que:

> ***"Cyberspace** the environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify and Exchange data using computer networks."*

Por último a definição a sob a égide do *NATO Glossary of Terms and Definitions AAP-06 – Edition 2019*, diz-nos que:

> ***"Cyberspace / Cyberespace** The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data."*

Depois de uma série de definições de organismos de referência nesta área, digamos que muito coincidentes, deixamos aqui, aquela que muitos autores asseguram ser a origem do termo ciberespaço, com a contribuição da ficção científica, tal como aparece no romance *Neuromancer*[166]

[166] ***Neuromancer***, de William Gibson, é um dos mais famosos romances do género alternativo de ficção cientifica publicado em 1984, que introduzia novos conceitos para a época, como inteligências artificiais avançadas, uma rede de *matrix* e um ciberespaço quase que "físico".

*"**Cyberspace.** A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."*

3.1. A importância crescente do Ciberespaço

Hoje em dia, poucos são aqueles que são capazes de refutar a importância crescente do ciberespaço no mundo atual, quer seja nos negócios, nas telecomunicações, nas empresas, nas organizações públicas e privadas, na comunicação entre as pessoas, na cultura, na economia, em suma, em toda atividade em que estamos envolvidos diariamente.

Segundo *The Rt Hon Francis Maude MP Minister for the Cabinet Office and Paymaster General*, (GOV.UK, 2011) "O crescimento da internet foi a maior mudança social e tecnológica da minha vida. É uma força enorme para o bem no mundo, na maneira como promove o crescimento, reduz as barreiras ao comércio e permite que pessoas de todo o mundo se comuniquem e cooperem. Como vimos nesta primavera no mundo árabe, pôde ajudar a dar voz ao inédito e responsabilizar os governos. Terá um papel enorme a desempenhar no apoio ao desenvolvimento sustentável nos países mais pobres. Ao mesmo tempo, a nossa crescente dependência do ciberespaço trouxe novos riscos, dados e sistemas importantes nos quais agora confiamos possam ser comprometidos ou danificados, de maneiras difíceis de detetar ou defender"[167].

William Gibson, em 1984, utilizou o termo ciberespaço num livro de sua autoria intitulado *Neuromancer*. Este livro, de ficção científica, apresentava novos conceitos para a época, como a inteligência artificial e um espaço de comunicação aberta de interligação mundial entre todos os computadores designado – ciberespaço.

Passados 30 anos, em 2016, o conceito é uma realidade e na Cimeira de Varsóvia de 2016, a OTAN considerou o ciberespaço como um domínio operacional oficial de guerra, tais como o são a terra, o mar e o ar.

"We also turned our attention to cyberspace.

[167] GOV.UK. ***The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.*** Introduction by the Rt Hon Francis Maude MP, Minister for the Cabinet Office [Em linha]. 2011. [Consult. 03 nov. 2019]. Disponível em https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. (tradução livre do autor)

> *We agreed that we will recognise cyberspace as an operational domain just like air, sea and land.*
> *Cyber defence is part of collective defence. Most crises and conflicts today have a cyber dimension.*
> *So treating cyber as an operational domain would enable us to better protect our missions and operations.*
> *All our efforts to strengthen defence and deterrence depend on the right capabilities and the right resources."*[168]

No mundo interconectado e globalizado de hoje, a segurança cibernética tornou-se extremamente importante para os Estados. Os Estados desenvolvidos contam com sistemas informatizados nas principais áreas, como são a defesa nacional, as infraestruturas, os sistemas bancários e, como não poderia deixar de ser todo o comércio eletrónico dentro e fora das suas fronteiras.

O ciberespaço tornou-se, assim, num espaço apetecível para ataques cibernéticos capazes de afetar gravemente a tranquilidade das populações, podendo mesmo ter como consequência perdas relevantes no plano económico, de vidas humanas, constituindo-se como uma ameaça séria à defesa nacional.

O primeiro grande ciberataque foi em 2007 e teve a Estónia como alvo (Graça, 2013). Com início a 27 de abril de 2007 a Estónia sofreu inúmeros ciberataques a diversos servidores da sua infraestrutura nacional de internet que deixaram vários sites governamentais fora de serviço.

A arma utilizada para estes ataques foi o *DDoS* (*Distributed Denial of Service*) (Graça, 2013) que se materializa em um computador *master* ter sob seu comando milhares de outros computadores e faz com que todos esses computadores executem um pedido de serviço a uma mesma hora a um determinado servidor fazendo com que este colapse por incapacidade de atender a todos os pedidos.

Este tipo de ataques, para além de indisponibilizarem os acessos aos sites, por algumas horas, não causam danos permanentes. No entanto, mostram como os sistemas ligados à Internet são vulneráveis e este foi o primeiro aviso para vários países com serviços idênticos e que poderiam vir a ser futuros alvos de ataques.

[168] NATO. ***Press conference by NATO Secretary General Jens Stoltenberg*** following the North Atlantic Council meeting at the level of NATO Defence Ministers [Em linha]. 2016. [Consult. 19 set. 2019]. Disponível em http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

O segundo ataque ocorreu no verão de 2008, e teve um cariz mais militar (Graça, 2013). Este foi o primeiro caso em que um ciberataque ocorreu de um modo sincrónico com um ataque convencional e aconteceu no conflito que opôs a Geórgia à Rússia (Crowell, 2017).

Se dúvidas restavam, este acontecimento esclareceu que havia um novo espaço para o conflito armado – o ciberespaço.

O terceiro ataque atingiu maior grau de sofisticação (Richardson, 2011). Em 2010, as centrifugadoras usadas no programa nuclear do Irão, instaladas em *Natanz*, foram atacadas com o *malware*[169] *Stuxnet* que fez com que as centrifugadoras, usadas para enriquecer urânio, começassem a funcionar erraticamente, até se autodestruírem, apesar de os instrumentos de monitorização indicarem estar tudo bem.

Estes três exemplos reforçam a ideia de que o novo espaço de guerra está aí, obrigando os Estados a aumentar a prevenção e a criar uma capacidade de ciberdefesa de forma a combater os efeitos desses ataques e retardar, ou mesmo inibir, os ciberataques. Todos eles diferentes, mas com um ponto em comum:

– Em nenhum deles se provou o culpado pelo ataque.

> *"No caso da ciberguerra, a questão da relevância dos atores não estaduais levanta-se com especial acuidade. Os exemplos dos ciberataques mais conhecidos – Estónia (2007) e Geórgia (2008), ao qual se poderá juntar o caso do ataque do vírus Stuxnet (2010), às instalações nucleares do Irão –, podem ser vistos como uma espécie de «guerras por procuração». De facto, o ponto comum é que ocorreram ciberataques contra esses estados, mas, oficialmente, não têm qualquer autoria de outros estados. Aparentemente, a responsabilidade caberia apenas a elementos da «sociedade civil»: netizens («cibercidadãos»), ativistas ou «hackers patrióticos». Estes, teoricamente, atuariam de motu próprio, à margem e sem qualquer conhecimento dos estados dos quais são cidadãos."*[170]

Portugal tem estado atento a esta nova realidade *"cyber"*. Muito se tem dito e escrito sobre o assunto e o governo também tem percebido a importância do ciberespaço e tudo o que nele circula e, por isso, tem legislado sobre esta matéria.

A Resolução do Conselho de Ministros n.º 36/2015, "aprovou a primeira Estratégia Nacional de Segurança do Ciberespaço, visando aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por

[169] ***Malware*** é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros softwares.

[170] FERNANDES, José Pedro Teixeira - ***A ciberguerra como nova dimensão dos conflitos do século XXI*.** p. 60.

parte de todos os cidadãos e das entidades públicas e privadas. Face ao rápido desenvolvimento intrínseco ao ciberespaço e, consequentemente, à crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização, ficou definido que a referida estratégia seria objeto de revisão num prazo de três anos."[171]

> *A sociedade, a economia e o Estado são dependentes das tecnologias de informação e de comunicação (TIC). Temos assistido a um desenvolvimento acelerado da sociedade da informação e a uma crescente dependência das TIC em funções vitais do funcionamento do País. A definição de uma agenda digital permite disponibilizar benefícios económicos e sociais, estimular a criação de emprego, a sustentabilidade e a inclusão social, extrair o máximo benefício das novas tecnologias e melhorar a estrutura de enquadramento nacional. Estas tecnologias são, no entanto, vulneráveis, criando riscos sociais e materiais. Se, por um lado, trazem claros benefícios à sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos. O ciberespaço transpõe a vida real para um mundo virtual, com características únicas que impõem novas formas de interação e de relacionamento.*[172]

No entanto, existem autores, como *Thomas Rid*, que duvidam que alguma vez a guerra cibernética esteja a chegar. Mas *Rid* vai mais longe e diz-nos que a guerra cibernética nunca ocorreu no passado, não está a ocorrer e que muito provavelmente não irá ocorrer no futuro (Rid, 2011).

> *"For almost two decades, experts and defense establishments the world over have been predicting that cyber war is coming. But is it? This article argues in three steps that cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the."*[173]

Segundo *Brandon Valeriano* (2013) *(Ph.D. Vanderbilt University)* "*Thomas Rid* escreveu um volume importante em um momento crítico no debate sobre conflitos cibernéticos (...) o seu argumento é baseado na lógica e num compromisso cuidadoso do que realmente significa o termo "guerra" (...) *Cyber War Will Not Take Place* é um texto fundamental no campo da

[171] DRE. ***Texto inicial da Resolução do Conselho de Ministros n.º 92/2019*** que a Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 [Em linha]. 2019. [Consult. 03 dez. 2019]. Disponível em https://dre.pt/web/guest/home/-/dre/122498962/details/maximized.
[172] DRE. ***Resolução do Conselho de Ministros*** n.º 36/2015 [Em linha]. 2015. [Consult. 19 set. 2019]. Disponível em https://dre.pt/home/-/dre/67468089/details/maximized?p_auth=pKf7McIZ.
[173] RID, Thomas – ***Cyber War Will Not Take Place***. p. 5.

segurança cibernética e qualquer académico responsável deve usar esse volume para combater a perspetiva divergente."[174]

3.2. Ataques cibernéticos

Carl von Clausewitz, em o seu livro Da Guerra diz-nos que "A guerra é, portanto, um ato de força para obrigar nosso inimigo a fazer nossa vontade"

Desde do Tratado de *Vestefália*, que a guerra passou a ser definida como força dirigida pelo Estado para alcançar fins políticos. Decorrente deste tratado, um vasto conjunto de diplomas deu início ao moderno sistema Internacional respeitando noções e princípios, como o de soberania estatal[175] e o de estado-nação[176]. Segundo *Jubilut* (2010), "embora o imperativo da paz tenha surgido em decorrência de uma longa série de conflitos generalizados, surgiu com eles a noção embrionária de que uma paz duradoura derivava de um equilíbrio de poder, noção essa que se aprofundou com o Congresso de Viena (1815) e com o Tratado de Versalhes (1919). Por essa razão, a Paz de *Vestefália* costuma ser o marco inicial do Direito Internacional clássico e uma das bases de estudo das Relações Internacionais."

Entretanto a "evolução da guerra" tem vindo a verificar-se quer nas abordagens, quer nos meios. Segundo Fernandes (2012), "De facto, se pensarmos em vários conflitos do passado recente verificamos que houve guerra – casos do *Kosovo* em 1999, do Afeganistão em 2001, do Iraque em 2003, do Líbano em 2006 –, sem declaração formal de guerra de Estado a Estado. Verificamos, também, que nem sempre as partes em confronto são estados – casos, por exemplo, da *Al-Qaida* e dos *taleban* no Afeganistão versus Estados Unidos/NATO, ou do *Hezbollah* no Líbano versus Israel."

A tecnologia tem contribuído muito para esta evolução. Não só invadiu as nossas casas, os nossos locais de trabalho e mesmo as nossas vidas, trazendo não só facilidades e melhorias ao nosso quotidiano, mas também tem trazido ameaças. Aquilo a que habitualmente chamamos

[174] Valeriano, Brandon. **Review Essay of Thomas Rid's Cyber War Will Not Take Place.** [Em linha]. 2013. [Consult. 02 dez. 2019]. Disponível em https://issforum.org/essays/17-cyber-war-will-not

[175] **Soberania estatal** - A autoridade imposta à sociedade permite que certos limites não sejam ultrapassados, coibindo abusos e permitindo a organização de uma estrutura estatal.

[176] E**stado-nação –** É uma área histórica que pode ser identificada como possuidora de uma política legitimada, que pelos próprios meios, constitui um governo soberano. Enquanto um estado é uma entidade política e geopolítica, uma nação é uma unidade étnica e cultural. O termo "estado-nação" implica uma situação onde os dois são coincidentes. O Estado-nação afirma-se por meio de uma ideologia, uma estrutura jurídica, a capacidade de impor uma soberania, sobre um povo, num dado território com fronteiras, com uma moeda própria e forças armadas próprias também.

segurança, tem hoje, um novo estrato que não vem do mundo real, mas sim do mundo virtual trazendo ameaças que vêm por um simples cabo de rede e/ou simplesmente pelo ar.

"Porém, junto com esta rápida evolução, também vieram novas ameaças, que proporcionalmente à modernidade dos novos recursos, também trazem constantes desafios para a segurança. Mas não a segurança que estávamos acostumados há alguns anos atrás no "mundo físico", mas sim num mundo novo e virtual – o espaço cibernético, ou simplesmente "ciberespaço" – um espaço virtual composto por cada computador e usuário conectados na rede mundial, a internet, onde as pessoas passam a criar conexões e relacionamentos capazes de fundar um espaço de sociabilidade virtual."[177]

Face a esta nova realidade, os ataques cibernéticos ganham espaço nesta "nova maneira de fazer guerra" quase sempre, sem rosto. "Todavia, a revolução tecnológica e digital em marcha desde finais do século passado está, indiscutivelmente, a transformar a economia, a sociedade e a maneira de fazer a guerra. Tanto quanto é possível avaliar hoje, a tendência é para que o ciberespaço – entendido como a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores – se transforme, também, numa nova dimensão dos conflitos internacionais. Apesar das dificuldades de avaliação das reais consequências de uma genuína ciberguerra, é de recear que estas possam ser bem destrutivas para o normal funcionamento de sociedades complexas."[178]

3.2.1. Ataque à Estónia em 2007

Segundo *Jon Brodkin*, na *Computerworld*, e tendo por base o Relatório Virtual de Criminologia[179] da *McAfee*[180], publicado a 30 de novembro de 2007 e produzido com contribuições da OTAN, do *Federal Bureau of Investigation* (FBI), da Agência de Crimes Graves Organizados do Reino Unido e de vários grupos e universidades, com o objetivo de avaliar a segurança cibernética global àquela altura, "governos e grupos aliados em todo o mundo usam a Internet para espionar e lançar ataques cibernéticos aos seus inimigos, visando

[177] Luciano Marques. ***Risco Cibernético: A Ameaça Real do Mundo Virtual*** [Em linha]. 2019. [Consult. 13 dez. 2019]. Disponível em https://administradores.com.br/artigos/risco-cibernetico-a-ameaca-real-do-mundo-virtual

[178] José Pedro Teixeira Fernandes. ***A ciberguerra como nova dimensão dos conflitos do século XXI.*** [Em linha]. 2012 [Consult. 24 nov. 2019]. Disponível em *http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri33/n33a05.pdf*

[179] Department of Computer Science. ***McAfee Virtual Criminology Repo***rt [Em linha]. 2007. [Consult. 24 nov. 2019]. Disponível em http://www.cs.utsa.edu/~bylander/cs1023/mcafee_vcr_us.pdf

[180] ***McAfee, Inc.*** é uma empresa americana de informática, sediada em Santa Clara, na Califórnia, fundada por John McAfee focada em soluções de segurança.

sistemas críticos, incluindo eletricidade, controle de tráfego aéreo, mercados financeiros e redes de computadores do governo."[181]

> *"This year, China has been accused of launching attacks against the United States, India, Germany and Australia, but the Chinese are not alone: 120 countries including the United States are said to be launching Web espionage operations, according to McAfee's Virtual Criminology Report."*[182]

Foi neste contexto que a escultura do Soldado de Bronze com a cabeça arriada, punho cerrado e vestindo o uniforme do Exército Vermelho, da Segunda Guerra Mundial, que se encontra hoje num canto silencioso de um cemitério nos arredores de *Tallinn*, ficou famosa.

Em abril de 2007 uma luta por essa mesma estátua desencadeou o que acabaria por ficar conhecido como o primeiro ataque cibernético contra um país.

Com as tensões sociais geradas pela transferência da estátua abriu-se, inadvertidamente, uma Caixa de Pandora virtual de práticas ilegais contra as redes nacionais da Estónia tendo sido lançados ataques cibernéticos concertados causando danos generalizados na sociedade.

Durante três semanas, a Estónia foi vítima de ataques cibernéticos com motivação política sofrendo ataques a sites de partidos políticos, ataques contra organizações governamentais e comerciais incluindo escolas, provedores de serviços de Internet, canais de media e sites privados.

Recuemos então à história do Soldado de Bronze, que foi instalado pelas autoridades soviéticas em 1947, originalmente chamado de "Monumento aos Libertadores de Tallinn". Para os estónios de língua russa, este monumento representa a vitória da antiga União Soviética sobre os nazis, na segunda Guerra Mundial. Mas para os de etnia estoniana, o exército russo não estava a libertar aquela República dos alemães pois eles próprios encontravam-se na Estónia como invasores.

As tensões bilaterais entre a Rússia e a Estónia estão profundamente enraizadas e, desde 1918, quando a Estónia conquistou sua independência da Rússia até 1991, quando recuperou sua independência final, a Estónia viu sempre a presença da Rússia como ocupação ilegal. Neste sentido, para os de etnia estoniana, o soldado de bronze era uma lembrança dolorosa de meio século de ocupação e opressão soviética.

---

[181] Jon Brodkin. ***Government-sponsored cyberattacks on the rise, McAfee says***. [Em linha]. 2007. [Consult. 24 nov. 2019]. Disponível em https://www.computerworld.com/article/2540217/government-sponsored-cyberattacks-on-the-rise--mcafee-says.html (tradução livre do autor).

[182] ***Idem.***

No entanto, à época, a Estónia tinha uma população substancial de língua russa, quase um terço da população, e quando o governo da Estónia decidiu transferir o soldado de bronze, a decisão gerou muita ira e os media de língua russa e muitos falantes de russo saíram às ruas para protestar.

As manifestações foram acaloradas devido a notícias falsas que saíam nos media russos que alegavam que a estátua e as sepulturas militares soviéticas estavam próximas de ser destruídas.

Hackers patrióticos e grupos de jovens russos que já se haviam envolvido em ataques cibernéticos hostis contra sites chechenos, foram imediatamente mobilizados para defender a Rússia em nome dos interesses nacionalistas[183]. A reação do governo russo ao ato do governo estónio foi firme, ameaçando a Estónia com um corte das relações diplomáticas e apelidando a remoção da estátua como uma postura "blasfema e bárbara".

Em 26 de abril de 2007, *Tallinn* entrou em erupção com duas noites de tumultos e saques. Uma pessoa morreu, 156 ficaram feridas e havia 1.000 detidos[184].

Em 27 de abril, a Estónia começou a ser alvo de enormes ataques cibernéticos a sites de bancos e media, a maioria das agências governamentais entraram em colapso devido a níveis sem precedentes de tráfego na Internet face a um ataque de *distributed denial-of-service* (*DDoS*).

Em consequência desse brutal ataque cibernético, os estónios não conseguiram usar os serviços financeiros de utilização diária, como multibanco e serviços bancários online. Em termos estatais houve ataques ao serviço do correio eletrónico e os funcionários do estado não puderam comunicar por *email*. Os jornais e os media de repente viram-se incapazes de transmitir as notícias. *Liisa Past*, editora da página de opinião de um jornal da Estónia na época, lembra como repentinamente os jornalistas não podiam enviar os seus artigos para o sistema de edição para posterior impressão.

Este tipo de ataques cibernéticos permite que um país hostil crie inquietação e instabilidade num país pertencente à Organização do Tratado do Atlântico Norte, como a Estónia, sem ter receio de retaliação militar dos aliados da OTAN. Embora o Artigo 5º dessa aliança garanta que os membros da OTAN se defenderão, mesmo diante de um ataque no

[183] BOROGAN, Irina; SOLDATOV, Andrewi. ***"The Kremlin and the Hackers: Partners in Crime?"*** [Em linha]. 2012. [Consult. 24 nov. 2019]. Disponível em https://www.opendemocracy.net/en/odr/kremlin-and-hackers-partners-in-crime/

[184] McGUINNESS, Damien. ***Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*** [Em linha]. 2012. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/mundo/noticias-39800133

ciberespaço, a aplicação desse artigo só seria concretizada se esse mesmo ataque cibernético causasse uma perda significativa de vidas, semelhante à gerada por uma ação militar tradicional.

> *As Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar, cada uma, no exercício do direito de legítima defesa, individual ou colectiva, reconhecido pelo artigo 51.° da Carta das Nações Unidas, prestará assistência à Parte ou Partes assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a acção que considerar necessária, inclusive o emprego da força armada, para restaurar e garantir a segurança na região do Atlântico Norte. Qualquer ataque armado desta natureza e todas as providências tomadas em consequência desse ataque serão imediatamente comunicados ao Conselho de Segurança. Essas providências terminarão logo que o Conselho de Segurança tiver tomado as medidas necessárias para restaurar e manter a paz e a segurança internacionais.*[185]

Por outro lado, salienta-se, uma vez mais, que o ciberespaço como sistema do caos, com caráter de desterritorialização e omnipresente, torna difícil a retaliação quando não sabemos a quem atacar, pois é difícil identificar a pessoa, grupo ou país responsável pelo ataque**.**

Segundo (McGUINNESS, 2017), os ataques de 2007 foram feitos a partir de endereços *IP*[186] russos, as instruções online estavam em russo e Moscovo ignorou os pedidos de ajuda da Estónia. No entanto**,** não há evidências concretas de que esses ataques tenham sido realizados pelo governo russo[187].

Ainda segundo (McGUINNESS, 2017), um representante do governo da Estónia disse à *British Broadcasting Corporation (BBC),* sob condição de anonimato, que as evidências sugerem que o ataque "foi orquestrado pelo *Kremlin*, mas gangues maliciosos aproveitaram a oportunidade para se juntar ao ataque contra a Estónia"[188].

Aliás aquando deste tipo de ataques, os países hostis costumam contar com *hackers*, grupos criminosos e atores políticos *independentes* para se juntar a eles, de modo a que o impacto seja, por um lado, mais incisivo e poderoso e, por outro lado, seja menos rastreável e identificável.

Este acontecimento de 2007, foi um alerta para os estónios e ajudou-os a identificarem *in loco* as suas vulnerabilidades. Em reação podiam ter uma de duas atitudes, ficar furiosos e

---

[185] OTAN. ***5º artigo do Tratado do Atlântico Norte, Washington D.C.*** [Em linha]. 1949. [Consult. 5 jun. 2019]. Disponível em https://www.nato.int/cps/su/natohq/official_texts_17120.htm?selectedLocale=pt

[186] ***Internet Protocol*** - é um protocolo de comunicação usado entre todas as máquinas em rede para encaminhamento dos dados.

[187] McGUINNESS, Damien. ***Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*** [Em linha]. 2017. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/mundo/noticias-39800133

[188] ***Idem.***

lastimar ou aprender com a situação. Optaram pela aprendizagem e colocaram em prática o saber da palavra crise em chinês como o fez John F. Kennedy no discurso em Indianápolis, no dia 12 de abril de 1959.

> *"When written in Chinese, the word "crisis" is composed of two characters - one represents danger and one represents opportunity."*[189]

A Estónia sofreu com esta situação, mas face à oportunidade tornaram-se especialistas em defesa cibernética**.**

"Foi um ótimo teste de segurança. Não sabemos para quem enviar o cheque", diz *Tanel Sepp*, especialista em segurança cibernética do Ministério da Defesa da Estónia.

Os ataques cibernéticos do Soldado de Bronze foram os primeiros ataques a serem suspeitos de terem sido lançados por uma nação contra outra.[190]

3.2.2. Ataque à Geórgia em 2008

Antes de analisarmos o ataque à Geórgia em 2008 iremos fazer uma retrospetiva, de modo a contextualizarmos o tema.

Assim, recuemos até 1989 aquando a Ossétia do Sul, por sua iniciativa corta o vínculo com a República Socialista Soviética Georgiana e afirma-se como região autónoma. Este facto, leva a um conflito armado que, após alguns avanços e recuos e a independência da Geórgia, termina em 1992 com a constituição de uma força de paz composta por georgianos, ossétios e russos. No entanto, a comunidade internacional continuou a reconhecer a Ossétia do Sul como parte integrante da Geórgia.

No verão de 2008, houve uma escalada da tensão na região com o suposto abate de um avião, seguindo-se outros incidentes e acusações cruzadas. No dia 7 de agosto de 2008 as forças georgianas lançaram um ataque surpresa contra as forças separatistas da Ossétia do Sul numa tentativa de recuperar o território, afirmando que estavam a responder aos ataques efetuados contra as suas forças de paz e que, concomitantemente, a Rússia estava a deslocar unidades não pertencentes à manutenção da paz para o país. No dia seguinte, a Rússia respondeu ao ataque efetuando operações militares em território georgiano.

---

[189] ***John F. Kennedy – Presidential Library and Museum*** [Em linha]. 1959. [Consult. 24 nov. 2019]. Disponível em https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/indianapolis-in-19590412

[190] McGUINNESS, Damien. ***Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*** [Em linha]. 2012. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/mundo/noticias-39800133

Segundo (SHAKARIAN, 2011) um dia antes da invasão russa diversos ataques cibernéticos coordenados acompanharam a campanha militar. "Essa foi a primeira vez que uma operação de ataque contra uma rede de computadores em grande escala foi executada em conjunto com importantes operações de combate terrestres. O ataque não teve ligação direta com o governo russo, mas exerceu importante impacto psicológico e de informação na Geórgia isolando-a do resto do mundo."

Desta forma tornou-se o primeiro caso em que um conflito internacional político e militar, foi acompanhado, ou mesmo precedido por uma ofensiva no domínio cibernético.

Ainda segundo (SHAKARIAN, 2011), "Especialistas em segurança identificaram duas fases na campanha cibernética russa. A primeira teve início no anoitecer de 7 de agosto, quando *hackers* atacaram sítios internet do governo da Geórgia e da media local. O Coronel *Anatoly Tsyganok*, chefe do Centro de Previsão Militar da Rússia, disse que essas primeiras ações eram uma reação à invasão de sítios da imprensa da Ossétia do Sul por parte da Geórgia, que haviam ocorrido no início da semana. O facto de esses alegados contra-ataques terem ocorrido apenas um dia antes do desencadeamento da campanha terrestre levou muitos especialistas a sugerirem que os *hackers* sabiam a data da invasão."

A principal ação dos *hackers* russos, durante esta primeira fase, consistiu num ataque distribuído de negação de serviço (*DDoS*), tentando impedir o acesso a vários sítios da internet do governo georgiano e dos media local.

A segunda fase, para além do continuado ataque de *DDoS*, já referido, e ainda segundo (SHAKARIAN, 2011), "…a operação cibernética russa foi ampliada de modo a infligir danos a mais alvos, incluindo instituições financeiras, empresas, instituições de ensino, media ocidental (*BBC* e *CNN*) e um sítio internet de *hackers* da Geórgia. Os ataques contra esses servidores não incluíram apenas negação de serviço, mas também a desfiguração dos sítios (um exemplo foi a "*grafitagem*" pró-russa nas páginas do governo, como o emprego de uma imagem comparando o Presidente georgiano *Mikheil Saakashvili* a *Adolf Hitler*). Além disso, vários *hackers* russos utilizaram endereços de correio eletrónico de políticos georgianos, disponíveis ao público, para iniciar uma campanha de proliferação de mensagens eletrónicas."

"Andro Barnovi, vice-ministro da Defesa da Geórgia, referiu que os objetivos operacionais da operação cibernética realizada contra a sua nação, visavam criar:

- Sentimento de insegurança na sociedade;
- Desconfiança do governo;
- Pânico causado por desinformação;
- Impedir a política de informação do governo;

- Dano económico direto;
- Desordem de sistemas de comunicação;
- Coordenação enfraquecida dentro das agências governamentais;
- Disfunção dos sistemas de comando e controlo e subsequente dano físico direto;
- Diminuição da legitimidade das atividades do governo dentro e fora do país;
- Adquirir informações confiáveis sobre as ações e deslocamentos das unidades e lideranças do exército da Geórgia."[191]

Estes objetivos operacionais apontavam claramente para o controlo do ciberespaço e para afetação da decisão humana criando o pânico e a desinformação.

As ligações da internet para a Geórgia vêm via Rússia e Turquia. Os *hackers* assumiram o controlo dessas ligações, de modo a que nenhum tráfego passasse, impossibilitando os georgianos de se ligarem a qualquer fonte de noticia ou informação externa, não podendo enviar *mail* para fora do país. A Geórgia perdeu o controlo sobre o domínio *".ge"* e foi forçada a mudar muitos dos sites do seu governo para servidores fora do país.

Segundo *Richard A. Clark e Robert K. Knak*, no seu livro *Cyber War The Next Threat to National Security and What to Do About It*, "os georgianos bem que tentaram defender o seu ciberespaço utilizando soluções alternativas para frustrar os ataques de *DDoS*, mas os russos rebateram cada movimento. A Geórgia tentou bloquear o tráfego vindo da Rússia e os russos redirecionaram os seus ataques para parecerem pacotes vindos da China.

O sector bancário georgiano desligou os seus servidores e planeou superar os ataques, imaginando perda de temporária do sistema bancário online. Segundo os responsáveis bancários seria mais tranquilo do que correr o risco de roubo dos seus dados críticos ou danos internos nos sistemas.

Face a esse "apagão" bancário georgiano, os russos enviaram uma enxurrada de tráfego para a comunidade bancária internacional fingindo serem ataques cibernéticos oriundos da Geórgia. Esses ataques desencadearam uma resposta automática da maioria dos bancos estrangeiros que encerraram as suas ligações com o sector bancário georgiano. Sem acesso ao sistema de compensação europeu as operações bancarias da Geórgia ficaram paralisadas. O sistema de cartões de credito também foi abaixo seguido do serviço móvel de telefone.

[191] CROWELL, Richard M. – ***Some Principles of Cyber Warfare Using Corbett to Understand War in the Early Twenty–First Century***. Corbett Paper, nº19, p. 18

À imagem e semelhança do caso da Estónia o governo russo alegou que os ciberataques eram uma resposta popular e que estavam fora do controle do Kremlin."[192]

Concluiu ainda (CLARKE, 2010), que "este ataque teve nitidamente uma origem externa e proveniente de vários locais do mundo. Existem referências a endereços de Protocolo da Internet (*IP*, sigla inglesa) dos Estados Unidos da América, Europa Ocidental e Irão. No entanto, estes *IP* pouco ou nada nos dizem dado que, apesar de poderem ser verdadeiros, pertencem a máquinas que estão comprometidas e fazem parte de *botnets* e, desta forma, nem o seu próprio proprietário sabe."

No seu estudo de caso de guerra cibernética, *Cyberwar Case Study: Georgia 2008, David Hollis* afirma que:

> *"The culmination of these trends resulted in a situation that prevented government agencies in Georgia from communicating, both locally with their population and strategically with the rest of the world. Russia was able to successfully attack the Georgian center of gravity across several warfighting domains, to include the cyberspace domain through propaganda operations, and denial, disruption, and degradation of Georgian communications.*
>
> *This allowed the Russians to dominate the strategic communications environment during the several-week build-up to, and the conduct of military operations in the physical domain environments. Doctrinal concepts such as center of gravity and effects based targeting; and military principals such as mass, economy of force, C2, surprise, and unity of effort apply equally to military operations in the cyberspace domain as to operations in the other domains. Attacking and defeating the enemy"s center of gravity and breaking the will of the enemy to continue the conflict are traditional objectives of warfare and they are as applicable to the cyberspace domain as any other warfighting domain."*[193]

Nesta guerra, contra a Geórgia, os níveis, operacional e tático das Forças Armadas Russas no domínio terrestre, aéreo e marítimo estavam completamente sincronizadas com as (supostas) operações russas no ciberespaço, de modo, a obter o maior impacto possível.

Redes e sítios em locais geográficos específicos foram alvo de operações de negação e interrupção de serviço, a fim de causar pânico e incerteza na população civil da Geórgia, dificultando uma resposta militar eficaz. [194]

---

[192] CLARKE, Richard A;KNAKE, Robert K. – ***Cyber War The Next Threat to National Security and What to Do About It***. p.16 (tradução livre pelo autor).
[193] HOLLIS, David. ***Cyberwar Case Study: Georgia 2008*** **[Em linha]**. 2011. [Consult. 24 nov. 2019]. Disponível em https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf
[194] ***Idem.***

Os ataques foram bastante generalizados e conseguiram parar a quase totalidade do serviço de internet. Organismos públicos como a Presidência, o Parlamento e Ministérios foram afetados, assim como, os media, a banca e empresas de telecomunicações.

No entanto, apesar do ataque ter sido devastador, causando a indisponibilidade de serviços, e durante muito tempo, não teve grandes efeitos sobre a vida normal no país pois, na Geórgia, só 7 habitantes em cada 100 possuíam ligação à internet e, ao contrário da Estónia, o dia a dia georgiano não está baseado nas *TIC*.

Como já referido, este foi o primeiro caso em que um conflito internacional político e militar, foi acompanhado, ou mesmo precedido, por uma ofensiva de ataques cibernéticos e foi bem-sucedido, pois ao mesmo tempo que era lançado um ataque cibernético apontando para o controlo do ciberespaço, criando o pânico e desinformação, foi efetuada uma invasão militar utilizando os domínios terrestre, aéreo e marítimo.

3.2.3. Ataque ao Irão em 2010

Em janeiro de 2010, os inspetores da Agência Internacional para a Energia Atómica visitavam as instalações em *Natanz*, no Irão, e constataram que as centrifugadoras usadas para enriquecer o urânio estavam com falhas sem precedência. Meses depois, uma empresa de segurança de computadores sediada na Bielorrússia foi chamada ao Irão para solucionar um problema com computadores que se reiniciavam constantemente. Aparentemente, as duas situações misteriosas nada tinham a haver uma com a outra até à altura em que os analistas encontraram um série de arquivos maliciosos em um dos sistemas e descobriram a primeira arma digital do mundo[195].

> *In January 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the Iranian technicians replacing the centrifuges as to the inspectors observing them.*
>
> *Five months later a seemingly unrelated event occurred. A computer security firm in Belarus was called in to troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. Again, the cause of the problem was a mystery. That is,*

[195] ZETTER, Kim. ***An Unprecedented Look at Stuxnet, the World's First Digital Weapon*** **[Em linha]**. 2014. [Consult. 24 nov. 2019]. Disponível em https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

> *until the researchers found a handful of malicious files on one of the systems and discovered the world's first digital weapon*[196]

No seguimento dessa descoberta, o Irão divulgou publicamente que uma arma cibernética tinha danificado as centrifugadoras a gás na instalação de enriquecimento de urânio em *Natanz*.

Identificado pela empresa Bielorussa *VirusBlokAda*, o *Stuxnet* foi descrito como sendo "altamente sofisticado" e complexo, lançado com o único objetivo de sabotar as centrifugadoras de enriquecimento de urânio. O *malware* tinha como objetivo um controlador industrial específico, de modo a danificar com sucesso um número significativo de centrifugadoras iranianas, fazendo com que girassem fora de controlo.

Esse *malware* foi injetado numa rede que não estava ligada à Internet, o que não era novidade, pois as pessoas estão constantemente a infetar máquinas e redes autónomas através da inserção, conscientes ou de forma involuntária, de dispositivos infetados.

A importância deste evento foi o facto de que este foi o primeiro incidente documentado em que uma arma cibernética real foi implantada e cuja intenção era negar, degradar, interromper e destruir uma informação específica de um determinado sistema[197].

Em setembro deste mesmo ano a *BBC*, com base em informações da agência de notícias oficial *IRNA*[198], fazia uma reportagem intitulada "*Worm Stuxnet* atinge computadores da equipa da central nuclear do Irão" dizendo que um complexo *worm* tinha infetado os computadores pessoais da primeira central nuclear do Irão.

> *A complex computer worm has infected the personal computers of staff at Iran's first nuclear power station, the official IRNA news agency reported.*
> *However, the operating system at the Bushehr plant - due to go online in a few weeks - has not been harmed, project manager Mahmoud Jafari said.*
> *The Stuxnet worm is capable of seizing control of industrial plants.*
> *Some Western experts say its complexity suggests it could only have been created by a "nation state".*
> *An electronic war has been launched against IranMahmoud Liayi, Ministry of industries*
> *It is the first sign that Stuxnet, which targets systems made by the German company Siemens, has reached equipment linked to Iran's nuclear programme.*
> *The West fears Iran's ultimate goal is to build nuclear weapons. Iran says its programme is aimed solely at peaceful energy use.*

---

[196] ***Idem.***
[197] ***Idem.***
[198] ***Agência de Notícias da República Islâmica***, conhecida internacionalmente como **IRNA** (de sua denominação em inglês: ***Islamic Republic News Agency***) é uma agência de notícias oficial da República Islâmica do Irão, mantida com recursos públicos e controlada pelo Ministério da Cultura e da Orientação Islâmica.

> *Stuxnet is tailored to target weaknesses in Siemens systems used to manage water supplies, oil rigs, power plants and other utilities.*[199]

Segundo (JOHN, 2010) a sofisticação deste *malware*, a sua funcionalidade, a intenção que existiu no seu desenvolvimento e o seu aparecimento clandestino num sistema de controle industrial "não-Internet", indiciou que teve que haver um patrocínio de um estado, dando início à primeira instância da guerra cibernética.

Esta ideia foi apoiada pelos analistas que levaram meses a fazer *reverse-engineering* do código do *Stuxnet*, concordando que aquele nível de sofisticação teria que ter sido apoiado por um estado. No entanto, colocaram igualmente fora de hipótese de que o *Stuxnet* tivesse o objetivo de explodir as centrifugadoras afirmando que aquele código tinha o objetivo subtil de sabotar.

Suspeitas de que os Estados Unidos e Israel tinham sido os possíveis autores deste ato foram reforçadas, mas não confirmadas, em 2012, quando um funcionário (sob anonimato) dos EUA reconheceu o envolvimento deste país como fazendo parte do programa *Operation Olympic Games*[200] iniciado por Presidente *George W. Bush* e continuado pelo Presidente *Barack Obama*. A Administração Americana não fez nenhum pronunciamento oficial sobre o assunto.

Voltemos então ao verão de 2010, aquando a empresa Bielorussa *VirusBlokAda* com a sua descoberta marcou a segurança da indústria de software de equipamentos industriais.

Segundo (KARNOUSKOS, 2011), este novo *worm* de computador tinha como alvos sistemas industriais altamente especializados, em infraestruturas críticas de alta segurança. Nos meses seguintes, ficou claro que este foi um ataque sofisticado, sem precedentes e com amplas implicações para futuros sistemas do género. Para muitos foi um alerta e aumentou a consciencialização sobre a segurança que ainda é vista como uma reflexão tardia e um complemento, e não como um processo contínuo que deve ser integrado em todos os aspetos operacionais.

O objetivo principal deste *worm* é controlar sistemas industriais, modificando o seu código fonte, "obrigando-os" a desviar-se do comportamento esperado. Este desvio é diminuto

---

199 JOHN, Sian. ***Stuxnet worm hits Iran nuclear plant staff computers*** [Em linha]. 2010. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/news/world-middle-east-11414483

200 ***Operation Olympic Games*** foi uma campanha secreta e ainda não reconhecida, de sabotagem por meio de interrupção cibernética, dirigida às instalações nucleares iranianas pelos Estados Unidos e provavelmente por Israel. É um dos primeiros usos conhecidos de armas cibernéticas ofensivas. Iniciado sob a administração de George W. Bush em 2006, os Jogos Olímpicos foram acelerados sob a presidência de Barack Obama

e só é detetável ao fim de um longo período de tempo pois os criadores do *Stuxnet* esconderam esse desalinhamento forçando os sistemas a fornecer "reports" sem desvios.

Segundo (LANGNER, 2013), consultor de segurança alemão,

> *O sistema de proteção em cascata da Natanz conta com os controladores industriais Siemens S7-417 para operar as válvulas e sensores de pressão de até seis cascatas, ou grupos de 164 centrifugadoras cada um. Um controlador pode ser pensado como um pequeno computador incorporado e diretamente ligado a equipamentos físicos, como por exemplo, válvulas. O Stuxnet foi projetado para infetar esses controladores e assumir o seu controle completo de uma maneira que os utilizadores nunca imaginaram e que nunca tinha sido discutido em conferências de sistemas de controlo industrial.*
>
> *Um controlador infetado com Stuxnet, na verdade, é dissociado da realidade física. A lógica de controlo legítimo apenas "vê" o que o Stuxnet deseja que ele veja. Antes da execução da sequência de ataque (que é aproximadamente uma vez por mês), o código malicioso é benevolente o suficiente para mostrar aos operadores na sala de controlo a realidade física da fábrica. Mas isso muda durante a execução do ataque.*[201]

Ainda segundo (LANGNER, 2013),

> *Uma das primeiras coisas que o Stuxnet faz é tomar medidas para esconder as suas pegadas, usando um truque direto de Hollywood. O Stuxnet regista os valores do sensor do sistema de proteção em cascata por um período de 21 segundos. Em seguida, repete esses 21 segundos em um loop constante durante a execução do ataque. Na sala de controlo, tudo parece normal, tanto para operadores humanos quanto para qualquer rotina de alarme implementada por software.*
>
> *Então o Stuxnet começa seu trabalho malicioso. Fecha as válvulas de isolamento para os dois primeiros e os últimos dois estágios de enriquecimento. Isso bloqueia a saída de gás de cada cascata afetada e, por sua vez, aumenta a pressão sobre o restante das centrifugadoras. As centrifugadoras a gás para enriquecimento de urânio são extremamente sensíveis a aumentos de pressão perto do vácuo. Um aumento na pressão resultará na entrada de mais hexafluoreto de urânio na centrifugadora, causando maior stress mecânico no rotor. A pressão na parede do rotor é uma função da velocidade (velocidade do rotor) e da pressão operacional; quanto mais gás, mais pressão contra a parede do rotor o que implica mais força mecânica contra o tubo fino. Por fim, a pressão pode fazer com que o hexafluoreto de urânio gasoso se solidifique, prejudicando fatalmente as centrífugas.*[202]

[201] Tradução livre do autor
[202] Tradução livre do autor

A descoberta do *Stuxnet* pode não ter sido por acaso, podia até ser sido parte da estratégia.

> *"The shift of attention may have been fueled by a simple insight: Nuclear proliferators come and go, but cyberwarfare is here to stay. Operation Olympic Games started as an experiment with an unpredictable outcome. Along the road, one result became clear: Digital weapons work."*[203]

Ainda segundo (LANGNER, 2013), esta guerra digital é diferente da "guerra analógica", ela não coloca as forças militares em perigo, produz menos danos colaterais, pode ser implantada furtivamente e é barata. No entanto, o conteúdo desta caixa de Pandora tem implicações muito além do Irão. Fizeram a guerra analógica parecer de baixa tecnologia, brutal e, portanto, do século XX.

Continuando com (LANGNER, 2013) "…explodir a capa dessa campanha de sabotagem pode ter trazido benefícios. Descobrir o *Stuxnet* foi o fim da operação, mas não necessariamente o fim de sua utilidade. Ao contrário do hardware tradicional do *Pentágono*, não é possível exibir unidades *USB* num desfile militar. A revelação do *Stuxnet* mostrou ao mundo o que as armas cibernéticas poderiam fazer nas mãos de uma superpotência. Também salvou a América do constrangimento. Se outro país - talvez até um adversário - tivesse sido o primeiro a demonstrar proficiência no domínio digital, não haveria nada menos que outro momento do *Sputnik* na história dos EUA. Portanto, havia muitas boas razões para não sacrificar o sucesso da missão por medo de ser detetado."[204]

Não temos certeza se o *Stuxnet* foi divulgado intencionalmente. Como em muitas criações humanas, pode ter sido simplesmente um efeito colateral não intencional que revelou a sua existência. Uma coisa sabemos: mudou a estratégia militar global no século XXI (LANGNER, 2013).

Em resumo o *Stuxnet* demonstrou, com sucesso, a viabilidade de um ataque cibernético muito direcionado e altamente sofisticado.

No entanto, a sua arquitetura não é específica deste domínio industrial e com algumas modificações pode ser preparado para atacar outros sistemas e.g. indústria automóvel ou energia. Nesse sentido, este *worm*, nas mãos de grupos com tendência criminal, pode ser uma arma cibernética muito eficaz e com um impacto significativo, agravado com a circunstância de que muitos dos modernos sistemas industriais em todo o mundo têm a mesma infraestrutura

[203] LANGNER, Ralph. ***Stuxnet's Secret Twin*** [Em linha]. 2013. [Consult. 24 nov. 2019]. Disponível em https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/
[204] Tradução livre do autor.

que a existente em *Natanz* e que podemos ter visto, em 2010, apenas uma demonstração da capacidade desta "arma".[205]

3.3. O Ciberespaço como a nova fronteira em defesa

> *"The problem is not Stuxnet. Stuxnet is history," said Langner in an e-mail message. "The problem is the next generation of malware that will follow." Ralph Langner, a well-respected expert on industrial systems security,*

Hoje o ciberespaço passou a fazer parte do "léxico diário" e tornou-se tema frequente.

A expansão da conectividade digital e móvel e a proliferação de dispositivos *"Internet das Coisas" (IoT, sigla inglesa)*[206] não tem sido acompanhada, ao mesmo ritmo, pela segurança em infraestruturas da Internet ou hardware e software. Hoje é mais fácil e barato para os criminosos obterem ferramentas para iniciar ataques cibernéticos com alto grau de sofisticação, com o ciberataque a ser cada vez mais um método entre muitos para grupos criminosos organizados. Por outro lado, temos assistido a um crescimento adicional de ameaças cibernéticas dos estados e as suas capacidades não param de se desenvolver.[207]

Seguidamente, deixamos alguns pareceres de instituições, entidades e pessoas, sobre o tema ciberespaço, desde do seu aparecimento até à sua afirmação como um novo domínio das operações militares.

Principiemos pelo "Conceito Estratégico pela defesa e segurança dos membros da Organização do Tratado do Atlântico Norte " Adotado pelos Chefes de Estado e de Governo, em Lisboa, corria o ano de 2010:

> *"Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks."*

---

[205] KARNOUSKOS, Stamatis. ***Stuxnet Worm Impact on Industrial Cyber-Physical System Security*** **[Em linha]**. 2011. [Consult. 24 nov. 2019]. Disponível em https://ieeexplore.ieee.org/document/6120048 (tradução livre do autor)

[206] IoT – ***Internet of Things***, é um conceito que se refere à ligação digital de objetos quotidianos com a internet.

[207] Progress Report. ***National Cyber Security Strategy 2016 – 2021*** [Em linha]. 2019. [Consult. 22 dez. 2019]. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf. (tradução livre do autor)

Em 2010, *Richard A. Clarke and Robert K. Knake*, no seu livro *Cyber War The Next Threat to National Security and What to Do About It*, numa passagem sobre as ciberguerras que envolveram a Rússia com a Estónia e posteriormente a Rússia com a Geórgia, dizia-nos que é muito provável que a Rússia, à imagem e semelhança de um bom jogador de póquer, não revelou todo o seu jogo e por isso terá seguramente outros trunfos quando os jogadores forem mais fortes.

> *"The Russians, in fact, showed considerable restraint in the use of their cyber weapons in the Estonian and Georgian episodes. The Russians are probably saving their best cyber weapons for when they really need them, in a conflict in which NATO and the United States are involved."*

Ainda em 2010, *Kim Zetter*, jornalista e autor premiado que investiga temas como segurança cibernética e segurança nacional desde 1999, no seu livro *Countdown to zero day Stuxnet and the Launch of the World s First Digital Weapon*, sobre o *worm Stuxnet*, diz-nos que:

> *In January 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery---apparently as much to the Iranian technicians replacing the centrifuges as to the inspectors observing them.*
>
> *Five months later a seemingly unrelated event occurred. A computer security firm in Belarus was called in to troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. Again, the cause of the problem was a mystery. That is, until the researchers found a handful of malicious files on one of the systems and discovered the world's first digital weapon.*

Avançando mais um ano, mais propriamente em novembro de 2011, aquando a publicação do *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, mais precisamente no seu capítulo 2, dedicado a *Changing threats*, dizia-nos que:

> *Some of the most sophisticated threats to the UK in cyberspace come from other states which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. 'Patriotic' hackers can act upon states' behalf, to spread disinformation, disrupt critical services or seek advantage during times of increased tension. In times of conflict, vulnerabilities in cyberspace could be exploited*

> *by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home.*
>
> *Cyberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile physical attacks, the threat that they might also use cyberspace to facilitate or to mount attacks against the UK is growing. We judge that it will continue to do so, especially if terrorists believe that our national infrastructure may be vulnerable.*

Nesta publicação já era claro a utilização do ciberespaço como meio para atingir fins.

Em 2015, foi publicado a Resolução do Conselho de Ministros (RCM) n.º 36/2015 e o seu anexo que apresentava a Estratégia Nacional de Segurança do Ciberespaço que nos dizia que:

> *Este «mundo em rede» desenvolve novos modos de atuação com características únicas, de onde se destacam o cibercrime e, em particular, o cibercrime organizado, associado à fraude bancária e à usurpação de identidade com este mesmo propósito, o hacktivismo político nas suas várias expressões, como são o desvio e a revelação de informação sensível ou classificada e a sabotagem informática, ou ainda a crescente espionagem de Estado e industrial. Tanto a nível interno como internacional, são evidentes as capacidades de ativismos políticos e religiosos, criminosos ou terroristas para conduzir ações com impacto na segurança de infraestruturas vitais de informação, criando sérias ameaças à sobrevivência do Estado de Direito democrático e ao espaço de liberdade, segurança e justiça.*

Em 2016, num *white paper* sobre *Cyberspace: the Fifth Domain of War!?, a Critical Infrastructure Protection & Resilience Cyber Research Center – Industrial Control Systems*, dizia-nos que:

> *"Cyberspace has become a full-blown war zone as governments across the globe clash for digital supremacy in a new, mostly invisible theater of operations. Once limited to opportunistic criminals, cyber attacks are becoming a key weapon for governments seeking to defend national sovereignty and project national power."*

Ainda no mesmo ano, o diretor do serviço de inteligência espanhol, o General de quatro estrelas, *Félix Sanz Roldán*, alertou sobre essa nova geração de ataques ao Conselho de Segurança da ONU, em Nova Iorque, e reafirmou em entrevista no seu quartel general nas vizinhanças de Madrid: "Os ciberataques deveriam estar na Carta das Nações Unidas, no seu capítulo VII, que define as ameaças e quebras da paz e os atos de agressão. Seria uma conquista para a humanidade".

Por último, deixamos mais dois juízos sobre esta temática. O primeiro é de 2017 e foi redigido na Revista Militar pelo Contra-Almirante António Gameiro Marques, atual Autoridade de Segurança Nacional e o final é um estudo publicado em dezembro de 2019, na *Security Magazine,* intitulado "Guerra cibernética representa uma ameaça sem precedentes em 2020".

Dizia-nos então o Contra-Almirante Gameiro Marques que:

> *As evidências de ciberataques contra Estados Soberanos – Estónia (abril/maio de 2007), Geórgia (agosto de 2008) e Ucrânia (no âmbito do conflito na Crimeia) –, perpetrados por pequenos grupos de atores, muitas vezes ao serviço de estados, fez com que muitas das maiores potências mundiais (EUA, China e Rússia), já detentoras de uma capacidade militar convencional de dimensão significativa, tenham vindo a criar, ao longo dos últimos anos, não só os mecanismos necessários para evitarem ser atacadas, mas também a capacidade para projetar poder neste novo domínio operacional. Neste contexto, com a criação do U.S. Cyber Command, em 2010 (que atingiu a Final Operating Capability em 3 de novembro de 2010), os EUA passaram a assumir doutrinariamente o ciberespaço como um novo domínio operacional. Ao nível europeu, esta decisão foi, entretanto, seguida pela Alemanha, Reino Unido, Espanha e França, que anunciaram a criação de comandos responsáveis pela condução de operações militares no ciberespaço.*
>
> *Demonstrando grande preocupação com o impacto crescente do ciberespaço no ambiente de segurança internacional, na Cimeira de Varsóvia (7-9 de julho de 2016), a Aliança Atlântica reconheceu o ciberespaço como um quarto domínio operacional, a par do mar, da terra e do ar, estando em curso todo o processo que levará à concretização desta decisão. Ainda que sujeito a confirmação, existem indicações que fazem supor que o Allied Command Transformation possa vir a assumir no futuro a função de Cyber Command da Aliança Atlântica.*[208]

Quanto ao estudo da *Security Magazine* diz-nos que a ciberguerra alcançará um novo nível em 2020.

"As ameaças *ciber* em 2020 estarão em destaque, com ataques cibernéticos de alto impacto contra infraestruturas críticas. As medidas de dissuasão Ocidental não conseguiram combater a corrente de ataques e os "atacantes" estão a usar métodos cada vez mais sofisticados. Os EUA irão retaliar para mostrar ao mundo a importância que atribuem a essa ameaça.

Em cenários de conflito estratégico, medidas militares inaceitáveis darão lugar a ataques *ciber*. Começará um novo ciclo de intensificação: os rivais cibernéticos do Ocidente e os atores que atuam em seu nome aumentarão o nível de ataques, trazendo consequências imprevisíveis,

[208] MARQUES, António Gameiro. ***O Poder da Informação no Poder Militar.*** Revista Militar. Lisboa. Nº 2589 (outubro 2017) p. 775 [Em linha]. 2017. [Consult. 5 dez. 2019]. Disponível em https://www.revistamilitar.pt/artigo/1271

aponta estudo. Se as empresas líderes atingiram um nível aceitável de resiliência cibernética, o mesmo não se verifica nas infraestruturas nacionais em todo o mundo, sendo estas últimas a principal vulnerabilidade no conflito internacional."

Como acabamos de ver, muitas opiniões e de variadíssimas fontes, desde de pessoais até institucionais, entendem que o ciberespaço é, e será, um espaço de guerra. Estamos perante um novo paradigma onde reina o caos, a desterritorialização e a omnipresença, e em muitas das situações com fronteiras e inimigos desconhecidos.

O ciberespaço traz consigo um novo teatro de operações e representa um enorme desafio para as Forças Armadas obrigando-as a reinventar e adaptar os conceitos militares tradicionais em todos os níveis da guerra: estratégica, operacional e tática

A OTAN, atenta a este novo domínio da guerra, terá um centro de controlo militar cibernético em plena operação até 2023.

"Quando estiver totalmente operacional, o centro cibernético coordenará a dissuasão da OTAN por meio de uma equipa de 70 especialistas apoiados por inteligência militar e informações em tempo real sobre *hackers*, desde militantes islâmicos a grupos do crime organizado que operam em nome de governos hostis.

Embora a OTAN não tenha as suas próprias armas cibernéticas, a aliança, liderada pelos Estados Unidos, estabeleceu um centro de operações no seu centro militar na Bélgica. Os EUA, o Reino Unido, a Estónia e outros aliados estão desde então oferecendo as suas capacidades cibernéticas."[209]

Poderá a história repetir-se?

Há cerca de 100 anos atrás, decorria ainda a primeira Grande Guerra, o poder aéreo era uma realidade em crescendo e a sua utilidade era óbvia, mudando os níveis estratégico, operacional e tático da guerra. A 1 de abril de 1918, foi criada, aquela que reclama ter sido a primeira Força Aérea independente, a *Royal Air Force* (RAF) através da fusão do *Royal Flying Corps* do Exército Britânico com o *Royal Naval Air Service* da *Royal Navy*.

Dada a relevância que o ciberespaço está a conquistar em quase todos os países é bem provável, e tema para possíveis novas dissertações, que à imagem e semelhança do que aconteceu com a Força Aérea, em 1952, criada a partir do Exército e da Marinha se possa a vir formar um "novo ramo das Forças Armadas – Comando Cibernético da Defesa", em Portugal,

[209] Security Report. ***OTAN terá centro de controle militar cibernético em plena operação até 2023*** [Em linha]. 2018. [Consult. 3 jan. 2020]. Disponível em http://www.securityreport.com.br/overview/otan-tera-centro-de-controle-militar-cibernetico-em-plena-operacao-ate-2023/#.XiEREUf7QdV

tendo porventura como missão o controlo de toda tecnologia de informação e comunicações (TIC), serviços de inteligência e geoinformação.

Estes exemplos começam a existir na Europa e, um deles, vem da Alemanha, com a criação do Comando do Espaço Cibernético e de Informação como um novo ramo das Forças Armadas Alemãs. Criado em abril de 2017 tem planeado ficar totalmente operacional por volta de 2021.

"Neste desiderato, interessará referir que em Portugal, o levantamento das questões relativas às ações no ciberespaço encontra-se previsto no novo Conceito Estratégico de Defesa Nacional com o desenvolvimento da respetiva estratégia.

Também estabelece o desenvolvimento de uma Estratégia Nacional de Cibersegurança e de uma rede nacional de CSIRT (*Computer Security Incident Response Teams*), tendo em consideração as diretivas da OTAN e da EU."[210]

O que é que Portugal já tem sobre estratégia cibernética e quais as suas possibilidades de poder vir a ser um Polo estratégico de ciberdefesa, no âmbito da OTAN, serão temas que iremos explorar no próximo capítulo.

[210] TOMÉ, António de Almeida. ***A Segurança e a Defesa no Ciberespaço*** [Em linha]. 2015. [Consult. 5 jan. 2020]. Disponível em http://recil.grupolusofona.pt/bitstream/handle/10437/9597/A%20Seguran%C3%A7a%20e%20a%20Defesa.pdf?sequence=1

4. Portugal como centro de excelência no âmbito da ciberdefesa

> *"O ciberespaço é por natureza um espaço aberto desprovido de fronteiras tangíveis, onde tanto o setor público como o privado, civis e militares, atores nacionais e internacionais interagem em simultâneo e de forma interdependente e interligada. Por essas razões, não é um espaço seguro e protegido, sendo vulnerável a ataques cibernéticos, que podem ter como consequência perdas relevantes no plano económico e social ou constituir uma ameaça séria à Defesa Nacional, quer no plano da degradação ou destruição de infraestruturas críticas quer no plano da neutralização ou negação ao acesso a recursos informacionais."*[211]

Neste capítulo iremos investigar o que se concretizou, em Portugal e na Organização do Tratado do Atlântico Norte, em termos de produção normativa de política e estratégia para a ciberdefesa.

Como é óbvio, com o passar dos anos e face à escalada de interesse mundial pelo tema ciberespaço, muito se tem escrito e legislado sobre o assunto. No entanto, iremos dar especialmente atenção àqueles que nos pareceram ser mais relevantes para o nosso trabalho e que irão apoiar a nossa linha de raciocínio.

Ainda neste capítulo, demonstraremos que Portugal, membro fundador da OTAN, deverá estar comprometido com a inovação e transformação que a Aliança está a protagonizar sobre o tema ciberespaço. Por outro lado, é nossa convicção de que Portugal tem todas as condições para ir mais além nesse projeto assumindo um papel fundamental e tornando-se num Polo relevante e estratégico para a OTAN, no domínio da Ciberdefesa.

Este novo domínio de operações, passou a fazer parte do "*core business*" da Aliança, tendo iniciado na Cimeira de Lisboa, em 2010, afirmado na Cimeira de Varsóvia, em 2016, e reafirmado na Cimeira de Bruxelas, em 2018.

> *"NATO adopted a new Strategic Concept at the Lisbon Summit in 2010, during which the North Atlantic Council (NAC) was tasked to develop an in-depth NATO cyber defence policy and to prepare an action plan for its implementation."*[212]

> *"At the Warsaw Summit in July 2016, Allied Heads of State and Government reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on*

[211] DRE. ***Orientação para a Ciberdefesa,*** Despacho n.º 13692/2013 [Em linha]. 2013. [Consult. 07 dez. 2019]. Disponível em https://dre.pt/application/file/a/3295546

[212] OTAN. ***Cyber Defence Evolution*** [Em linha]. 2019. [Consult. 02 jan. 2020]. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.htm

land and at sea. This improved NATO's ability to protect and conduct its missions and operations."[213]

"Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive, and coercive. NATO will continue to adapt to the evolving cyber threat landscape, which is affected by both state and non-state actors, including state-sponsored. Cyber defence is part of NATO's core task of collective defence. We must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defence posture. We therefore continue to implement cyberspace as a domain of operations. We have agreed how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight."[214]

No espaço reservado à Ciberdefesa, no sítio da Defesa Nacional, é referido que "As atividades de ciberdefesa constituem uma nova área operacional da defesa nacional e um contributo fundamental para a cibersegurança do país." Por este motivo, muita da produção normativa que iremos abordar tem uma interdependência dos dois "ramos" do ciberespaço – segurança e defesa. É nesse sentido que, Paulo Viegas Nunes, no contributo que deu para a estratégia Nacional de Ciberdefesa, diz-nos que "assim como existe uma estreita ligação entre a Segurança e a Defesa Nacional, também a cibersegurança se revela indissociável da ciberdefesa do Estado. Na prática, isto significa que não será possível garantir a cibersegurança sem o levantamento de uma capacidade de ciberdefesa."[215]

Como vemos, cibersegurança e ciberdefesa são interdependentes compreendendo áreas comuns e áreas específicas. Assim, e fazendo apelo a um artigo de opinião do meu Camarada e Amigo, Coronel Jorge Ralo, iremos deixar uma definição de cada um dos "ramos" (segurança e defesa) do ciberespaço. Dizia então, àquela altura, o Tenente-coronel Jorge Ralo, que "Por ciberdefesa entendem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco a soberania e a segurança nacional (ciberguerra) e cuja responsabilidade de resposta recai nas Forças Armadas. Na cibersegurança incluem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco o espaço de liberdade individual/coletiva e de prosperidade que ele constitui e cuja responsabilidade de policiamento deve caber às Forças de Segurança e aos Serviços de Informações. A diferença entre a ciberdefesa e a cibersegurança é, por vezes, muito ténue e, devido à natureza de algumas

[213] ***Idem.***
[214] OTAN. ***Brussels Summit Declaration*** [Em linha]. 2018. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[215] ***Contributos para uma estratégia Nacional de Ciberdefesa***, IDN Cadernos, nº28, 2018, p. 64

ameaças, acabam por se sobrepor numa larga percentagem. Um ataque a uma infraestrutura crítica nacional, rede elétrica por exemplo, abrange as duas esferas."[216]

4.1. Política e Estratégia Nacional para a Ciberdefesa

Ao investigar esta matéria, "Política e Estratégia Nacional para a Ciberdefesa", e antes de nos centrarmos exclusivamente no normativo que diz respeito à ciberdefesa iremos fazer uma "viagem" àquilo que esteve na génese de grande parte da legislação que existe hoje sobre ciberdefesa.

Assim, começaremos por recuar à década de 90 do século XX, mais propriamente ao ano 1990.

A 28 de fevereiro de 1990 a Presidência do Conselho de Ministros emitiu a Resolução do Conselho de Ministros (RCM), n.º 5/90, que aprovava as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas e segurança informática (SEGNAC 4). Dizia a norma que "A diversidade e evolução dos equipamentos e programas dos sistemas informáticos não se coaduna com o estabelecimento de normas rígidas que prevejam todas as situações. Entendeu-se, por isso, estabelecer um conjunto de regras suficientemente flexível, de forma a deixar à Autoridade Nacional de Segurança a possibilidade de, caso a caso, apreciar a oportunidade das medidas a aplicar."[217]

A norma prognosticava que os sistemas informáticos iriam ser parte importante em certas atividades e dizia igualmente, no seu texto, que a falta de segurança dos dados e programas poderia afetar a integridade da informação, "…os sistemas informáticos tendem a tornar-se o principal suporte de certas atividades industriais, tecnológicas, administrativas e das investigações e que a falta de segurança de dados e programas pode influenciar, distorcendo, a ação competitiva nestas atividades."[218]

Esta RCM, de há 30 anos atrás, já manifestava uma preocupação na segurança dos dados e já considerava a informação como um ativo importante de empresas, instituições e organizações.

---

[216] Artigo de Opinião - ***CiberSegurança e CiberDefesa, Direção-Geral de Política de Defesa Nacional*** (DGPDN) [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em http://dgpdn.blogspot.com/2013/03/artigo-de-opiniao-ciberseguranca-e.html

[217] DRE. ***Resolução do Conselho de Ministros, nº5/90*** [Em linha]. 1990. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa-avancada/-/asearch/307435/details/maximized?perPage=100&anoDR=1990&types=SERIEI&search=Pesquisar

[218] ***Idem.***

No entanto, à data, segurança era quase sempre associado a segurança física e esta RCM, não fugia "à norma" tendo dois capítulos especialmente para esse efeito, capítulo III - Segurança física das instalações e Capítulo IV - Segurança de suportes físicos, "O presente capítulo define as instruções para a garantia da proteção física dos centros de informática, de forma a garantir a segurança dos dados, programas e materiais classificados contra a espionagem, sabotagem, terrorismo, comprometimento e divulgação não autorizada, especialmente a captação de radiações eletromagnéticas, introdução dos vulgarmente denominados «vírus informáticos» e violação dos acessos lógicos."[219]

Como se atesta na transcrição anterior, já se aborda o tema, "vírus informáticos", e embora o primeiro vírus informático tenha a data 1971 ou 1972, conforme autores, foi no final da década de 80 que eles começaram a proliferar.

Avançamos quase 20 anos, mais especificamente 19, e analisaremos uma lei, emitida pela Assembleia da República, a lei nº 109/2009, conhecida como a lei do Cibercrime, que "transponha para a ordem jurídica interna uma decisão da Comunidade Europeia (Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro)."[220]

Nesta lei já era visível a preocupação do acesso ilegítimo, estando tipificado na norma como "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático."[221] Assim como, de interceção ilegítima "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes"[222]

Três anos mais tarde começavam a ser edificados os pilares da Cibersegurança, e com base na RCM 42/2012, é criada a Comissão Instaladora do Centro Nacional de Cibersegurança, na dependência do Primeiro-Ministro. Esta Comissão tinha por "missão definir as medidas e os instrumentos necessários à criação, instalação e operacionalização de um Centro Nacional de Cibersegurança, bem como a estimativa dos encargos necessários à sua instalação e funcionamento."[223]

---

[219] ***Idem.***

[220] DRE. ***Cibercrime, Lei nº 109/2009*** [Em linha]. 2009. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa/-/search/489693/details/maximized

[221] ***Idem.***

[222] ***Idem.***

[223] Gabinete Nacional de Segurança. ***RCM, nº 42/2012*** – Comissão Instaladora do Centro Nacional de Cibersegurança [Em linha]. 2012. [Consult. 05 dez. 2019]. Disponível em https://www.gns.gov.pt/media/1924/rcm-42-2012.pdf

Em 2013, é aprovado o conceito estratégico de Defesa Nacional onde se começa a levantar uma capacidade de ciberdefesa nacional, "…a Assembleia da República, por iniciativa do Governo, debateu as grandes opções do conceito estratégico de defesa nacional. Este debate constituiu o corolário de uma ampla consulta aos mais diversos sectores da sociedade civil, conseguindo-se assim uma discussão a um tempo participada e aprofundada da política de defesa nacional.

Depois, tendo presente o conteúdo do debate produzido, que permitiu consolidar, nas suas grandes linhas, a orientação constante da proposta do Governo, foi elaborado o projeto de conceito estratégico de defesa nacional, o qual foi apreciado, num primeiro momento, pelo Conselho de Chefes de Estado-Maior e, posteriormente, pelo Conselho Superior de Defesa Nacional"[224]

Portugal encontrava-se ainda sob a intervenção da *troika* (FMI, Comissão Europeia e Banco Central Europeu) e encontrava-se mergulhado numa crise económico-financeira que se tinha concentrado na Europa, em particular na Zona Euro. Mas é neste cenário que é aprovado o "Conceito Estratégico de Defesa Nacional" onde é afirmado que Portugal deveria edificar uma capacidade de ciberdefesa nacional, "…definir uma Estratégia Nacional de Cibersegurança; montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários; sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de ciberdefesa nacional. Para fazer face aos atentados ao ecossistema, Portugal deverá reforçar a sua capacidade de resposta através da promoção de uma adequada articulação entre as políticas públicas com intervenção neste domínio e da maximização das capacidades civis-militares."[225]

Este Conceito Estratégico de Defesa Nacional (CEDN) "é um dos principais elementos que estruturam a política nacional de ciberdefesa, onde se identifica um conjunto de ameaças ao ciberespaço, a ter em conta, e o papel que a Defesa deve ter na manutenção das infraestruturas que suportam as sociedades e as economias globalizadas e interdependentes do século XXI."[226]

Nesse mesmo ano, e por despacho do Ministro da Defesa Nacional, nº 13692/2013 é publicado a orientação política para a Ciberdefesa, que em conjunto com o CEDN são

[224] DRE. ***Resolução do Conselho de Ministros, nº 19/2013*** – Aprova o Conceito Estratégico de Defesa Nacional [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa/-/search/259967/details/maximized

[225] ***Idem.***

[226] ***Sitio da Defesa Nacional.*** [Em linha]. 2020. [Consult. 02 jan. 2020]. Disponível em https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa

considerados documentos basilares para a edificação da ciberdefesa em Portugal. Estes dois documentos, produzidos em 2013, estão fortemente marcados com os acontecimentos ciber nos anos anteriores – ataques cibernéticos em 2007 (Estónia), 2008 (Geórgia) e 2010 (Irão). Essa constatação é confirmada na orientação política nacional de ciberdefesa, no seu texto inicial, dando grande ênfase ao potencial devastador que os ataques cibernéticos podem ter e preconiza a edificação de uma capacidade de ciberdefesa,

> *Considerando que o atual Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 21 de março, antecipa como grande tendência no ambiente de segurança global, o potencial devastador dos ataques cibernéticos, identificando o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários; Considerando que essas ações têm como alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada, constituindo por isso, riscos e ameaças prioritários que se replicam e multiplicam diretamente no plano interno; Reconhecendo que essas ações representam uma ameaça crescente sobre infraestruturas críticas, cujos efeitos e impactos podem provocar o colapso da estrutura tecnológica da organização social e económica do País; Tendo presente que o atual Conceito Estratégico de Defesa Nacional, reconhecendo esses desafios de segurança do ciberespaço, preconiza a edificação ao nível das Forças Armadas de uma capacidade de Ciberdefesa; (…)*
>
> *Determino a publicação da diretiva iniciadora com a Orientação Política para a Ciberdefesa, anexa ao presente despacho e que dele faz parte integrante.*[227]

Como observamos estava dado um importante passo para a criação de uma capacidade de ciberdefesa que tinha como pressupostos, vertidos na orientação, "a importância do ciberespaço como um espaço de defesa de valores e interesses; a afirmação do ciberespaço como espaço de atuação de operações militares; a dependência das Forças Armadas da livre utilização do ambiente de informação e do ciberespaço para gerirem as operações; a utilização do espaço cibernético, de modo a impedir ou dificultar ações contra interesses nacionais; garantir a segurança da informação que circula nos sistemas de informação e comunicações; harmonizar o planeamento da Defesa Militar com o desenvolvimento tecnológico da capacidade de ciberdefesa; potenciar sinergias no âmbito da União Europeia e OTAN e por fim atuar em colaboração com a sociedade portuguesa envolvendo MDN, EMGFA, Ramos, academia, setores público e privado e a indústrias da defesa."[228]

[227] DRE - ***Orientação para a política de Ciberdefesa***, Despacho n.º 13692/2013 [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/3295679/details/maximized?jp=true
[228] ***Idem.***

Para além dos pressupostos, a orientação política para a Ciberdefesa esta sectorizada em objetivos, princípios da ciberdefesa, responsabilidades e atualização e conta com 7 linhas orientadoras. Uma das linhas orientadoras, planeamento de defesa militar, já toma como adquirido que o ciberespaço é um teatro de operações,

> *Implementar a capacidade de ciberdefesa com vista a integrar as operações no ciberespaço no âmbito das capacidades militares. Para o efeito, incorporar no Processo de Planeamento de Defesa Militar, em conjugação com o NATO Defence Planning Process (NDPP) e com o Capability Defence Plan (CDP) da UE, o desenvolvimento da capacidade nacional de ciberdefesa. O levantamento desta capacidade deve ter por base o Conceito Estratégico de Defesa Nacional, o preconizado na diretiva "Defesa 2020", e todos os documentos relevantes para a mesma. De acordo com este enquadramento, identificar e hierarquizar através do Processo de Planeamento de Defesa os requisitos de ciberdefesa relevantes.*
>
> *A defesa contra as ameaças cibernéticas deve incluir o reforço da proteção das redes, a monitorização e análise dos padrões de tráfego, a deteção precoce de ataques e a resposta aos mesmos, envolvendo para esse efeito, sempre que necessário, a condução de operações no ciberespaço.*[229]

Em resumo, a orientação política para a Ciberdefesa é um documento estruturante e "identifica medidas concretas com vista à edificação de uma capacidade de ciberdefesa nacional, incluindo a criação de um Centro de Ciberdefesa, no âmbito do Estado-Maior-General das Forças Armadas (EMGFA)."[230]

Em nosso entender, estes dois documentos, o CEDN (2013) e o Despacho nº 13692/2013 do Ministro da Defesa Nacional, anteriormente analisados, são basilares para a construção da capacidade de Ciberdefesa em Portugal em concomitância com a Estratégia Nacional de Segurança do Ciberespaço e a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. É nestes dois documentos de 2015 e 2019 que nos vamos debruçar, em seguida, após a análise do normativo que estabelece o regime jurídico da segurança do ciberespaço transpondo a Diretiva 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

A lei nº 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço, "define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional e deverá ser aprovada por resolução do Conselho de

---

[229] ***Idem.***

[230] Sitio da Defesa Nacional. ***Ciberdefesa.*** [Em linha]. 2020. [Consult. 02 jan. 2020]. Disponível em https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa

Ministros, sob proposta do Primeiro-Ministro, ouvido o Conselho Superior de Segurança do Ciberespaço."[231] e aplica-se "à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais que prestam serviços de mercado em linha, de motor de pesquisa em linha e de computação em nuvem e que tenham o seu estabelecimento principal em território nacional ou, não o tendo, designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais, e a quaisquer outras entidades que utilizem redes e sistemas de informação."[232] Esta lei regula também a "Equipa de Resposta a Incidentes de Segurança Informática Nacional e o Centro Nacional de Cibersegurança, que deverá funcionar no âmbito do Gabinete Nacional de Segurança e é a Autoridade Nacional de Cibersegurança."

Em conclusão, todas as organizações que estão ligadas à internet podem ser vítimas de ataques cibernéticos e, consequentemente, podem vir a constituir uma importante ameaça ao normal funcionamento das redes e dos sistemas de informação, em particular da internet. Nesse sentido, apela-se "à necessidade de adoção de medidas de segurança das redes e dos sistemas de informação, tendo em conta os progressos técnicos mais recentes, para evitar os incidentes ou ataques cibernéticos; notificar os incidentes ao Centro Nacional de Cibersegurança e; cumprir as instruções de cibersegurança emanadas pelo Centro Nacional de Cibersegurança." [233]

No entanto, esta lei não se aplica, "a) Às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas; b) Às redes e sistemas de informação que processem informação classificada."[234]

Para finalizarmos esta análise, em relação à Política e Estratégia Nacional para a Ciberdefesa iremos analisar as RCM nº 36 e nº 92, de 2015 e 2019, respetivamente, documentos que consideramos estruturantes para a edificação da ciberdefesa em Portugal.

A RCM nº 36/2015, define a primeira estratégia nacional de segurança do ciberespaço, "A necessidade de proteger as áreas que materializam a soberania nacional, assegurando a autonomia política e estratégica do País, bem como o crescente número de incidentes e ataques

[231] CTSU Sociedade de Advogados SP, RL, S.A. – ***Alerta Legal 70*** [Em linha]. 2019 [Consult. 05 jan. 2020]. Disponível em https://www.ctsu.pt/ct/pt/pages/comunicacoes/articles/alerta-legal-70.html

[232] ***Idem.***

[233] Regime Jurídico da Segurança do Ciberespaço – ***Lei n.º 46/2018*** [Em linha]. 2018. [Consult. 05 jan. 2020]. Disponível em https://www.aguiarbranco.pt/noticias/regime-juridico-da-seguranca-do-ciberespaco-%E2%80%93-lei-n-462018-de-13-de-agosto/5

[234] DRE - ***Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016***, Lei nº46/2016 [Em linha]. 2016. [Consult. 05 jan. 2020]. Disponível em https://dre.pt/home/-/dre/116029384/details/maximized

maliciosos, impõe que a segurança do ciberespaço seja considerada como uma prioridade nacional. Por isso, é fundamental que o País disponha de uma Estratégia Nacional de Segurança do Ciberespaço, que estabeleça objetivos e linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio."[235]

Esta estratégia é alicerçada em cinco pilares, a subsidiariedade, a complementaridade, a cooperação, a proporcionalidade e for fim a sensibilização. Estes cinco pilares são importantes no "compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas"[236] para isso é necessário que a responsabilidade da segurança se inicie no próprio indivíduo utilizando o ciberespaço de uma forma responsável e acabe no Estado enquanto garante da soberania e dos princípios constitucionais.

Esta estratégia, conta com os seguintes objetivos estratégicos: "a) Promover uma utilização consciente, livre, segura e eficiente do ciberespaço; b) Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; c) Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; d) Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação."[237] Estes objetivos, permitem definir uma orientação traduzida em seis eixos de intervenção: "Eixo 1 — Estrutura de segurança do ciberespaço; Eixo 2 — Combate ao cibercrime; Eixo 3 — Proteção do ciberespaço e das infraestruturas; Eixo 4 — Educação, sensibilização e prevenção; Eixo 5 — Investigação e desenvolvimento; Eixo 6 — Cooperação."[238]

Entretanto, "Face ao rápido desenvolvimento intrínseco ao ciberespaço e, consequentemente, à crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização, ficou definido que a referida estratégia seria objeto de revisão num prazo de três anos."[239] Assim, através "da Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto,

[235] DRE - Estratégia Nacional de Segurança do Ciberespaço, RCM nº36/2015 [Em linha]. 2015. [Consult. 05 jan. 2020]. Disponível em https://dre.pt/home/-/dre/67468089/details/maximized
[236] ***Idem.***
[237] ***Idem.***
[238] ***Idem.***
[239] DRE – ***Estratégia Nacional de Segurança do Ciberespaço 2019 -2023***, RCM nº92/2019 [Em linha]. 2019. [Consult. 05 jan. 2020]. Disponível em https://dre.pt/home/-/dre/122498962/details/maximized

foi constituído um grupo de projeto, denominado Conselho Superior de Segurança do Ciberespaço, que teve como um dos seus objetivos propor a revisão e elaborar a nova Estratégia Nacional de Segurança do Ciberespaço (ENSC)."[240] A ENSC, é um documento estruturante para a capacitação nacional em matéria de segurança do ciberespaço. Assim, esta estratégia assenta em três objetivos estratégicos, "maximizar a resiliência, promover a inovação e gerar e garantir recursos. As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica, traduzida em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço."[241]

"Esta estratégia pretende não só garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, como também potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas. A execução da ENSC 2019-2023 permitirá tornar Portugal um país mais seguro, através de uma ação inovadora e resiliente que preserve os valores fundamentais do Estado de Direito e garanta o regular funcionamento das instituições."[242]

4.2. Estratégia OTAN para a Ciberdefesa

> *"Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive and coercive. NATO will continue to adapt to the evolving cyber threat landscape. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces."*[243]

As ameaças cibernéticas à segurança da Aliança são cada vez mais frequentes, complexas, destrutivas e coercitivas.[244]

---

[240] ***Idem.***
[241] ***Idem.***
[242] CNCS. ***Governo aprova nova Estratégia Nacional de Segurança do Ciberespaço.*** [Em linha]. 2019. [Consult. 05 jan. 2020]. Disponível em https://www.cncs.gov.pt/recursos/noticias/governo-aprova-nova-estrategia-nacional-de-seguranca-do-ciberespaco/
[243] OTAN. ***Cyber defence.*** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.html
[244] OTAN. ***NATO's role in cyberspace*** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/docu/reviwew/articles/2019/02/12/natos-role-in-cyberspace/index.html

Durante a conferência na Academia Militar, na Amadora, *Jamie Shea*, adjunto do secretário-geral da OTAN para os Novos Desafios de Segurança, afirmou que a OTAN enfrenta 200 milhões de ciberataques por dia .[245]

Durante a última década, os Aliados deram importantes passos para enfrentar este novo desafio. Mas foi em, 2002, durante a Cimeira de Praga que a Aliança pela primeira vez colocou na agenda política o tema ciberdefesa.

> *"We, the Heads of State and Government of the member countries of the North Atlantic Alliance, met today to enlarge our Alliance and further strengthen NATO to meet the grave new threats and profound security challenges of the 21st century. Bound by our common vision embodied in the Washington Treaty, we commit ourselves to transforming NATO with new members, new capabilities and new relationships with our partners. We are steadfast in our commitment to the transatlantic link; to NATO's fundamental security tasks including collective defence; to our shared democratic values; and to the United Nations Charter."*[246]

> *"Endorse the implementation of five nuclear, biological and chemical weapons defence initiatives, which will enhance the Alliance's defence capabilities against weapons of mass destruction: a Prototype Deployable NBC Analytical Laboratory; a Prototype NBC Event Response team; a virtual Centre of Excellence for NBC Weapons Defence; a NATO Biological and Chemical Defence Stockpile; and a Disease Surveillance system. We reaffirm our commitment to augment and improve expeditiously our NBC defence capabilities. Strengthen our capabilities to defend against cyber attacks."*[247]

Com a perceção de que o esforço deveria continuar e de que o tema ciberdefesa estava "cada vez mais atual" a OTAN reiterou essa posição na Cimeira de Riga, em 2006.

> *"The adaptation of our forces must continue. We have endorsed a set of initiatives to increase the capacity of our forces to address contemporary threats and challenges.*
>
> *These include:*

245 DN. ***NATO enfrenta 200 milhões de ciberataques por dia*** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.dn.pt/mundo/nato-enfrenta-200-milhoes-de-ciberataques-por-dia-5438838.html

246 OTAN. ***Prague Summit Declaration*** [Em linha]. 2002. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_19552.htm

247 ***Idem.***

> *work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber attack; "*[248]

O óbvio aconteceu e, em 2007, um Estado foi alvo de um ataque cibernético. Este ataque cibernético, que a Estónia sofreu em 2007, foi provavelmente o *trigger* para que a OTAN em 2008, aprovasse a sua primeira Política de Defesa Cibernética.

> *"NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities."*[249]

Neste mesmo ano, a 14 de maio, é criado em *Tallinn*, na Estónia, o novo centro de excelência em Ciberdefesa a "OTAN *Cooperative Cyber Defence Centre of Excellence*".

"O Centro recebeu a acreditação plena pela OTAN e alcançou o *status* de Organização Militar Internacional, a 28 de outubro de 2008. A OTAN *Cooperative Cyber Defence Centre of Excellence* é uma organização internacional, militar, com a missão de aumentar a capacidade, a cooperação e a partilha de informações entre os países membros da OTAN e os seus parceiros na defesa cibernética, educação, investigação e desenvolvimento, lições aprendidas e consulta."[250]

> *"Seven NATO nations and the Allied Command Transformation signed the documents for the formal establishment of a Cooperative Cyber Defence (CCD) Centre of Excellence (COE) in Tallinn, Estonia.*
>
> *The centre will conduct research and training on cyber warfare and include a staff of 30 persons, half of them specialists from the sponsoring countries, Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain.*
>
> *The need for a cyber defence centre to be opened today is compelling," said General James Mattis, NATO's Supreme Allied Commander Transformation, at the*

[248] OTAN. ***Riga Summit Declaration*** [Em linha]. 2006. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en
[249] OTAN. ***Bucharest Summit Declaration*** [Em linha]. 2008. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natolive/official_texts_8443.htm
[250] OTAN**.** ***NATO Cooperative Cyber Defence Centre of Excellence*** [Em linha]. 2008. [Consult. 05 dez. 2019]. Disponível em https://pt.qwe.wiki/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence

signing ceremony, "it will help NATO defy and successfully counter the threats in this área."[251]

Nesse mesmo ano, a Rússia demonstrou o potencial que os ataques cibernéticos poderiam ter, aquando sincronizados com um ataque convencional. Decorria o verão de 2008, e um dia antes da invasão russa à Geórgia, a Rússia desencadeou diversos ataques cibernéticos coordenados com a campanha militar.

Cerca de dois anos mais tarde, durante a Cimeira de Lisboa, em 2010, a Aliança declara que os ciberataques estavam a ser mais frequentes e mais sofisticados. Desde logo traçou objetivos, até 2012, com a criação e total operação, da *NATO Computer Incident Response Capability* (NCIRC), de modo a colocar todos os organismos da OTAN sob proteção cibernética centralizada. Outro dos objetivos, este até junho de 2011, era criar uma política aprofundada de defesa cibernética da OTAN e preparar um plano de ação para sua implementação.

"We have adopted a new Strategic Concept that lays out our vision for the Alliance for the next decade: able to defend its members against the full range of threats; capable of managing even the most challenging crises; and better able to work with other organisations and nations to promote international stability. NATO will be more agile, more capable and more cost-effective, and it will continue to serve as an essential instrument for peace. In accordance with the detailed provisions of this Declaration, we have also:

- agreed to enhance our cyber defence capabilities;"[252]

"Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability. To address the security risks emanating from cyberspace, we will work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably

[251] OTAN. ***NATO opens new centre of excellence on cyber defence*** [Em linha]. 2008. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/news_7266.htm?selectedLocale=en

[252] OTAN. ***Lisbon Summit Declaration*** [Em linha]. 2010. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_68828.htm?selectedLocale=en

> *on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011 and to prepare an action plan for its implementation."*[253]

Conforme decidido na Cimeira de Lisboa, o *North Atlantic Council* ficou encarregado em desenvolver uma política aprofundada de defesa cibernética para a OTAN, até junho de 2011, e concomitantemente preparar um plano de ação para sua implementação. Nesse sentido, e em cumprimento com a data proposta, junho de 2011, os Ministros da Defesa adotaram uma nova política de defesa cibernética.

> *"The revised policy will offer a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber threats and building resilience. All NATO structures will be brought under centralised protection, and new cyber defence requirements will be applied. The policy clarifies political and operational mechanisms of NATO's response to cyber attacks, and integrates cyber defence into NATO's Defence Planning Process. The policy also sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia.*
>
> *In parallel to the policy, a cyber defence Action Plan has been agreed. The Action Plan will serve as the tool to ensure the timely and effective implementation of the policy."*[254]

Os esforços em aumentar a capacidade cibernética continuaram e em 2012, durante a Cimeira de Chicago os aliados reafirmaram o compromisso de melhorar as suas defesas cibernéticas e foi criada a Agência de Comunicação e Informação da OTAN.

> *"Cyber attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which are now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012. We have committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection, to ensure that enhanced cyber defence capabilities protect our collective investment in NATO. We will further integrate cyber defence measures into Alliance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber*

[253] ***Idem***.
[254] OTAN. ***NATO Defence Ministers adopt new cyber defence policy*** [Em linha]. 2011. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/news_75195.htm

> *defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks. To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia"*[255]
>
> *"At our Summit in Lisbon, we agreed on an ambitious reform programme. This package of reforms remains essential for guaranteeing the Alliance is responsive and effective in carrying out the ambitious tasks envisioned in our Strategic Concept, the Lisbon Declaration, as well as the Declaration on Defence Capabilities we have adopted today. To this end:*
>
> *NATO Agencies. The consolidation and rationalization of the existing NATO Agencies' functions and services is underway with new NATO Agencies for Support, Communication & Information, and Procurement, to be stood up on 1 July 2012. The new Agencies' executives will work to optimise savings and improvements in effectiveness as the new entities mature over the next two years."*[256]

Na parte final do ano de 2014, durante a Cimeira no País de Gales, os Aliados apoiaram uma nova política de defesa cibernética, passando a fazer parte integrante da defesa coletiva da OTAN e acordaram que o direito internacional se aplicaria no ciberespaço.

Concomitantemente lançaram um desafio de cooperação ao setor privado, no sentido de discutir uma colaboração nesta área. Desafio que foi aceite e foi efetuada uma conferência, em *Mons*, com 1.500 participantes.

> *"As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that*

[255] OTAN. ***Chicago Summit Declaration*** [Em linha]. 2012. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en
[256] ***Idem.***

> *threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."*[257]

Na agenda de colaboração OTAN-EU, foram identificadas áreas de cooperação, que vão desde esforços conjuntos para combater ameaças híbridas, segurança cibernética e recursos de defesa, até a promoção da resiliência entre os parceiros. Nesse sentido, a 10 de fevereiro de 2016, a OTAN, conjuntamente com a União Europeia, celebrou um acordo técnico sobre defesa cibernética, de modo a que ambas as organizações conseguissem prevenir e responder melhor a ataques cibernéticos.

> *"We are convinced that enhancing our neighbours' and partners' stability in accordance with our values, as enshrined in the UN Charter, contributes to our security and to sustainable peace and prosperity. So that our neighbours and partners are better able to address the numerous challenges they currently face, we will continue to support their sovereignty, territorial integrity and independence, as well as their reform efforts. In fulfilling the objectives above, we believe there is an urgent need to:*
>
> *Expand our coordination on cyber security and defence including in the context of our missions and operations, exercises and on education and training."*[258]

O ciberespaço começa a ganhar cada vez mais importância e ninguém ficou surpreso quando se recebeu a notícia, durante a Cimeira de Varsóvia, em 2016, que a OTAN acabava de reconhecer um novo domínio de operações – o ciberespaço.

Decorrente do reconhecimento deste novo domínio, a Aliança recomendou aos aliados que deveriam melhorar as suas defesas cibernéticas aumentando a resiliência e a capacidade de resposta a ataques cibernéticos.

> *"Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on*

[257] OTAN. ***Wales Summit Declaration*** [Em linha]. 2014. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[258] EU-OTAN. ***The EU and NATO The essential partners*** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20and%20NATO.pdf

> *land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure more effective organisation of NATO's cyber defence and better management of resources, skills, and capabilities. This forms part of NATO's long term adaptation. We continue to implement NATO's Enhanced Policy on Cyber Defence and strengthen NATO's cyber defence capabilities, benefiting from the latest cutting edge technologies. We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable. We will continue to follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace. We welcome the work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace."*[259]

Na Cimeira de Bruxelas em 2018, os líderes aliados concordaram que as ameaças cibernéticas, à segurança da Aliança, se estavam a tornar mais frequentes, complexas, destrutivas e coercitivas. Nesse sentido, a Aliança teria que continuar o seu trabalho de adaptação a este "novo" cenário tendo consciência de que estes ataques poderiam ter origem em atores estatais e não estatais, inclusive patrocinados pelo estado.

Por outro lado, a OTAN reafirmava que a defesa cibernética fazia parte da defesa coletiva e que deveria ser capaz de operar com tanta eficácia no ciberespaço como no ar, na terra e no mar, de modo a fortalecer e apoiar a postura geral de dissuasão e defesa da Aliança. Os aliados concordaram ainda que, em caso de necessidade, a OTAN poderia recorrer às capacidades cibernéticas nacionais para suas missões e operações e que todos deveriam aumentar a sua resiliência nacional conforme o *Cyber Defence Pledge*. Aliás este recurso às capacidades nacionais de defesa do ciberespaço para as missões e operações da OTAN está em consonância com o que acontece em outros domínios, com os Aliados a contribuir com tanques, aviões e navios para operações e missões da Aliança.

> *"We have also taken far-reaching decisions to adapt and strengthen the NATO Command Structure, the military backbone of the Alliance. It will enable our Supreme Commanders to command and control forces to deal with any military challenge or security threat at any time, from any direction, including large-scale operations for collective defence, as well as ensure adequate transformation and preparation for the future, in particular through capability development, education, and training. We will establish a Cyberspace Operations Centre in Belgium to provide situational awareness and coordination of NATO operational activity within*

[259] NATO. ***Warsaw Summit Communiqué*** **[Em linha]**. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_133169.htm

> *cyberspace, a Joint Force Command Norfolk headquarters in the United States to focus on protecting the transatlantic lines of communication, and a Joint Support and Enabling Command in Germany to ensure freedom of operation and sustainment in the rear area in support of the rapid movement of troops and equipment into, across, and from Europe."*[260]

Desde que os Aliados reconheceram o ciberespaço como um domínio de operações, em 2016, a OTAN alcançou vários marcos importantes. Talvez o mais notável seja a criação, em outubro de 2018, de uma capacidade inicial ciber denominada *Cyberspace Operations Center*, ou CyOC.

Este CyOC é responsável pela preparação e planeamento das operações e missões da Aliança no ciberespaço e pode utilizar armas cibernéticas para derrubar mísseis ou defesas aéreas inimigas, destruir redes de inimigos, desmantelar propaganda de terrorismo ou fluxos de financiamento, tudo isto em operações de dissuasão. No entanto, para lançar ataques cibernéticos ofensivos, os membros da Aliança terão que estar de acordo sobre a razão do ataque. Este CyOC deverá estar totalmente operacional em 2023.

Para encarar as ameaças cibernéticas que enfrenta, a OTAN precisa de usar todas as ferramentas à sua disposição, incluindo políticas, diplomáticas e militares.

Em fevereiro de 2019, os Ministros da Defesa da OTAN aprovaram uma visão e estratégia para o ciberespaço, como um domínio de operações, onde estabelecem uma série de ferramentas para fortalecer ainda mais a capacidade da OTAN de responder a significativas atividades cibernéticas maliciosas. As opções de resposta descritas nesse documento irão ajudar a Aliança e os seus Aliados a aumentar sua consciência sobre o que está a acontecer no ciberespaço, desenvolvendo a sua resiliência e predispondo-os a trabalhar em conjunto, com parceiros, com a intenção de impedir, defender e combater todo o espectro de ameaças cibernéticas.[261]

> *"Cyber defenders from across the Alliance have a new community where they can exchange information, share best practices and work together in an encrypted workspace with secure video, voice, chat and information gathering capabilities. The community was launched today (12 February 2019) by the NATO Communications and Information Agency (NCIA).*
>
> *Computer emergency response teams from five countries are already connected to NATO's protected business network: Belgium, France, Netherlands, United*

[260] OTAN. ***Brussels Summit Declaration*** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_156624.htm

[261] OTAN. ***Cyber defence*** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.htm

> *Kingdom, and United States. Access to the network will roll out to all 29 Nations later this year.*
>
> *The launch of the cyber defenders' community is the first step toward the creation of an information hub for Allies, called the Cyber Security Collaboration Hub. This initiative was announced last year by NATO Secretary General Jens Stoltenberg, who said that one of NATO's key roles in cyber space is "to act as a hub for information sharing, training and expertise".*
>
> *The future hub will not require additional funds or staff, or changes in policy. The collaboration is facilitated through existing Memorandums of Understanding with NATO Nations."*[262]

O desafio da OTAN, para os próximos anos, está em perceber a natureza das ameaças cibernéticas, às quais estará exposta, avaliando e adaptando-se continuamente, de modo, a que as suas respostas sejam dadas em conformidade e à imagem e semelhança dos outros domínios, como terra, mar e ar, no ciberespaço, as ações da OTAN deverão ser defensivas, proporcionadas e alinhadas ao direito internacional.

4.3. Possibilidades portuguesas como Polo estratégico de Ciberdefesa

> *"A ciberdefesa é uma área de futuro. Como no século XV estivemos na primeira linha da descoberta do então desconhecido, há sempre novos desconhecidos para descobrir e é velha e honrosa a tradição de Portugal."*[263]

Para os Estados, os ataques cibernéticos representam uma ameaça à segurança nacional e à estabilidade do sistema internacional. Face a este novo paradigma, os Estados desenvolveram estratégias de defesa cibernética e estabeleceram estruturas dentro dos seus serviços de defesa e inteligência para combater os ataques cibernéticos.

Portugal, não poderia ficar indiferente a este novo rumo e, em abril de 2013, aprova o Conceito Estratégico de Defesa Nacional (CEDN) reconhecendo os ataques cibernéticos como fator de enorme risco. Estes ataques, são mencionados no ponto III do CEDN no âmbito das grandes tendências do contexto internacional, "O processo de globalização e a revolução tecnológica tornaram possível uma dinâmica mundial de integração política, económica, social

[262] OTAN. ***New NATO hub will gather the Alliance's cyber defenders*** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natolive/news_163358.htm?selectedLocale=en

[263] Expresso. Discurso do Primeiro Ministro, António Costa. ***NATO lança em Oeiras escola para ciberdefesa.*** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://expresso.pt/politica/2017-05-23-NATO-lanca-em-Oeiras-escola-para-ciberdefesa

e cultural sem precedentes. Criou um quadro de interdependência crescente, uma forte tendência de homogeneização e novas condições de progresso. Mas tornaram, também, possível uma difusão equivalente de ameaças e riscos em todas as dimensões, que incluem tanto a projeção das redes terroristas e de crime organizado, como a proliferação das armas de destruição massiva, a fragilização de Estados e o potencial devastador dos ataques cibernéticos."[264]

Ainda no mesmo documento, e em resposta à constatação desta nova ameaça, são definidas linhas de ação prioritárias, no sentido de criar estruturas que possam prevenir, monitorizar e reagir a ameaças, "No domínio da cibercriminalidade, impõe-se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados. Neste domínio, definem-se como linhas de ação prioritárias: garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN); definir uma Estratégia Nacional de Cibersegurança; montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários; sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de ciberdefesa nacional."[265]

No seguimento do conceito de estratégia de Defesa Nacional, e na continua necessidade de melhorar a proteção dos sistemas de comunicação e informação, face ao "potencial devastador dos ataques cibernéticos, identificando o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários"[266], é publicado nesse mesmo ano a orientação para a política de Ciberdefesa, com a finalidade de "…determinar os princípios essenciais, definir objetivos e estabelecer as correspondentes linhas orientadoras dos esforços a desenvolver, no âmbito da Defesa Nacional, visando, nomeadamente, o levantamento da capacidade nacional de Ciberdefesa."[267]

Nesta orientação política de Ciberdefesa, era vaticinado a aposta na formação e treino como forma de tornar Portugal num polo de excelência, neste domínio, indicando o caminho que deveria ser percorrido de forma a consegui-lo, "Centralizar a formação e o treino em ciberdefesa e constituir um polo de excelência neste domínio, evitando duplicações e aproveitando as competências e os recursos já existentes nas Forças Armadas, tendo presente a

[264] DRE. ***Resolução do Conselho de Ministros n.º 19/2013*** Aprova o Conceito Estratégico de Defesa Nacional [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa/-/search/259967/details/maximized
[265] ***Idem.***
[266] DRE. ***Despacho n.º 13692/2013*** Orientação para a política de Ciberdefesa [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/3295679/details/maximized?jp=true
[267] ***Idem.***

ligação à Escola de Comunicações e Sistemas de Informação da OTAN, a implementar no nosso país, e a possibilidade de Portugal, vir a liderar um projeto de "*smart defence*" no âmbito da "*education and training for cyberdefence*"."[268] Eram prioridades e condições que se viriam a concretizar.

Dois anos mais tarde Portugal deu uma resposta positiva ao ensejo plasmado na orientação para a política de Ciberdefesa, e no âmbito do primeiro "*NATO Cyber Defence*" Portugal foi convidado a assumir um dos projetos de "*smart defence*", "Projectos NATO na área da Ciberdefesa – MNCD2, MISP e MNCDE&T – sendo Portugal o país convidado para assumir a liderança, tanto na área do CIS *e-Learning* como do Ensino, Formação e Treino em Ciberdefesa. A transferência para Oeiras, até 2017, da *Nato Communications and Information System School* (NCISS) constitui também um desafio e uma oportunidade de afirmação nacional nesse domínio."[269]

Estavam lançados os alicerces para que Portugal começasse a criar condições para vir a ser um polo estratégico no ensino, formação e treino em Ciberdefesa.

Decorria o ano de 2015, e o desenvolvimento acelerado da sociedade da informação associado a uma crescente dependência das TIC, estimula Portugal a aprovar uma Estratégia Nacional de Segurança do Ciberespaço com a clara noção de que as novas tecnologias "…são, no entanto, vulneráveis, criando riscos sociais e materiais. Se, por um lado, trazem claros benefícios à sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos."[270].

Já em 2016, Portugal, liderando o projeto "*NATO smart defence Multinational Cyber Defence Education and Training (MNCDE&T)*" organiza a *"2nd NATO Cyber Defence Smart Defence Project",* que "apresenta uma oportunidade única para explorar novas ideias, orientadas para uma aproximação mais sinérgica dos Projetos *NATO de Smart Defence*, estimulando a cooperação com a indústria e com o meio académico, reforçando a complementaridade de esforços *NATO-EU* na área da Ciberdefesa e da Cibersegurança."[271]

---

[268] ***Idem.***

[269] 1st Nato Cyber Defense Conference. ***Ministério da Defesa Nacional Organiza Evento em Parceria com a NATO Industry Cyber Partnership (NICP) CIIWA e AFCEA*** [Em linha]. 2015. [Consult. 05 dez. 2019]. Disponível em https://www.sensysgroup.com/s/index.php?option=com_content&view=article&id=135&catid=16&Itemid=353&lang=pt

[270] DRE. ***Resolução do Conselho de Ministros n.º 36/2015*** Aprova a Estratégia Nacional de Segurança do Ciberespaço ***AFCEA*** [Em linha]. 2015. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/home/-/dre/67468089/details/maximized

[271] ***2nd NATO Cyber Defence Smart Defence Projects´*** **Conference** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://academiamilitar.pt/2nd-nato-cyber-defence-smart-defence-projects-conference.html

Até agosto de 2018, altura em que é estabelecido o "regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União"[272], Portugal organiza e patrocina as 3ª e 4ª conferências da *NATO Cyber Defence*.

Com a organização destas conferências, Portugal vai consolidando a sua posição neste domínio "Neste contexto, tanto ao nível NATO como da UE, Portugal tem vindo a estabelecer pontes e a contribuir para estimular a cooperação NATO-EU, nomeadamente, no campo da Educação e Treino em Ciberdefesa."[273]

Mas é na 4ª conferência, em 2018, que é dado um salto de qualidade, sendo atribuído um maior peso a dois *players* importantíssimos – Academia e Indústria. Entre alguns objetivos, esta conferência tinha dois objetivos que considerámos como principais. O primeiro, visava "Discutir o currículo comum e o papel das Universidades no desenvolvimento de uma *Cyber Workforce* experiente, promover o envolvimento e a participação da Industria e das Universidades no processo de desenvolvimento de capacidades da NATO e nacionais, no sentido da transformação e inovação da E&T de Ciberdefesa."[274]. Este objetivo, foi amplamente discutido na conferência, de modo a criar um programa de treino de segurança cibernética fornecendo aos candidatos treino técnico avançado e certificações reconhecidas pela academia e indústria. O segundo objetivo, visava a "implementação do *Cyber Academia and Innovation Hub*."[275]

Ao discursar na sessão da abertura da 4ª Conferência Internacional *NATO Cyber Defence, Smart Defence Projects*, na Academia Militar, a 19 de abril, José Azeredo Lopes, Ministro da Defesa Nacional, "considerou que Portugal terá de desempenhar um papel crucial no processo de desenvolvimento de capacidades de ciberdefesa ao nível da educação, treino e qualificação dos recursos humanos face à transferência da Academia da NATO de Latina, em Itália, para Oeiras, e com o consórcio composto por 40 membros da academia, indústria e outras organizações, o *Cyber Academia and Innovation Hub*."[276]

---

[272] DRE. ***Lei n.º 46/2018*** Regime jurídico da segurança do ciberespaço. [Em linha]. 2018. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/116029384/details/normal?l=1

[273] Academia Militar. ***3rd NATO Cyber Defence Smart Defence Projects' Conference.*** [Em linha]. 2015. [Consult. 05 dez. 2019]. Disponível em https://academiamilitar.pt/3rd-nato-cyber-defence-smart-defence-projects-conference.html

[274] Academia Militar. ***4th NATO Cyber Defence Smart Defence Projects' (CD SDP) Conference.*** [Em linha]. 2018. [Consult. 18 nov. 2019]. Disponível em https://academiamilitar.pt/4th-nato-cyber-defence.html

[275] ***Idem.***

[276] Discurso de José Alberto Azeredo Lopes, Ministro da Defesa Nacional. ***Intervenção do Ministro da Defesa Nacional, José Alberto Azeredo Lopes, por ocasião da sessão de abertura da 4ª Conferência Internacional NATO Cyber Defence, Smart Defence Projects.*** [Em linha]. 2018. [Consult. 18 nov. 2019]. Disponível em

Dando resposta a esta vontade política e na senda da excelência em educação, formação e treino, Portugal viria a criar o *Cyber Academia and Innovation Hub*, sendo uma "…iniciativa nacional que surge do projeto *Smart Defence, NATO Multinational Cyber Defence Education and Training* (MN CD E&T), liderado por Portugal, com vista à edificação de uma *Interim Facility* onde possa ser ministrada formação em Ciberdefesa e Cibersegurança. Esta *Interim Facility* irá ficar instalada na Academia Militar – Sede, no Paço da Rainha, até à entrada em funcionamento da *NCI Academy* em Oeiras."[277]

"Portugal passará a dispor de uma infraestrutura para apoiar as necessidades de formação e treino, a nível nacional, das Forças Armadas, Forças e Serviços de Segurança, Administração Pública, meio académico e Indústria. Prevê-se ainda que profissionais estrangeiros, civis e militares, possam frequentar estes cursos no âmbito de acordos bilaterais ou estabelecidos com organizações internacionais, regionais e multilaterais, tais como a NATO, a União Europeia, a CPLP e a iniciativa 5+5."[278]

"Pretende-se construir um Centro de Excelência Nacional na área da Educação, Formação, Treino e Inovação nos domínios da Cibersegurança e Ciberdefesa, que se constitua como um nó de uma rede cooperativa internacional, onde Portugal desempenhe um papel central, articulando os esforços em curso no âmbito nacional com o contexto NATO e da UE. Este polo, funcionando como *Knowledge Hub*, desenvolverá uma estreita ligação com a Academia, Indústria e outros espaços de inovação nacionais e internacionais."[279]

Ainda na consecução do segundo objetivo da 4ª conferência da *NATO Cyber Defence*, Portugal, em 15 de março de 2019, entrega, numa cerimónia simbólica, a chave da Academia de Comunicações e Informação da OTAN, ao Diretor-Geral da Agência de Comunicações e Informação. "A Escola NATO de Comunicações e Sistemas de Informação contribui, assim, para afirmar Portugal como um centro de desenvolvimento de "*know how*" e conhecimento nos domínios das comunicações e da ciberdefesa, áreas estratégicas da NATO e de grande importância para a Defesa Nacional."[280]

---

https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=7f9455c6-cc7f-4b9e-a939-895ecf18aeae (Tradução livre do autor)

[277] Academia Militar. ***Cerimónia Oficial de Assinatura do Non Disclosure Agreement da iniciativa Cyber Academia and Innovation Hub.*** [Em linha]. 2018. [Consult. 17 nov. 2019]. Disponível em https://academiamilitar.pt/cerimonia-oficial-de-assinatura-do-non-disclosure-agreement.html

[278] ***Idem.***

[279] ***Idem.***

[280] Sitio da Defesa Nacional. ***Portugal entrega formalmente escola da NATO que pretende responder aos desafios da Ciberdefesa e Cibersegurança.*** [Em linha]. 2019. [Consult. 22 nov. 2019]. Disponível em https://www.defesa.gov.pt/pt/comunicacao/noticias/Paginas/Portugal-entrega-formalmente-escola-da-NATO-que-pretende-responder-aos-desafios-da-Ciberdefesa-e-Cibersegurança.aspx

Segundo o Ministro da Defesa Nacional, João Gomes Cravinho, a criação desta Academia reveste-se de grande importância para o mundo militar, assim como, para o mundo civil pois deverá debruçar-se sobre matérias de "duplo uso, civil e militar", "É, portanto, uma grande vantagem para Portugal termos entre nós a NCIA, porque temos a possibilidade de criar profícuas sinergias com o mundo universitário – o Instituto Universitário Militar, mas também todas as universidades civis, incluindo a Nova aqui ao lado", acrescentou."[281]

A capacidade desta nova Academia é enorme e trará um prestigio enorme a Portugal, dando um enorme passo no caminho da excelência, "Uma vez em funcionamento pleno, prevê-se que possam ser ministrados 400 cursos por ano, para um universo estimado de 6000 estudantes, oriundos de todos os países que integram a Aliança Atlântica. Uma nova vida para o Reduto Gomes Freire, como salientou o Ministro da Defesa, que será também sentida na economia nacional e local."[282]

Com toda esta dinâmica, Portugal, em 2019, organiza a *5th NATO Cyber Defence Smart defence Projects' Conference* consolidando e reforçando a posição portuguesa no domínio da ciberdefesa.

Em termos normativos, a última estratégia nacional de segurança do ciberespaço datava de 2015, e face à evolução digital ocorrida desde então havia que criar um novo normativo que fosse estruturante para a capacitação nacional neste âmbito "definindo o enquadramento, os objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço, de acordo com o interesse nacional."[283] Nesse sentido, em 5 de junho de 2019, é emitida uma resolução do conselho de Ministros, nº 92/2019 com a aprovação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

Esta estratégia, "assenta em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica, traduzida em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço.

A consecução da ENSC 2019-2023 permitirá tornar Portugal um país mais seguro e próspero, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores

[281] ***Idem.***
[282] ***Idem.***
[283] DRE. ***Resolução do Conselho de Ministros n.º 92/2019.*** Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. [Em linha]. 2018. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/home/-/dre/122498962/details/maximized

fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade."[284]

Por fim, e fazendo recurso ao sítio da Defesa Nacional – Ciberdefesa, de modo a demonstrar que Portugal tem condições para assumir um papel fundamental no âmbito da ciberdefesa enunciarei alguns dos projetos e exercícios em que Portugal participou e em alguns deles exercendo liderança.

Projeto *NATO de Smart Defence 1.36, Multinational Cyber Defence Education and Training (MN CD E&T)* – projeto que Portugal liderou de 2014 a 2019 com o objetivo de "…criar uma plataforma de coordenação da Educação e Treino em Ciberdefesa e desenvolver novas iniciativas de Formação e Treino, destinadas a ajudar a NATO e as nações participantes a preencher as lacunas identificadas."[285]

Projeto *Headline Gold Task Force/EU Military Training Group (HTF/EUMTG) Cyber Defence (CD) Discipline* – "Tendo por base a experiência adquirida no âmbito do Projeto MN CD E&T, Portugal manifestou também a sua disponibilidade para liderar, conjuntamente com a França, a *Cyber Defence Discipline* do *EU Military Training Group* (EUMTG), estabelecida pela União Europeia em junho de 2014."[286]

A extensão nacional do projeto *MultiNational Smart Defence Project on Cyber Defence Education & Training* – Em 2015 foi criada uma extensão nacional deste projeto com a participação de 118 organizações "…organizações públicas – incluindo o Centro de Ciberdefesa das Forças Armadas e o Centro Nacional de Cibersegurança, Instituições Universitárias, Centros de Investigação, Associações, Bancos e Empresas, tem-se vindo a afirmar como um elemento estruturante do desenvolvimento das capacidades nacionais de Cibersegurança e Ciberdefesa, onde a Direção-Geral de Recursos da Defesa Nacional, as Forças Armadas, a DIRCSI/EMGFA e a Academia Militar (AM) têm vindo a desenvolver um importante papel agregador das atividades em curso."[287]

Projeto *Cyber Defence Training and Exercise Coordination Platform* (CD TEXP) – em 2015 "foi atribuída ao nosso País a responsabilidade pela gestão da Plataforma Centralizada de Educação e Treino em Ciberdefesa da União Europeia. Prevendo-se que esta plataforma possa vir a ser utilizada tanto no domínio da UE como internacional (ex: NATO, CPLP, etc.) e

[284] ***Idem.***
[285] Sitio da Defesa Nacional. ***Ciberdefesa.*** [Em linha]. 2019. [Consult. 02 nov. 2019]. Disponível em https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa
[286] ***Idem.***
[287] ***Idem.***

nacional, Portugal passará a ocupar uma posição central numa rede de Centros de Excelência e polos de conhecimento nacionais e internacionais."[288]

Projeto de Federação de *Cyber Ranges* da União Europeia (UE) – este projeto de cooperação militar no âmbito da EU tem como objetivo principal "apoiar o treino e exercício de ciberdefesa, com a utilização de *Cyber Ranges*, otimizando as funcionalidades e o uso desta onerosa tecnologia."[289]

Projeto *Cyber Academia and Innovation Hub* – "Esta iniciativa nacional surge do projeto *Smart Defence da NATO, Multinational Cyber Defence Education and Training (MN CD E&T)*, liderado por Portugal, com vista à edificação de uma capacidade na formação e treino (E&T) em Ciberdefesa e Cibersegurança de forma a alimentar o ecossistema nacional com as competências necessárias.

A 16 de março de 2018, foi assinado por 40 organizações e empresas, do sector público e privado, nacionais e estrangeiras que constituem o Consórcio inicial, no Ministério da Defesa Nacional, o *Non Disclosure Agreement*, que marca o início da iniciativa *Cyber Academia and Innovation Hub*. Esta é uma iniciativa que se pretende aberta, inclusiva e autossustentada, com a adoção do modelo de custos partilhados (*burden sharing*), onde cada participante contribuirá com o que tem de melhor e ao melhor preço."[290]

Esta iniciativa é das iniciativas mais importantes destes últimos anos neste âmbito, pois "permitirá que Portugal passe a dispor de uma infraestrutura para apoiar as necessidades de formação e treino nacional (Forças Armadas, Forças e Serviços de Segurança, Administração Pública, meio académico e Indústria nacional) e internacional (NATO, União Europeia, CPLP e Iniciativa 5+5), podendo transformar-se num Centro de Excelência, nas áreas da Educação, Formação, Treino e Inovação no âmbito da Cibersegurança e Ciberdefesa, com o envolvimento da indústria e das universidades nacionais e estrangeiras."[291]

Projeto *Cyber Talks* – "Iniciativa implementada pela Direção-Geral de Recursos da Defesa Nacional (DGRDN) com vista a promover a reflexão e a partilha de conhecimento ligadas à Ciberdefesa. Com recurso a entidades relevantes no domínio da Ciberdefesa e Cibersegurança, nacionais e internacionais, pretende-se de uma forma periódica criar um fórum de discussão que possa aumentar a consciencialização e adicionar valor à capacidade de Ciberdefesa da Defesa Nacional e das Forças Armadas."[292].

[288] ***Idem.***
[289] ***Idem.***
[290] ***Idem.***
[291] ***Idem.***
[292] ***Idem.***

Como acabámos de demonstrar, Portugal tem vindo a definir uma política nacional, no âmbito do ciberespaço, criando competências e capacidades, principalmente ao nível do ensino, formação e treino.

Assim, em nosso entender, Portugal é um bom exemplo de como um pequeno país pode ter um papel importante na OTAN ao liderar uma determinada área.

Com o acolhimento da Academia de Comunicações e Informação da OTAN, com o *Cyber Academia and Innovation Hub*, com a formação na Academia Militar em ciberdefesa com uma pós-graduação, com o Instituto Universitário Militar a desenvolver formação também nesta área, em parceria com as universidades do país, com o reforço de verbas na lei de programação militar para o investimento em ciberdefesa, "triplicando os montantes existentes, para um total de 51 milhões de euros, para o período 2019-2030"[293], com a liderança nestes últimos quatro anos dos programas "*Smart Defense*" a criar operadores informáticos mais qualificados e a contribuir para acabar com a falta de competências, demonstrámos que Portugal está no caminho certo para ser considerado um Polo relevante e estratégico na rede de centros de excelência cibernéticos da OTAN e que não é preciso ser grande para se ser líder na Aliança.

[293] ***Idem.***

5. Conclusão

William Gibson, em 1984, utilizou o termo ciberespaço num livro de sua autoria intitulado *Neuromancer*. Este livro, de ficção científica, apresentava novos conceitos para a época, como a inteligência artificial e um espaço de comunicação aberta de interligação mundial entre todos os computadores designado – ciberespaço.

Passados 30 anos, este conceito é uma realidade e na parte final de 2014, durante a Cimeira no País de Gales, os Aliados apoiaram uma nova política de defesa cibernética, passando a fazer parte integrante da defesa coletiva da OTAN e acordaram ainda que o direito internacional se aplicaria neste novo domínio.

O ciberespaço começou a ganhar cada vez mais importância e ninguém ficou surpreso quando na Cimeira de Varsóvia, em 2016, foi anunciado que a OTAN acabava de reconhecer um novo domínio de operações – o ciberespaço, tais como o são a terra, o mar, o ar e o espaço.

Decorrente do reconhecimento deste novo domínio, a Aliança recomendou aos aliados que deveriam melhorar as suas defesas cibernéticas, aumentando a resiliência e a capacidade de resposta a ataques cibernéticos, pois neste mundo interconectado e globalizado de hoje, a segurança cibernética tornou-se extremamente importante para os Estados.

Os Estados desenvolvidos, contam com sistemas informatizados, nas principais áreas, como são, a defesa nacional, as infraestruturas, os sistemas bancários e, como não poderia deixar de ser, todo o comércio eletrónico, dentro e fora das suas fronteiras.

Assim, o ciberespaço tornou-se num espaço apetecível para ataques cibernéticos capazes de afetar gravemente a tranquilidade das populações, podendo mesmo ter como consequência perdas relevantes no plano económico, de vidas humanas ou constituir uma ameaça séria à defesa e integridade dos Estados.

Todos estes juízos, são alicerçados na história recente. O primeiro grande ciberataque foi em 2007 e teve a Estónia como alvo. Este ciberataque foi um alerta para os estónios, ajudando-os a identificar *in loco* as suas vulnerabilidades.

Cerca de um ano mais tarde, ocorreu um novo ataque, e teve um cariz mais militar. Foi o primeiro caso em que um ciberataque ocorreu de um modo síncrono com um ataque convencional e aconteceu no conflito que opôs a Geórgia à Rússia. Se algumas dúvidas restavam, este acontecimento esclareceu que havia um novo espaço para o conflito armado – o ciberespaço.

Como já referido, este foi o primeiro caso em que um conflito internacional político e militar, foi acompanhado, ou mesmo precedido, por uma ofensiva de ataques cibernéticos e

parece ter sido bem-sucedido, pois ao mesmo tempo que era lançado um ataque cibernético apontando para o controlo do ciberespaço, criando o pânico e desinformação, foi efetuada uma invasão militar utilizando os domínios terrestre, aéreo e marítimo.

O terceiro ataque atingiu o maior grau de sofisticação. Em 2010, as centrifugadoras de *Natanz*, usadas no programa nuclear do Irão foram atacadas com o *malware Stuxnet*.

A importância atribuída a este evento, prende-se com o facto de que este foi o primeiro incidente documentado, em que uma arma cibernética real foi implantada com a intenção de negar, interromper, degradar e destruir a operacionalidade de um determinado sistema.

Estes três exemplos reforçam a ideia de que o novo espaço de guerra está aí, obrigando os Estados a aumentar a prevenção e a criar uma capacidade de ciberdefesa de forma a combater os efeitos desses ataques e retardar ou mesmo inibir os ciberataques. Todos eles diferentes, mas com um ponto em comum. Em nenhum deles se provou o culpado pelo ataque.

No entanto, existem autores, como *Thomas Rid*, que duvidam que alguma vez a guerra cibernética esteja a chegar. Mas *Rid* vai mais longe e diz-nos que a guerra cibernética nunca ocorreu no passado, não está a ocorrer e que muito provavelmente não irá ocorrer no futuro.

No entanto, Portugal acredita que este mundo interconectado, com características muito peculiares, desenvolve "o cibercrime e, em particular, o cibercrime organizado, associado à fraude bancária e à usurpação de identidade com este mesmo propósito, o *hacktivismo* político nas suas várias expressões, como são o desvio e a revelação de informação sensível ou classificada e a sabotagem informática, ou ainda a crescente espionagem de Estado e industrial"[294]

Nesse sentido, Portugal, em 2013, publicou, por despacho do Ministro da Defesa Nacional, uma Orientação para a Política de Ciberdefesa que "tem por finalidade determinar os princípios essenciais, definir objetivos e estabelecer as correspondentes linhas orientadoras dos esforços a desenvolver, no âmbito da Defesa Nacional, visando, nomeadamente, o levantamento da capacidade nacional de Ciberdefesa"[295]. Ainda no referido despacho, são definidos "objetivos da Política de Ciberdefesa: 1) Garantir a proteção, a resiliência e a segurança das redes e dos Sistemas de Informação e Comunicações da Defesa Nacional contra ciberataques; 2) Assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil

[294] PRESIDÊNCIA DO CONSELHO DE MINISTROS – **Resolução do Conselho de Ministros n.º 36/2015**. p. 3738.
[295] O Ministro da Defesa Nacional, José Pedro Correia de Aguiar Branco. **Despacho n.º 13692/2013.** p. 31977.

contra o interesse Nacional; 3) Contribuir de forma cooperativa para a cibersegurança nacional."[296]

Dois anos mais tarde, o poder governativo volta a legislar sobre o tema, agora numa Resolução do Conselho de Ministros, n.º 36/2015, com o nome de Estratégia Nacional de Segurança do Ciberespaço.

Portugal começa a marcar posição nesta matéria e a aposta é clara face a uma ameaça constante.

Com todo este suporte legal, definição estratégica e alavancado com a infraestrutura acolhida em Oeiras – Escola da NATO de Comunicações e Sistemas de Informações (NCISS), Portugal começa a ganhar uma posição impar para potenciar um conjunto de capacidades de grande importância para a Defesa Nacional, contribuindo significativamente para a afirmação de Portugal como um centro de conhecimento e desenvolvimento nos domínios da Ciberdefesa.

Esta janela de oportunidade deve ser aproveitada por Portugal, no seio da OTAN, pois atualmente, o nosso país não tem uma posição de relevo no âmbito da Aliança, face à reduzida capacidade armamentista portuguesa, ocupando o modesto 19.º lugar entre os 27. Mesmo comparado com países congéneres, como a Bélgica, a Holanda e a Dinamarca, países de média dimensão europeia, fundadores da OTAN e membros da União Europeia (EU) e da Organização das Nações Unidas (ONU), Portugal continua a não ter uma posição de destaque.

O ranking OTAN destes três países Bélgica (20/27), Holanda (12/27) e Dinamarca (16/27) é proporcional aos recursos financeiros postos à disposição da Defesa destes países. Assim, segundo *The World Factbook* da CIA (dados de 2018), embora a percentagem em relação ao *PIB* não seja muito díspar 0,93% para a Bélgica, 1,21% para a Holanda, 1,30% para a Dinamarca e 1,43% para Portugal, quando analisamos em termos de valor (em euros), essas diferenças são exponenciadas em consequência da riqueza desses países. Exemplificando a afirmação anterior, Portugal é o país que mais esforço faz em relação à sua riqueza (1,43%) e a Bélgica está em completo contraste (0,93%), mas, segundo o *Military Balance* (2019) a diferença entre os valores que foram postos à disposição da Defesa dos dois países, em 2018, foi, aproximadamente, dois mil milhões de euros (2,18 mil milhões de euros para Portugal e 4,20 mil milhões de euros para a Bélgica).

[296] ***Idem.***

Esta diferença é agudizada quando falamos da Holanda e da Dinamarca, pois são postos à disposição da Defesa na Holanda 9,53 mil milhões e 3,82 mil milhões[297] para a Dinamarca (conversão de dólar para euro ao câmbio do dia 12jan2020).

Assim, em conclusão, e respondendo ao nosso primeiro objetivo específico, "Avaliar e comparar a capacidade armamentista portuguesa face a alguns congéneres no âmbito da Aliança", diríamos que, Portugal tem uma débil capacidade armamentista, mesmo comparado com países congéneres. Em termos de capacidade militar, Portugal ocupa o 67.º lugar ao nível mundial (entre 137 países considerados pela *GFP* na avaliação da capacidade militar), o que significa que se encontra a meio da tabela, sendo reflexo da sua capacidade militar. Em comparação com os três países só a Bélgica se encontra ainda abaixo de Portugal no 68.º lugar. Holanda e Dinamarca, encontram-se alguns lugares acima, embora a Holanda se encontre substancialmente acima com os 35.º e 61.º lugares respetivamente.

Deixando a perspetiva mundial e passando para uma perspetiva europeia, os valores pioram para Portugal pois deixa de estar a meio da tabela, passando para uns lugares abaixo desse patamar, ocupando, em termos europeus, o 18.º lugar (de 25). A Bélgica continua um lugar abaixo e a Holanda e a Dinamarca continuam com a mesma preponderância manifestada a nível mundial, ocupando os 10.º e 13.º lugares entre os 25 países da EU abrangidos na análise da *GFP*.

O cenário não muda de figura quando analisamos a OTAN. Como anteriormente, Portugal e Bélgica encontram-se separados por um lugar, ocupando a segunda parte da tabela com os lugares 19.º e 20.º e a Holanda e a Dinamarca ocupam a primeira parte da tabela com a Holanda em lugar de destaque, no 12.º lugar, enquanto Dinamarca ocupa a 16.ª posição.

Fica, deste modo, demonstrado que Portugal não tem uma posição de relevo, na OTAN, no que à sua capacidade armamentista diz respeito.

Quanto ao segundo objetivo específico, "Demonstrar que o ciberespaço como sistema do caos, com um caráter de desterritorialização e omnipresença, é tão crítico para a defesa nacional e internacional, quanto os domínios clássicos da terra, do mar, do ar e do espaço sendo por isso apelidado como o quinto domínio das operações militares. Ao mesmo tempo, representa um desafio aos conceitos militares tradicionais em todos os níveis da guerra: estratégica, operacional e tática.", os três ciberataques, anteriormente mencionados (Estónia, Geórgia e Irão) são só por si, "exemplos reais" de que o ciberespaço é tão crítico para a defesa nacional,

[297] ***Banco de Portugal*** **Conversor de moeda do Banco de Portugal.** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.bportugal.pt/conversor-moeda?from=USD&to=EUR&date=1578787200&value=4250000000

como são os domínios terra, mar, ar e espaço. Por outro lado, a aprovação por parte da OTAN, na Conferência em Varsóvia, de que o ciberespaço seria considerado um novo domínio das operações militares é a constatação de que este novo domínio é uma realidade, levando a que todos os países da Aliança o adotassem.

Entretanto, o ciberespaço vem desafiar todos os conceitos militares tradicionais, pois como observámos no ataque à Geórgia, este novo domínio, conjugado com os outros quatro, vem trazer ao teatro de operações novos conceitos e ações nunca antes utilizadas, e.g. inibição de acesso a informação e desinformação.

Fica, deste modo, demonstrado, face aos argumentos descritos anteriormente, que o ciberespaço é um instrumento na área do armamento.

Quanto ao terceiro e último objetivo específico, "Demonstrar que Portugal, membro fundador da OTAN, deverá estar comprometido com a inovação e a transformação que a Aliança está a protagonizar sobre o tema ciberespaço, tornando-se num polo relevante e estratégico", demonstrámos que Portugal, para além de todo o comprometimento inscrito na diversa legislação publicada, e.g. Criação da Comissão Instaladora do Centro Nacional de Cibersegurança, Orientação para a política de Ciberdefesa e Estratégia Nacional de Segurança do Ciberespaço 2019-2023, tem condições para ir mais além, estando a concretizar-se, e.g. na liderança do programa *Smart Defence - Multinational Cyber Defence Education and Training Project*, no acolhimento da Academia de Comunicações e Informação da OTAN, na criação do *Cyber Academia and Innovation Hub,* que congrega a indústria e a comunidade académica e outros espaços de inovação nacionais e internacionais, até ao reforço de verbas na lei de programação militar para o investimento em ciberdefesa, "triplicando os montantes existentes, para um total de 51 milhões de euros, para o período 2019-2030."[298]

Fica, deste modo, demonstrado que Portugal pode, e tem condições, no que ao ciberespaço diz respeito, para ser considerado um país indispensável em operações combinadas e conjuntas OTAN.

Após utilizar como metodologia de pesquisa para desenvolvimento da dissertação o método de abordagem dedutivo e no que se refere ao procedimento, os métodos comparativo e estudo de caso, estamos em condições de responder à pergunta de partida deste trabalho, "Haverá condições para Portugal suprir as suas carências armamentistas do presente através do desenvolvimento cibernético?"

[298] Sitio da Defesa Nacional. ***Ciberdefesa.*** [Em linha]. 2019. [Consult. 02 nov. 2019]. Disponível em https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa

Em nosso entender, demonstrámos que Portugal, tem carências armamentistas, pois, segundo o ranking da *GFP*, encontra-se num lugar modesto em termos mundiais, europeus, assim como, em relação à OTAN. Mesmo quando comparado com a Bélgica, a Holanda e a Dinamarca, fica em 3º lugar, ficando somente à frente da Bélgica. Por outro lado, Portugal tem uma janela de oportunidade, e em nossa opinião, está a dar passos certos e seguros, para suprir essa carência com uma posição forte no desenvolvimento cibernético. A implementação do *Cyber Academia and Innovation Hub*, onde Portugal desempenha um papel central, na área da educação, formação e treino nos domínios da Cibersegurança e Ciberdefesa; o acolhimento da Escola OTAN de Comunicações e Sistemas de Informação que contribui para afirmação de Portugal como um centro de desenvolvimento de "*know how*" e conhecimento nos domínios das comunicações e da ciberdefesa, áreas estratégicas da OTAN e de grande importância para a Defesa Nacional; com a experiência de liderança, nestes últimos quatro anos, dos programas *Smart Defence* a criar condições para a formação de operadores informáticos mais qualificados e a contribuir para melhores competências; Portugal, é um bom exemplo de como um pequeno país pode ter um papel importante na OTAN ao liderar uma área.

Portugal demonstrou que não é preciso ser grande para se ser líder na Aliança.

6. Bibliografia

1st NATO **Cyber Defence Conference.** [Em linha]. 2015. [Consult. 05 dez. 2019]. Disponível em https://www.sensysgroup.com/s/index.php?option=com_content&view=article&id=135&catid=16&Itemid=353&lang=pt

2nd NATO **Cyber Defence Smart Defence Projects´ Conference** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://academiamilitar.pt/2nd-nato-cyber-defence-smart-defence-projects-conference.html

3rd NATO **Cyber Defence Smart Defence Projects' Conference** [Em linha]. 2015. [Consult. 05 dez. 2019]. Disponível em https://academiamilitar.pt/3rd-nato-cyber-defence-smart-defence-projects-conference.html

AED – **A Stock take of Capabilities for Cyber Defence in the military domain (milCyberCAP)** [Em linha]. Bruxelas: AED, 2011. [Consult. 15 jun. 2017]. Disponível em http://www.eda.europa.eu/procurement-gateway/opportunites/eda-procurement/procurement-view/11-cap-op-111---a-stock-take-of-capabilities-for-cyber-defence-in-the-military-domain-(milcybercap).

AFCEA – **Intelligence and the New National Security Environment** [Em linha]. Fairfax: AFCEA Intelligence Committee, 2004. [Consult. 18 jul. 2017]. Disponível em http://www.afcea.org/mission/intel/documents/innse.pdf.

AKHGAR, Babak; BREWSTER, Ben – **Combatting Cybercrime and Cyberterrorism**: Challenges, Trends and Priorities. Basileia: Springer, 2016. ISBN 978-3-319-38929-5.

Artigo de Opinião – **CiberSegurança e CiberDefesa, Direção-Geral de Política de Defesa Nacional (DGPDN)** [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em http://dgpdn.blogspot.com/2013/03/artigo-de-opiniao-ciberseguranca-e.html

Banco de Portugal. **Conversor de moeda do Banco de Portugal.** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.bportugal.pt/conversor-moeda?from=USD&to=EUR&date=1578787200&value=4250000000

BOROGAN, Irina; SOLDATOV, Andrewi. **"The Kremlin and the Hackers: Partners in Crime?"** [Em linha]. 2012. [Consult. 24 nov. 2019]. Disponível em https://www.opendemocracy.net/en/odr/kremlin-and-hackers-partners-in-crime/

BRODKIN, Jon. **Government-sponsored cyberattacks on the rise, McAfee says.** [Em linha]. 2007. [Consult. 24 nov. 2019]. Disponível em https://www.computerworld.com/article/2540217/government-sponsored-cyberattacks-on-the-rise--mcafee-says.html (tradução livre do autor).

BUDNICK, Kris – **Cyber Intelligence** [Em linha]. 2011. [Consult. 12 ago. 2017]. Disponível em https://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/Cyber_Intelligence.pdf.

C4ISR JOURNAL – **12th Annual Conference: Cyber Security, Stop Treating Cyber as Alien** [Em linha]. Arlington: C4ISR Journal, 2013. [Consult. 04 ago. 2017]. Disponível em http://c4isrjournal.com/blogs/insider/2013/04/25/experts-stop-treating-cyber-as-alien/.

CAVELTY, Myriam Dunn – **Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.** London: Routledge, 2008. ISBN 978-0415569880

CHOUCRI, Nazli – **Cyberpolitics in International Relations**. Massachusetts: Massachusetts Institute of Technology, MIT Press Ldt., 2012. ISBN 978-0-262-01763-3.

CIA The World Factbook – **Portugal** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/po.html

_____ – **Bélgica** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/be.html

_____ – **Dinamarca** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/da.html

_____ – **Holanda** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.cia.gov/library/publications/resources/the-world-factbook/geos/nl.html

CIBERSEGURANÇA – Nº 133, Lisboa: IDN, 2012. ISSN 0870-757X.

Cibersegurança e Políticas Públicas. Análise comparada dos casos chileno e português – Nº 29, Lisboa: IDN, 2018. ISBN: 978-972-27-1994-0

CISA. **2009 Cyberspace Policy Review** [Em linha]. 2009. [Consult. 15 dez. 2019]. Disponível em https://www.cisa.gov/publication/2009-cyberspace-policy-review.

CLARKE, Richard A.; KNAKE, Robert K. – **CyberWar**: **The Next Threat to National Security and What to Do About It.** Nova Iorque: HarperCollins Publishers, 2010. ISBN 978-0-06-196224-0.

COELHO, José – **O Ciberespaço na defesa coletiva e na gestão de crises: Articulação entre a Cibersegurança e a Ciberdefesa.** Lisboa: IESM, 2018. 105 f. Trabalho de Investigação Individual (CPOG)

COLLINS, S – **Stuxnet: Computer Worm opens new era of warfare** [Em linha]. 60 Minutes, CBSnewsonline, 2012. [Consult. 14 jun. 2017] Disponível em: http://www.youtube.com/watch?v=6WmaZYJwJng

Conceito Estratégico de Defesa Nacional [Em linha]. [Consult. 17 set. 2019]. Disponível em https://www.idn.gov.pt/conteudos/documentos/CEDN_2013.pdf

Contributos para uma estratégia Nacional de Ciberdefesa, Nº 28, Lisboa: IDN, 2018. ISBN 978-972-27-1994-0.

CORNISH, Paul; HUGHES, Rex; LIVINGSTONE, David – **Cyberspace and the National Security of the United Kingdom.** London. Chatham House, 2009. ISBN 978-1862032156

COSTA, José **– Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da Cibersegurança Nacional: A definição de responsabilidades e a coordenação com os diferentes atores.** Lisboa: IESM, 2017. 59 f. Trabalho de Investigação Individual (CPOS)

CROWELL, Richard M.; **Some Principles of Cyber Warfare: Using Corbett to Understand War in the Early Twenty–First Century.** Corbett Papers [Em linha]. Nº 19 (2017), p. 1-32. [Consult. 19 jun. 2017]. Disponível em https://www.kcl.ac.uk/sspp/departments/dsd/research/researchcentres/strategyandpolicy/corbett/publications/Corbett-Paper-No19.pdf.

CTSU Sociedade de Advogados SP, RL, S.A. – **Alerta Legal 70** [Em linha]. 2013. [Consult. 27 jul. 2017]. Disponível em https://www.ctsu.pt/ct/pt/pages/comunicacoes/articles/alerta-legal-70.html

DENNING, Dorothy E – **Activism, Hacktivism, and Cyberterrorism**: The Internet as a Tool for Influencing Foreign Policy [Em linha]. (10-12-99). [Consult. 04 ago. 2017]. Disponível em https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/.

Department of Computer Science. **McAfee Virtual Criminology Repo**rt [Em linha]. 2007. [Consult. 24 nov. 2019]. Disponível em http://www.cs.utsa.edu/~bylander/cs1023/mcafee_vcr_us.pdf

DEZABALA, Ted – **Getting Smart About Cyber Intelligence** [Em linha]. 2012. [Consult. 12 mai. 2017]. Disponível em http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Services/ERS/Security/uk-ers-getting-smart-about-cyber-intelligence.pdf.

DN – **NATO enfrenta 200 milhões de ciberataques por dia** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.dn.pt/mundo/nato-enfrenta-200-milhoes-de-ciberataques-por-dia-5438838.html

DOA – ATP2-22-9 – **Open Source Intelligence** [Em linha]. 2012. [Consult. 20 mai. 2017]. Disponível em http://www.fas.org/irp/doddir/army/atp2-22-9.pdf.

DOD – JP 2-01 – **Doctrine for Joint and National Intelligence Support to Military Operations** [Em linha]. 2012. [Consult. 19 ago. 2017]. Disponível em https://www.fas.org/irp/doddir/dod/jp2_01.pdf.

DOUTRINA Militar de Defesa Cibernética: MD31-M-07 [Em linha]. 2014 [Consult. 07 ago. 2017]. Disponível em http://defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

DRE – **Resolução do Conselho de Ministros nº5/90.** Instruções sobre a segurança informática (SEGNAC 4) [Em linha]. 1990. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa-avancada/-

/asearch/307435/details/maximized?perPage=100&anoDR=1990&types=SERIEI&search=Pesquisar

_____ – **Despacho n.º 13692/2013.** Orientação para a política de Ciberdefesa, [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/3295679/details/maximized?jp=true

_____ – **Lei n.º 31-A/2009**. Lei de Defesa Nacional. [Em linha]. 2009. [Consult. 15 mar. 2019]. Disponível em https://dre.pt/pesquisa/-/search/345292/details/maximized

_____ – **Lei n.º 46/2018.** Regime jurídico da segurança do ciberespaço [Em linha]. 2018. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/116029384/details/normal?l=1

_____ – **Lei nº 109/2009.** Cibercrime [Em linha]. 2009. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa/-/search/489693/details/maximized

_____ – **Lei Orgânica n.º 1-A/2009**. Lei Orgânica de Bases da Organização das Forças Armadas. [Em linha]. 2009. [Consult. 15 mar. 2019]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/345291/details/normal?l=1

_____ – **Resolução do Conselho de Ministros n.º 19/2013.** Conceito Estratégico de Defesa Nacional [Em linha]. 2013. [Consult. 05 dez. 2019]. Disponível em https://dre.pt/pesquisa/-/search/259967/details/maximized

_____ – **Resolução do Conselho de Ministros n.º 36/2015.** Estratégia Nacional de Segurança do Ciberespaço [Em linha]. 2015. [Consult. 19 set. 2019]. Disponível em https://dre.pt/home/-/dre/67468089/details/maximized?p_auth=pKf7McIZ.

_____ – **Resolução do Conselho de Ministros n.º 92/2019.** Estratégia Nacional de Segurança do Ciberespaço 2019-2023 [Em linha]. 2019. [Consult. 03 dez. 2019]. Disponível em https://dre.pt/web/guest/home/-/dre/122498962/details/maximized.

Economist. **War in the fifth domain** [Em linha]. 2010. [Consult. 22 dez. 2019]. Disponível em https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

Encyclopedia of the Nations – **Portugal** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Portugal.html

_____ – **Bélgica** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Belgium.html

_____ – **Dinamarca** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Denmark.html

_____ – **Holanda** [Em linha]. 2019. [Consult. 27 nov. 2019]. Disponível em https://www.nationsencyclopedia.com/Europe/Netherlands.html

Estratégia da Informação e Segurança no Ciberespaço. Nº 12, Lisboa: IDN, 2013. ISBN 978-972-27-2272-8.

EU-OTAN. **The EU and NATO The essential partners** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20and%20NATO.pdf

EUROPEAN COMMISSION [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/digital-single-market/en/desi

EUROSTAT – Science, technology and innovation – Overview. [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/web/science-technology-innovation

_____ **– Doctorate students in science and technology fields.** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00028/default/table?lang=en

_____ **– High-tech exports** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tin00140/default/table?lang=en

_____ **– High-tech patent applications to the European patent office (EPO) by priority year** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00010/default/table?lang=en

_____ **– Human resources in science and technology.** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00025/default/table?lang=en

_____ **– Research and development expenditure, by sectors of performance.** [Em linha]. [Consult. 22 set. 2019]. Disponível em https://ec.europa.eu/eurostat/databrowser/view/tsc00001/default/table?lang=en

Expresso. **NATO lança em Oeiras escola para ciberdefesa.** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://expresso.pt/politica/2017-05-23-NATO-lanca-em-Oeiras-escola-para-ciberdefesa

FERNANDES, José Pedro Teixeira**. A ciberguerra como nova dimensão dos conflitos do século XXI** [Em linha]. 2012. [Consult. 24 nov. 2019]. Disponível em http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri33/n33a05.pdf

FERNANDES, José Pedro Teixiera – Utopia, Liberdade e e Soberania no Ciberespaço. In Cibersegurança. **IDN - Nação e Defesa**. Lisboa. ISSN 0870-757X. Nº133, 5ª Série (2012), p. 11-31.

FRAGA, Luís Alves de – **Metodologia da Investigação.** Lisboa: Abdul's Angels, 2017. ISBN 978-972-89-7349-0.

Gabinete Nacional de Segurança. **RCM, nº 42/2012** – Comissão Instaladora do Centro Nacional de Cibersegurança [Em linha]. 2012. [Consult. 05 dez. 2019]. Disponível em https://www.gns.gov.pt/media/1924/rcm-42-2012.pdf

Global Firepower 2019 World Military Strength Rankings – **Portugal Military Strength** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível em https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=portugal

_____ – **Belgium Military Strength** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível em https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=belgium

_____ – **Comparison Results (Portugal vs Belgium)** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível https://www.globalfirepower.com/countries-comparison-detail.asp?form=form&country1=portugal&country2=belgium&Submit=COMPARE

_____ – **Comparison Results (Portugal vs Denmark)** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível https://www.globalfirepower.com/countries-comparison-detail.asp?form=form&country1=portugal&country2=denmark&Submit=COMPARE

_____ – **Comparison Results (Portugal vs Netherlands)** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível https://www.globalfirepower.com/countries-comparison-detail.asp?form=form&country1=portugal&country2=netherlands&Submit=COMPARE

_____ – **Denmark Military Strength** [Em linha]. 2019. [Consult. 17 dez. 2019]. Disponível em https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=denmark

_____ – **NATO Member States Military Strength (2020)** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível em https://www.globalfirepower.com/countries-listing-nato-members.asp

_____ – **Netherlands Military Strength** [Em linha]. 2019. [Consult. 15 dez. 2019]. Disponível em https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=netherlands

GOV.UK. **The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.** Introduction by the Rt Hon Francis Maude MP, Minister for the Cabinet Office [Em linha]. 2011. [Consult. 03 nov. 2019]. Disponível em https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Government of Georgia – **Cyber Security Strategy of Georgia 2012-2015** [Em linha]. 2012. [Consult. 27 nov. 2019]. Disponível em https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Georgia_2012_National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

GRAÇA, Pedro José Bentes – **O Ciberataque como Guerra de Guerrilha O Caso dos Ataques DoS/DDoS à Estónia, Geórgia e ao Google – China**. Lisboa: ISCSP – Universidade de Lisboa, 2013. 74 f. Dissertação de Mestrado em Estratégia

HOLLIS, David. **Cyberwar Case Study: Georgia 2008 [**EM LINHA]. 2011. [Consult. 24 nov. 2019]. Disponível em https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

HONORATO, Manuel; SANTOS, Luís, MATEUS, Regina – **O Ciberespaço como 5.º domínio operacional. Impacto estratégico na política de Defesa Nacional.** Lisboa: IESM, 2017. 46 f. Trabalho de Investigação de Grupo (CPOG). Área de Ensino de Estratégia

JOHN, Sian. Stuxnet worm hits Iran nuclear plant staff computers [Em linha]. 2010. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/news/world-middle-east-11414483

JUBILUT, Liliana Lyra. **Os Fundamentos do Direito Internacional Contemporâneo: da Coexistência aos Valores Compartilhados** [Em linha]. 2010. [Consult. 02 dez. 2019]. Disponível em http://centrodireitointernacional.com.br/static/anuario/5_V2/anuario_5_v2.pdf#page=203

KARNOUSKOS, Stamatis. **Stuxnet Worm Impact on Industrial Cyber-Physical System Security** [Em linha]. 2011. [Consult. 24 nov. 2019]. Disponível em https://ieeexplore.ieee.org/document/6120048

KENNEDY, John F. **– Presidential Library and Museum** [Em linha]. 1959. [Consult. 24 nov. 2019]. Disponível em https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/indianapolis-in-19590412

LANGNER, Ralph. **Stuxnet's Secret Twin** [Em linha]. 2013. [Consult. 24 nov. 2019]. Disponível em https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

MARQUES, António Gameiro. **O Poder da Informação no Poder Militar.** Revista Militar. Lisboa. Nº 2589 (outubro 2017) p. 775 [Em linha]. 2017. [Consult. 5 dez. 2019]. Disponível em https://www.revistamilitar.pt/artigo/1271

McGUINNESS, Damien. **Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país** [Em linha]. 2017. [Consult. 24 nov. 2019]. Disponível em https://www.bbc.com/mundo/noticias-39800133

MILITÃO, Octávio Pimenta – **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional.** Lisboa: FSCH – Universidade Nova de Lisboa, 2014. 97 f. Dissertação em Ciência Política e Relações Internacionais, especialização em Relações Internacionais.

NUNES, Paulo Fernando Viegas – Mundos Virtuais, Riscos Reais: Fundamentos para a definição da Estratégia da informação Nacional. **Revista Militar**. Lisboa: EUROPRESS, Editores e Distribuidores de Publicações Lda. ISSN: 0873-7630. N.º 2506 (novembro 2010), p. 1169 - 1198.

O Conceito Estratégico da NATO – Nº 126, Lisboa: IDN, 2010. ISSN 0870-757X.

OTAN – **Cybersecurity a Generic Reference Curriculum** [Em linha]. 2016. [Consult. 19 jul. 2017]. Disponível em http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf.

_____ – **5º artigo do Tratado do Atlântico Norte, Washington D.C.** [Em linha]. 1949. [Consult. 5 jun. 2019]. Disponível em https://www.nato.int/cps/su/natohq/official_texts_17120.htm?selectedLocale=pt

_____ – **Brussels Summit Declaration.** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_156624.htm

_____ – **Bucharest Summit Declaration.** [Em linha]. 2006. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natolive/official_texts_8443.htm

_____ – **Chicago Summit Declaration.** [Em linha]. 2012. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

_____ – **Cyber Defence Evolution.** [Em linha]. 2019. [Consult. 02 jan. 2020]. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.htm

_____ – **Cyber defence.** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.htm

_____ – **Defence Expenditure of NATO Countries (2009-2016)**. [Em linha]. 2017. [Consult. 13 set. 2019]. Disponível em https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_170313-pr2017-045.pdf

_____ – **Defence Expenditure of NATO Countries (2011-2018)** [Em linha]. 2019. [Consult. 13 set. 2019]. Disponível em

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_03/190314-pr2018-34-eng.pdf

_____ – **Lisbon Summit Declaration.** [Em linha]. 2010. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_68828.htm?selectedLocale=en

_____ – **NATO Cooperative Cyber Defence Centre of Excellence.** [Em linha]. 2008. [Consult. 05 dez. 2019]. Disponível em https://pt.qwe.wiki/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence

_____ – **NATO Defence Ministers adopt new cyber defence policy.** [Em linha]. 2011. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/news_75195.htm

_____ – **NATO opens new centre of excellence on cyber defence.** [Em linha]. 2008. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/news_7266.htm?selectedLocale=en

_____ – **NATO's role in cyberspace.** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/docu/reviwew/articles/2019/02/12/natos-role-in-cyberspace/index.html

_____ – **New NATO hub will gather the Alliance's cyber defenders.** [Em linha]. 2019. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natolive/news_163358.htm?selectedLocale=en

_____ – **Prague Summit Declaration.** [Em linha]. 2002. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_19552.htm

_____ – **Press conference by NATO Secretary General Jens Stoltenberg.** [Em linha]. 2016. [Consult. 19 set. 2019]. Disponível em http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

_____ – **Riga Summit Declaration.** [Em linha]. 2006. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en

_____ – **Wales Summit Declaration.** [Em linha]. 2014. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_112964.htm

_____ – **Warsaw Summit Communiqué.** [Em linha]. 2016. [Consult. 05 dez. 2019]. Disponível em https://www.nato.int/cps/en/natohq/official_texts_133169.htm

PINTO, Renato Fernando Marques – As indústrias militares e as armas de fogo portáteis no Exército Português. **Revista Militar** [Em linha]. Nº 2495 (2009), pp 1543-1634. [Consult. 15 set. 2019]. Disponível em https://www.revistamilitar.pt/artigo/528.

PINTO, Rui – **Novas fronteira criadas pelos ciberataques. Um novo desafio para a cooperação internacional.** Lisboa: IESM, 2013. 73 f. Trabalho de Investigação Individual (CPOG)

PORDATA – **Base de dados Portugal contemporâneo** [Em linha]. [Consult. 11 jan. 2020]. Disponível em https://www.pordata.pt/Europa/PIB+per+capita+(PPS)-1778

Progress Report. **Chancellor of the Duchy of Lancaster National Cyber Security Strategy 2016 – 2021** [Em linha]. 2019. [Consult. 22 dez. 2019]. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf.

RICHARDSON, John Charles – **Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield.** J. Marshall J. Computer & Info. [Em linha]. Vol.29 (2011), p. 2-4. [Consult. 08 set. 2019]. Disponível em https://repository.jmls.edu/cgi/viewcontent.cgi?article=1697&context=jitpl

Regime Jurídico da Segurança do Ciberespaço – **Lei n.º 46/2018** [Em linha]. 2013. [Consult. 27 jul. 2017]. Disponível em https://www.aguiarbranco.pt/noticias/regime-juridico-da-seguranca-do-ciberespaco-%E2%80%93-lei-n-462018-de-13-de-agosto/5

RID, Thomas – **Cyber War Will Not Take Place.** [Em linha]. Londres: Journal of Strategic Studies, 2011. [Consult. 19 jun. 2017]. Disponível em http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf.

SAALMAN, Lora – **Integrating Cybersecurity and Critical Infrastructure: National, Regional and International Approaches** [Em linha]. 2018. [Consult. 27 nov. 2019]. Disponível em https://www.sipri.org/publications/2018/other-publications/integrating-cybersecurity-and-critical-infrastructure-national-regional-and-international-approaches.

SANTOS, Lino; BRAVO, Rogério; NUNES, Paulo Viegas – **Protecção do Ciberespaço: Visão Analítica** [Em linha]. 2012. [Consult. 27 nov. 2019]. Disponível em https://comum.rcaap.pt/bitstream/10400.26/3578/1/Artigo_ENRSF_Revisto.pdf

SANTOS, Luís **– Contributos para uma estratégia Nacional de Ciberdefesa.** Lisboa: IESM, 2017. 108 f. Trabalho de Investigação Individual (CPOG)

Security Report. **OTAN terá centro de controle militar cibernético em plena operação até 2023** [Em linha]. 2018. [Consult. 3 jan. 2020]. Disponível em http://www.securityreport.com.br/overview/otan-tera-centro-de-controle-militar-cibernetico-em-plena-operacao-ate-2023/#.XiEREUf7QdV

SERRONHA, Marco Paulino – **A Cimeira de Lisboa: uma NATO para o século XXI** [Em linha]. 2010. [Consult. 28 ago. 2019]. Disponível em https://comum.rcaap.pt/bitstream/10400.26/3026/1/NeD126_MarcoPaulinoSerronha.pdf

SHAKARIAN, Paulo Cpt. **Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008** – MILITARY REVIEW [Em linha]. 2011. [Consult. 2 out. 2019]. Disponível em https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20111231_art011POR.pdf

Sítio da Defesa Nacional. [Em linha]. 2020. [Consult. 02 jan. 2020]. Disponível em https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa

SMITH, Dan – **Introduction: International stability and human security in 2017** [Em linha]. 2018. [Consult. 27 nov. 2019]. Disponível em https://www.sipri.org/yearbook/2018/01.

SPIGEL, Carla – **Securing Cyberespace: NATO'S Cyber Defence Policy as a Security Dispositive.** Utrecht: Universidade de Utrecht, 2017. 78 f. Dissertação de Mestrado

SWANSON, Lesley – **The Era of Cyber Warfare:** Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict [Em linha]. 2010. [Consult. 27 jul. 2017]. Disponível em http://digitalcommons.lmu.edu/ilr/vol32/iss2/5.

TALLINN Manual on the International Law Applicable to Cyber Warfare. NATO Cooperative Cyber Defense Centre of Excellence (CCD COE). Cambridge: Cambridge University Press, 2013. ISBN 978-1-107-61377-5.

The Military Balance 2019 – **Annual assessment of global military capabilities and defence economics.** The International Institute for Strategic Studies (IISS). Washington. ISSS, 2019. ISBN-13: 978-1857439885.

THE WHITE HOUSE – **NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-54 – Cybersecurity Policy** [Em linha]. 2008. [Consult. 3 jun. 2019]. Disponível em https://www2.epic.org/foia/odni/russian-hacking/EPIC-v-ODNI-EPIC-Reply-Exhibit.pdf

TIKK, Eneken – **Comprehensive Legal Approach to Cyber Security**. Estónia: Faculdade de Direito, Universidade de Tartu, 2011. 170 f. Tese de Doutoramento em Direito.

VALERIANO, Brandon. **Review Essay of Thomas Rid's Cyber War Will Not Take Place.** [Em linha]. 2013. [Consult. 02 dez. 2019]. Disponível em https://issforum.org/essays/17-cyber-war-will-not

VENÂNCIO, Pedro Dias – **Lei do Cibercrime – Anotada e Comentada**. Coimbra: Coimbra Editora, 2011. ISBN 978-9-723-21906-7.

VIHUL, Liis – **The Tallinn Manual on the International Law applicable to Cyber Warfare** [Em linha]. 2013. [Consult. 27 jul. 2017]. Disponível em https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/#more-7982.