ACADEMIA MILITAR

Ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias
Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2019

ACADEMIA MILITAR

Ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias

Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2019

EPÍGRAFE

"Threat is a mirror of security gaps. Cyber-threat is mainly the reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience"

Stephane Nappo

AGRADECIMENTOS

Esta investigação não teria seguimento não fosse a colaboração de diversas pessoas, a quem eu, desde já, demonstro o meu apreço e gratidão por toda a disponibilidade e ajuda que me prestaram.

Em primeiro lugar, gostaria de agradecer ao meu orientador, Major de Transmissões Luís Dias, pelo esforço, dedicação e acima de tudo paciência que demonstrou durante este período. Muito obrigado, meu Major.

Agradeço também ao meu coorientador, Major de Transmissões Tiago Guedes pela disponibilidade mostrada desde o primeiro dia em que o contactei, contribuindo com os seus conhecimentos técnicos relativos ao Sistema Automático de Comando e Controlo.

Agradeço aos oficiais que colaboraram, respondendo às minhas questões de carácter exploratório relativas ao Sistema Automático de Comando e Controlo que permitiram que chegasse a um estado de esclarecimento que não seria possível sem a sua ajuda. Desta forma agradeço ao Coronel Tirocinado de Transmissões Jorge Ribeiro, ao Major de Artilharia Alexis da Fonseca, ao Major de Artilharia Elton Feliciano e por fim ao Capitão de Artilharia João Chora por terem sido pacientes e me esclarecerem relativamente às questões.

Dirijo o meu profundo agradecimento ao Tenente-Coronel de Infantaria Lourenço Martins, por me elucidar e esclarecer as minhas dúvidas no que diz respeito à gestão da segurança da informação por parte das organizações de âmbito civil. Obrigado pela paciência e pela sua capacidade de simplificar esta matéria.

Por fim desejo agradecer a todos os camaradas, família e amigos por me terem acompanhado não só nesta investigação, mas também em todo o percurso na Academia Militar.

A todos, muito obrigado!

RESUMO

O presente trabalho de investigação incide sobre o tema "Ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha".

O principal objetivo deste trabalho é avaliar a ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha e propor medidas ou métodos que a elevem, recorrendo à análise das normas de segurança estabelecidas internacionalmente e à análise das boas práticas realizadas por outros países.

A investigação foi dividida em duas partes. A primeira parte teórica e a segunda prática. A abordagem ao tema foi materializada numa primeira fase, na análise documental de artigos, publicações internacionais de referência e publicações doutrinárias internacionais relativas à cibersegurança e ciber-resiliência necessária tanto nas Forças Armadas como em organizações civis. Numa fase seguinte foram realizadas entrevistas a quatro oficiais que mantiveram/mantêm contacto com o Sistema Automático de Comando e Controlo e uma entrevista a um oficial especialista na área da gestão da segurança da informação.

Os resultados obtidos permitiram concluir que o estado de ciber-resiliência do Sistema Automático de Comando e Controlo contém algumas lacunas. Também são sugeridas algumas medidas de forma a melhorar a ciber-resiliência do mesmo.

PALAVRAS-CHAVE: Comando e Controlo; Artilharia; Ciber-resiliência; Cibersegurança; Ciberdefesa

ABSTRACT

The present research focuses on the topic "Cyber-resilience of the Automatic Command and Control System of the Field Artillery".

The main objective of this work is to evaluate the cyber-resilience of the Automatic Command and Control System and to propose measures or methods that increase it, using the analysis of internationally established standards and the analysis of good practices carried out by other countries.

The investigation was divided into two parts. The first theoretical part and the second is practical. The approach, at an early stage, was materialized in documentary analysis of articles, international reference publications and international doctrinaire publications related to cybersecurity and cyber-resilience, necessary both in the Armed Forces and in civil organizations. In the following phase, interviews were conducted with four officers who maintained/maintain contact with the Automatic Command and Control System and an interview with a specialist officer in the area of information security management.

The results obtained allowed to conclude that the cyber-resilience state of the Automatic Command and Control System contains some gaps. Some actions are also suggested to improve cyber-resilience.

KEYWORDS: Command and Control; Artillery; Cyber-resillience; Cyber-security; Cyber-defence

ÍNDICE GERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

A

AC – Artilharia de Campanha

AFATDS – *Advanced Field Artillery Tactical Data System*

B

BCS – *Battery Computer System*

C

C2 – Comando e Controlo

C4I – Comando, Controlo, Computadores, Comunicações e Informações

CB – Campo de Batalha

COB – Centro de Operações da Bateria

D

DSB – *Defense Science Board*

E

EAF – Elemento de Apoio de Fogos

EID – Empresa de Investigação e Desenvolvimento de Eletrónica SA

F

FMS – *Foreign Military Sales*

FOS – *Forward Observer System*

G

GAC – Grupo de Artilharia de Campanha

GAC/BrigInt – Grupo de Artilharia de Campanha da Brigada de Intervenção

GAC/BrigMec – Grupo de Artilharia de Campanha da Brigada Mecanizada

GAC/BrigRR – Grupo de Artilharia de Campanha da Brigada de Reação Rápida

GDU-R – *Gun Display Unit – Replacement*

I

IPL – Instituto Politécnico de Leiria

IP – Internet Protocol

L

LAN – *Local Area Network*

LPM – Lei de Programação Militar

M

M3TR – Rádio Tático Multibanda, Multimodo e Multifunção

N

NATO – *North Atlantic Treaty Organization*

NIST – *National Institute of Standards and Technology*

O

OAF – Oficial de Apoio de Fogos

OAv – Observador Avançado

OTAN – Organização do Tratado do Atlântico Norte

P

PC – Posto de Comando

PCT – Posto Central de Tiro

R

RA4 – Regimento de Artilharia nº 4

RCFTIA – Relatório Cientifico Final do Trabalho de Investigação Aplicada

S

SACC – Sistema Automático de Comando e Controlo

U

UEB – Unidade de Escalão Batalhão

UDP – *User Datagram Protocol*

W

WAN – *Wide Area Network*

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA), subordinado ao tema "Ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha", insere-se no Mestrado Integrado em Ciências Militares, na especialidade de Artilharia da Academia Militar.

Cada vez mais a sociedade encontra-se dependente de sistemas informáticos[1] complexos e interconectados para conduzirem as suas vidas diárias. Desde as finanças pessoais à gestão das capacidades defensivas de uma Nação, passando pelo controlo de uma vasta rede de tráfego de aeronaves, os sistemas de informação digitais e os programas de computador tornaram-se integrados em praticamente todos os níveis das atividades. Embora se tenha verificado um enorme aumento na eficiência da prestação de serviços, esta evolução também está sujeita a um conjunto diversificado de ameaças oriundas de *hackers* nocivos, grupos criminosos e até órgãos de determinados governos. Estas ameaças, como negação de serviço, roubo de dados, modificação de dados, infeção de computadores através de vírus informáticos e muitas outras, têm sido mutáveis ao longo dos tempos e visam afetar várias funcionalidades informáticas.

Os alvos destes ataques divergem, podendo atingir indivíduos, organizações ou Estados. No que diz respeito ao campo de batalha, as ciberameaças[2] poderão, brevemente, ser um dos fatores decisivos para o resultado de uma guerra (Kott et al., 2015). Os sistemas de armas são cada vez mais complexos (como por exemplo: requisitos de performance, requisitos operacionais, manutenção), estão mais dependentes de fornecedores externos (aquisição) e são assentes em redes de computadores. No entanto, toda a conectividade e automação que possibilita grandes vantagens poderá ser também uma fraqueza a ser exploradas por forças opositoras (DSB, 2014). O atual secretário-geral da Organização das Nações Unidas, António Guterres, na ocasião do seu doutoramento honoris causa no

[1] **Sistema informático** – "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção"
in http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis.

[2] **Ciberameaça** – "Acção perpetrada através da Internet ou de outra rede de computadores com objectivo de intrusão ou acesso ilegal"
in Dicionário Priberam da Língua Portuguesa, 2008-2013,
https://dicionario.priberam.org/ciberamea%C3%A7a [consultado em 27-04-2019].

Instituto Superior Técnico fez notar "que a próxima guerra será precedida de um ciberataque"[3] o que vem realçar esta ideia.

O departamento da defesa americano, através do relatório (DSB, 2014) produzido pelo seu painel de ciência da defesa considera que os desafios de implementar uma ciberdefesa eficiente são apreciados tanto pelos seus líderes civis como pelos seus líderes militares, no entanto, o ambiente em constante evolução de ciberameaças e o aumento das vulnerabilidades do sistema representam um agravamento da situação e exigem uma abordagem de gestão de risco mais abrangente e proactiva. A gestão eficaz implica a avaliação dos pontos fortes e fracos relativos às capacidades Ciber bem como o progresso organizacional em direção à implementação da melhoria (DSB, 2014). Como é indicado pelo *United States Government Accountability Office* um ciberataque pode ter como alvo qualquer subsistema de armas que seja dependente em software, podendo levar ao não cumprimento de missões ou mesmo à perda de vidas (GAO, 2018).

Também o Mitre[4] considera que a ciber-resiliência é cada vez mais reconhecida como uma necessidade, tanto dos sistemas em geral como das missões em particular, à medida que aumenta a noção da existência de ciberameaças sofisticadas e em evolução (Bodeau & Graubart, 2017). Com a ciber-resiliência pretende-se que a gestão do risco de cibersegurança (falhas ou ataques informáticos), minimize ao máximo o impacto de um incidente informático, tendo sempre em consideração que eliminar o risco é impraticável porque impede a agilidade necessária (Bodeau, 2016).

Neste contexto o presente relatório tem como objetivo geral de investigação avaliar a ciber-resiliência do Sistema Automático de Comando e Controlo (C2) da Artilharia de Campanha, recorrendo à análise das normas de segurança e boas práticas estabelecidas internacionalmente. No primeiro capítulo, numa primeira fase, é feito um enquadramento teórico da investigação, explicando no que consiste o Sistema Automático de Comando e Controlo, quais os equipamentos que o constituem e como é que este é organizado e, numa segunda fase, são esclarecidos os conceitos relacionados com o ciberespaço, a forma como se insere no âmbito da NATO e no contexto nacional, é definido o conceito de ciber-resiliência e por fim é exposta a relação entre a ciber-resiliência e o ciber-risco. No segundo

[3] Fonte: https://www.dn.pt/portugal/interior/guterres-alerta-que-a-proxima-guerra-sera-precedida-de-um-ciberataque-9128969.html

[4] "*The Mitre Corporation*" é uma organização sem fins lucrativos que faz a gestão de centros de desenvolvimento e pesquisa financiados pelos Estados-Unidos que apoiam diversas agências governamentais americanas
in https://en.wikipedia.org/wiki/Mitre_Corporation

capítulo é mencionada a metodologia aplicada nesta investigação, fazendo referência aos métodos e materiais utilizados na mesma. O terceiro capítulo diz respeito à temática de ciber-resiliência em sistemas e redes, dividindo-se em diversas secções. Este capítulo pretende expor um modelo de ameaças aplicado ao SACC, referindo as vulnerabilidades a que este poderá estar sujeito e por fim sugerir formas de as mitigar. O quarto capítulo intitula-se "Ciber-resiliência em contexto empresarial". Este capítulo terá como objetivo principal explorar como é que a ciber-resiliência é gerida no contexto empresarial, tendo como foco relacionar as metodologias utilizadas nas empresas com o que é realizado no Sistema Automático de Comando e Controlo. Por fim, são apresentadas as conclusões relativas à análise dos resultados obtidos em geral, estabelecendo uma relação entre as questões inicialmente colocadas que levaram à realização desta investigação. Após a apresentação das limitações da investigação é exposta a bibliografia consultada que foi essencial à realização deste trabalho. Em apêndice encontram-se os guiões de entrevista que serviram de suporte às entrevistas realizadas no decorrer da investigação.

CAPÍTULO 1. ENQUADRAMENTO TEÓRICO

A evolução tecnológica a nível militar que se tem verificado nos últimos anos permitiu que surgissem novos materiais e equipamentos na Artilharia de Campanha (AC).

Assim, foi em 1996 que teve início o processo de aquisição dos equipamentos constituintes do atual Sistema Automático de Comando e Controlo (SACC) da AC, seguido de uma proposta do Exmo. General Espírito Santo, para que este complemento das Unidades de Artilharia, com programas da 2ª Lei de Programação Militar (LPM), fosse feito através de uma negociação Governo-a-Governo com os EUA, o processo *"Foreign Military Sales"*(FMS) (Simões & Dias, 2007). Em março de 2007, realizou-se a última fase do processo de aquisição do SACC.

De acordo com Feliciano (2015, p. 14) o "Sistema Automático de Comando e Controlo permite efetuar, de forma automática, o planeamento e coordenação de todos os meios de Apoio de Fogos, determinar o melhor meio de Apoio de Fogos e métodos de ataque para bater um determinado objetivo em função das orientações do Comandante, solicitar e controlar fogos de Artilharia de Campanha, de Morteiros[5], bem como pedidos de Apoio Aéreo (desde AIRMEDEVAC[6] ao CLOSE AIR SUPPORT[7])".

Para Oliveira (2014) o SACC permite primeiramente ao Comandante a integração do Comando, Controlo, Computadores, Comunicações e Informações (C4I), fornecendo-lhe oportunamente informação precisa, na qual se irá apoiar para tomar as suas decisões. A missão secundária do SACC, no entanto, é ser "interoperável com outras áreas funcionais do Campo de Batalha (CB), de modo a fornecer informação relativa ao Apoio de Fogos em apoio à missão da força, permitindo ao Comandante ter uma visão global, assegurando a troca de informação necessária entre os elementos de Estado-maior, no planeamento e condução de operações táticas, tendo ainda a capacidade de fornecer meios automatizados para a condução do treino individual e coletivo" (Oliveira, 2014).

Este capítulo divide-se em duas secções sendo a primeira secção destinada a definir os conceitos relativos ao Sistema Automático de Comando e Controlo e a segunda secção destinada a caracterizar os conceitos relativos ao ciberespaço e à ciber-resiliência.

[5] Esta capacidade não está disponível em Portugal, dado que não foram adquiridos computadores de tiro de morteiros compatíveis com o AFATDS.
[6] Na terminologia anglo-saxónica a Evacuação Sanitária efetuada por meios aéreos é designada por Air Medical Evacuation (AIRMEDEVAC) (PDE 4.0 Logística - p. 9-2).
[7] Apoio Aéreo Próximo.

1.1. SACC

O SACC apoia o Comandante na aplicação e integração de todo o Apoio de Fogos no CB, através do emprego de 4 equipamentos diferentes, entre os quais o *Advanced Field Artillery Tactical Data System* (AFATDS), o *Battery Computer System* (BCS), *Forward Observer System* (FOS) e por fim o *Gun Display Unit - Replacement* (GDU-R). Os três primeiros são ligados entre si por rádios GRC-525, fabricados na Empresa de Investigação e Desenvolvimento de Eletrónica SA (EID), em Portugal (Feliciano, 2015).

Uma vez que o GAC da Brigada Mecanizada (GAC/BrigMec) não recebeu rádios GRC-525, o SACC foi apenas utilizado esporadicamente, longe da sua máxima capacidade uma vez que foi utilizado somente através de meios filares (Oliveira, 2014). Apesar de algumas dificuldades técnicas, em 2012 utilizaram-se os rádios P/PRC-425 na ligação de todos os subsistemas do GAC/BrigMec desde o Observador Avançado (OAv) até à Secção (Oliveira, 2014).

No que diz respeito ao GAC da Brigada de Intervenção (GAC/BrigInt), o primeiro exercício de fogos reais com o SACC remonta a dezembro de 2007, sendo que, no entanto, todos os intervenientes do tiro de Artilharia de Campanha estavam ligados entre si por meio filar. Em dezembro de 2008 o SACC do GAC/BrigInt fica completo e "com vista à maximização da capacidade de efetuar comunicações digitais seguras…foi idealizada uma configuração de redes para o SACC que permitia que todas as comunicações do GAC fossem seguras", isto é, utilizando canais de comunicação digitais em substituição dos analógicos, "à exceção das comunicações do PCT/GAC para os PCT/Btr" uma vez que por razão de incompatibilidades dos sistemas não foi possível comunicar de forma digital entre o AFATDS e o BCS. No entanto, à semelhança do caso do GAC/BrigMec, foram detetados problemas de interoperabilidade entre os subsistemas que constituem o SACC e o rádio GRC-525, que " condicionaram a utilização de comunicações seguras e rápidas, bem como o número de redes internas de transmissão de dados do GAC" (Feliciano, 2013).

Numa tentativa de determinar as possibilidades de comunicação entre o rádio GRC-525 e os diferentes equipamentos norte americanos que constituem o SACC, foram realizadas experiências conjuntamente com elementos da Direção de Comunicações e Sistemas de Informação (DCSI) do Exército Português e da Empresa de Investigação e Desenvolvimento de Eletrónica SA até ao ano de 2011 (Feliciano, 2015). Destas experiências surgiu um impasse, não encontrando solução que permitisse a completa interoperabilidade entre os equipamentos do SACC "quando os investigadores envolvidos

esgotaram as hipóteses colocadas para as incompatibilidades entre o SACC e os rádios GRC-525" (Feliciano, 2015).

Em 2012 é submetida ao Centro de Investigação, Desenvolvimento e Inovação da Academia Militar (CINAMIL) a proposta do projeto de investigação COMSAF – Comunicações em Redes de Tiro sem Fios, que envolvia o RA4 e o Instituto Politécnico de Leiria (IPL) (Feliciano, 2015). Este projeto foi iniciado em 2014 e tinha como objetivo a criação de um dispositivo eletrónico que permitisse aos subsistemas do SACC comunicarem entre si através do rádio GRC-525 e o estudo de alternativas para a interligação dos subsistemas do SACC, nomeadamente através da utilização de interfaces Ethernet (Feliciano, 2015).

Para além dos problemas de interoperabilidade supracitados, também se verificou que os meios automáticos de comando e controlo adquiridos são "insuficientes face às necessidades de Comando e Controlo do Sistema de Apoio de Fogos em Portugal" (Feliciano, 2015) uma vez que os Oficiais de Ligação nos Elementos de Apoio de Fogos (EAF), os Pelotões de Morteiros Pesados e Médios das Unidades de Escalão Batalhão (UEB), os Centros de Operações das Baterias (COB), as Secções de Topografia dos GAC, a secção de Meteorologia, a Secção de Localização de Alvos Móveis (equipada com o radar RATAC-S) e o velocímetro AFAVR "não têm ligação de dados ao SACC, obrigando à comunicação por voz e à introdução manual de dados nos terminais SACC de destino" (Feliciano, 2015) . Por esta razão, surge também em 2012 uma proposta submetida pelo RA4 em parceria com o IPL de um projeto de investigação EMUL-BCS – Emulação do Sistema Computorizado da Bateria, procurando criar um software que funcione como interface entre os subsistemas do SACC e os periféricos que não têm comunicação automática com o SACC, nomeadamente a Estação Meteorológica Vaisala MW32, o velocímetro AFAMVR e o Radar de Localização de Alvos Móveis RATAC-S.

Atualmente esses projetos encontram-se estagnados, sendo que ainda não foi possível encontrar uma solução viável que resolva os problemas de interoperabilidade.

Nas próximas secções serão descritos os diferentes subsistemas do SACC.

1.1.1. *Advanced Field Artillery Tactical Data System*

O *Advanced Field Artillery Tactical Data System* (Figura 1) é um Sistema automático de comando e controlo utilizado ao nível dos Elementos de Apoio de Fogos (EAF) escalão Batalhão e Brigada e Posto de Comando (PC) /Posto Central de Tiro (PCT) do Grupo de Artilharia de Campanha (GAC). De acordo com Simões e Dias (2007) o AFATDS permite auxiliar o Comandante nas seguintes áreas:

- Planeamento do apoio de fogos;
- Execução do apoio de fogos;
- Controlo dos movimentos das unidades de AC;
- Apoio logístico à AC;
- Direção técnica e tática do tiro.

Figura 1 – Artillery Field Artillery Tactical Data System
Fonte: https://sill-www.army.mil/firesbulletin/

1.1.2. *Battery Computer System*

O *Battery Computer System* (Figura 2) é o sistema automático que funciona em rede e que se situa no PCT da Bateria. O BCS substitui o sistema manual de determinação de elementos de tiro como meio primário. Este opera como uma ponte entre o PCT da Bateria, o PCT do GAC, os OAv, os Oficiais de Apoio de Fogos (OAF) e as Bocas de Fogo (Ferreira, 2013).

Este equipamento permite automatizar os procedimentos a nível de PCT da Bateria uma vez que é capaz de auxiliar tanto na escolha do sistema de armas para bater cada objetivo (Direção Tática), como na determinação dos elementos de tiro (direção, elevação e graduação de espoleta) necessários ao eficaz cumprimento da missão (Ferreira, 2013).

Tem a capacidade de selecionar individualmente cada objetivo, registando os seus elementos topográficos e calcular os elementos de tiro individualmente para cada obus, tendo

em consideração a existência de regulações de precisão, velocidade inicial de cada obus e os meteogramas existentes.

Figura 2 – Battery Computer System
Fonte: (Ferreira, 2008, p. 2)

1.1.3. *Forward Observer System*

O FOS (Figura 3) é o subsistema utilizado ao nível das equipas de Observação Avançada. Este equipamento permite processar e armazenar dados de forma a auxiliar o apoio de fogos ao escalão Companhia (Simões & Dias, 2007). Este equipamento liga-se ao AFATDS e ao BCS através do rádio GRC-525 (Feliciano, 2013).

Figura 3 – Forward Observer System
Fonte:(Ferreira, 2008, p. 2)

1.1.4. *Gun Display Unit – Replacement*

O *Gun Display Unit - Replacement* (Figura 4) destina-se a equipar as secções da bateria de bocas-de-fogo permitindo que estas recebam elementos de tiro proveniente do BCS e que, durante uma missão de tiro, o comandante de secção possa informar o escalão superior relativamente ao estado da mesma. Uma vez que este equipamento é portátil, pequeno e leve, permite que seja transportado sem grande consumo de energia e que assegure uma rápida e eficaz transmissão dos dados entre o BCS e as secções, por meio filar.

Figura 4 – Gun Display Unit -Replacement
Fonte: (Ferreira, 2008, p. 2)

1.1.5. Rádio E/R P/PRC-525

O Rádio P/PRC-525, desenvolvido pela empresa portuguesa EID (Feliciano, 2015), é apresentado como uma mudança no campo de batalha digital uma vez que permite o máximo de flexibilidade em termos de bandas de frequências e funções.

Uma vez que é um rádio tático, este pode ser utilizado em aplicações portáteis, veiculares ou estacionárias. A versão *manpack* pode ser transportada por um combatente ou poderá ser instalada em modo veicular. Este Rádio cobre as bandas de HF, VHF e UHF[8] (EID, sem data).

A segurança das comunicações é outro ponto distintivo do PRC-525, ao dispor de encriptação do conteúdo da informação (COMSEC) e também de salto de frequência (TRANSEC), segundo algoritmos personalizados de acordo com o utilizador (EID, sem data).

[8] HF – *High Frequency*, VHF – *Very High Frequency*, UHF – Ultra High Frequency. (Variam de 1,5MHz até 512 MHz.

O P/PRC-525 é configurável e atualizável por software e firmware, suporta Internet Protocol (IP) over Air e permite a utilização de aplicações que utilizem protocolos de transporte *User Datagram Protocol* (UDP) e *Transmission Control Protocol* (TCP) através da rede rádio tática, assim como a integração com redes Internet Protocol. Possui um recetor GPS interno, que em conjunto com a sua capacidade *GPS Report*, contribui para *Common Operational Picture* (COP).

1.1.6. Arquitetura do SACC num Grupo de Artilharia de Campanha

A Figura 5 pretende representar uma possível arquitetura do SACC ao nível do GAC.

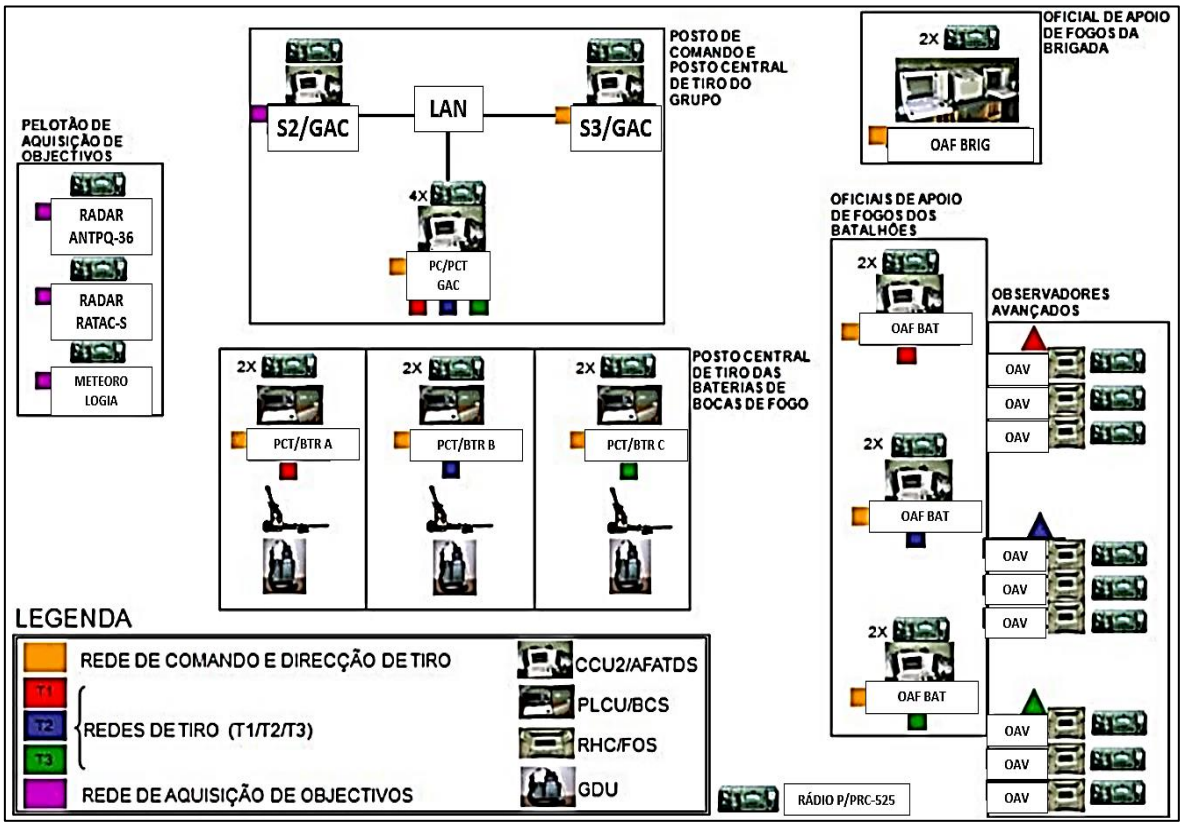

Figura 5 – Arquitetura do SACC num Grupo de Artilharia de Campanha
Fonte:(Escola Prática de Artilharia, 2006)

Como é possível verificar através da figura anterior, o SACC engloba 3 redes diferentes: Rede de Comando e Direção de Tiro que permite a comunicação entre o Oficial de Apoio de Fogos (OAF) da Brigada, os OAF dos Batalhões, o Oficial de Operações (S3) do GAC, o PC/PCT do GAC e os PCT das Baterias; Redes de Tiro que permitem a comunicação entre as bocas de fogo e os respetivos PCT da Bateria; Rede de Aquisição de Objetivos que permite a passagem de informação captada pelos radares RATAC-S e ANTPQ-36 e pela estação de Meteorologia Vaisala MW32 para o Oficial de Informações (S2) do GAC, através do rádio PRC-525 que equipa as secções radar e a secção de meteorologia. O S2 opera um AFATDS

que está em ligação com o AFATDS do Oficial de Operações (S3) e o AFATDS do PC/PCT do GAC, permitindo assim que estes possam utilizar os dados anteriormente referidos. Todas as transmissões presentes nestas redes, à exceção da comunicação realizada entre os AFATDS do S2, S3 e PC/PCT do GAC que são via LAN (uma vez que o PC/PCT do GAC se encontra numa infraestrutura mais fixa, ao escalão da Brigada), são realizadas via rádio PRC-525.

1.2. O Ciberespaço

Os domínios terrestre, marítimo, aéreo e espacial deixaram de ser, recentemente, os únicos domínios das operações militares. A NATO (Defesa Nacional, 2017) assim como o Instituto da Defesa Nacional (Santos, Nunes, Ralo, & Mendes, 2018) consideram determinante assumir o ciberespaço como um novo domínio operacional. O ciberespaço caracteriza-se como o domínio das operações militares mais recente e o mais diferente dos anteriores. Como sugere Gómez de Ágreda (2012), o ciberespaço não ocupa um espaço natural nem geográfico e é totalmente artificial, mas real, o que envolve maior vulnerabilidade uma vez que a estrutura que o sustenta é inerentemente mais débil e modificável.

A maioria das definições de ciberespaço estruturam-no em camadas, como sugere Bustelo (2017) (Figura 6):

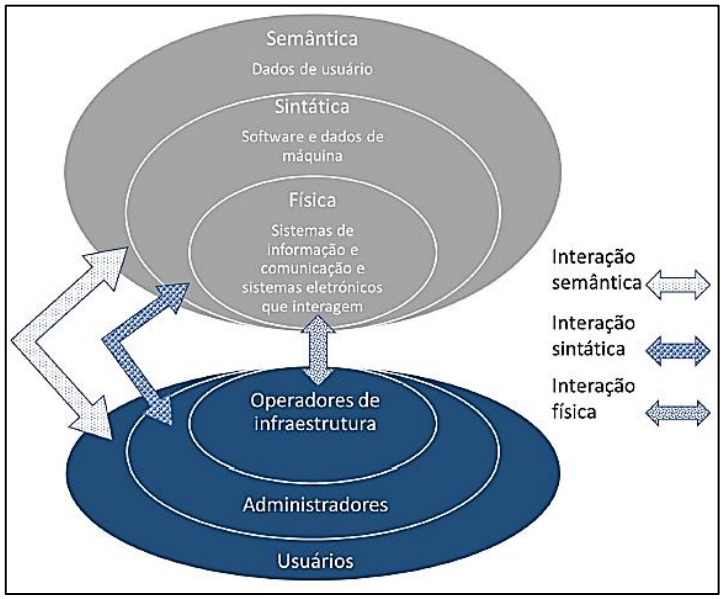

Figura 6 – Estrutura de camadas do ciberespaço e interação humana
Fonte: (Bustelo, 2017)

Para a Organização do Tratado do Atlântico Norte (OTAN), o ciberespaço corresponde ao domínio global que integra os sistemas de informação e de telecomunicações e outros sistemas eletrónicos, a sua interação e os dados que são armazenados, processados ou transmitidos por esses sistemas (NATO, 2014).

No Manual de Tallinn (CCDCOE, 2009) define-se ciberespaço como o "ambiente formado por componentes físicos e não físicos, caracterizado pelo uso de computadores e espectro eletromagnético, para armazenar, modificar e trocar dados usando rede de computadores".

Este novo domínio facilita, portanto, a troca de informações no campo de batalha como permite que exista uma maior eficiência dos exércitos no que diz respeito às operações militares. No entanto, como qualquer evolução, esta também traz novas vulnerabilidades que poderão influenciar negativamente no desenrolar de determinadas missões, caso estas não sejam previstas atempadamente, surgindo assim os conceitos de cibersegurança e de ciber-resiliência.

1.2.1. Cibersegurança na NATO

A cibersegurança visa garantir a confidencialidade, disponibilidade e integridade de informação digital guardada e/ou transmitida em qualquer formato dentro da redes internas e/ou na Internet (Babiceanu & Seker, 2019). De acordo com Paulo Moniz (2018) entende-se a cibersegurança "como o conjunto das atividades, que ocorrem no ciberespaço, de prevenção, monitorização e resposta às ameaças que, pela sua natureza disruptiva, coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadão ou organizações". No que diz respeito à ciberdefesa, "entende-se que esta inclui as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional, sendo que compete às Forças Armada assegurar a missão da ciberdefesa" (Santos et al., 2018, p. 23).

A NATO, embora sempre tenha protegido os seus sistemas de informação e comunicação, colocou a ciberdefesa pela primeira vez na agenda política da Aliança em 2002, em Praga. Em 2006, na Cimeira de Riga, os líderes aliados reiteraram a necessidade de reforçar a proteção dos sistemas de informação do ciberespaço (NATO, 2018).

Em abril e maio de 2007 ocorreram ataques cibernéticos na Estónia contra instituições públicas e privadas (NATO, 2011). Em consequência da urgência de reforçar a proteção nesta área, em janeiro de 2008 é aprovada a primeira Política de Ciberdefesa. No verão desse mesmo ano, o conflito entre a Rússia e a Geórgia vem demonstrar que os ataques

cibernéticos têm o potencial de se tornar um componente importante da guerra convencional (NATO, 2011).

É em 2010 que, na Cimeira de Lisboa, a NATO adota um novo Conceito Estratégico em que o *North Atlantic Council*[9] (NAC) fica encarregue de desenvolver uma política aprofundada de ciberdefesa da NATO e de preparar um plano de ação para a sua implementação (NATO, 2011).

Em junho de 2011 é aprovada a segunda Política da NATO sobre Ciberdefesa, que define uma visão para os esforços coordenados de ciberdefesa em toda a Aliança dentro do contexto de ameaça e tecnologia em rápida evolução e um plano de ação associado para a sua implementação (NATO, 2018).

Em abril de 2012, a ciberdefesa é introduzida no Processo de Planeamento da Defesa da NATO. Os requisitos relevantes de ciberdefesa são identificados e priorizados por meio do processo de planeamento de defesa (NATO, 2018). Na Cimeira de Chicago em maio de 2012, os líderes da Aliança reafirmaram o compromisso de melhorar a ciberdefesa, colocando todas as redes da NATO sob proteção centralizada e implementando uma série de atualizações para o *NATO Computer Incident Response Capability* (NCIRC) (NATO, 2018). Em julho de 2012, como parte da reforma das agências da NATO é estabelecida a *NATO Communications and Information Agency (*NCIA) (NATO, 2018).

Em fevereiro de 2014, os ministros da defesa aliados encarregam a NATO de desenvolver uma nova e melhorada política de ciberdefesa em relação à defesa coletiva, assistência aos Aliados, governança simplificada, considerações legais e relações com a indústria (NATO, 2018). Em maio de 2014, a capacidade operacional total do NCIRC é alcançada, proporcionando maior proteção às redes e utilizadores da NATO (NATO, 2018). Na Cimeira do País de Gales, em setembro de 2014, os Aliados apoiam uma nova política de ciberdefesa e aprovam um plano de ação que, juntamente com a política, contribui para o cumprimento dos principais objetivos da Aliança. A política e sua implementação estão sob revisão rigorosa nos níveis político e técnico da Aliança e são aprimoradas e atualizadas de acordo com a crescente ameaça no campo Ciber (NATO, 2018). Em 17 de setembro de 2014, a NATO lançou uma iniciativa para impulsionar a cooperação com o setor privado em ameaças e desafios informáticos. Aprovada pelos líderes aliados na Cimeira do País de Gales, a Cyber Partnership (NICP) da NATO foi apresentada numa conferência de dois dias realizada em Mons, Bélgica, onde 1.500 líderes do setor reuniram-se para discutir a

[9] *North Atlantic Council:* Conselho do Atlântico Norte – Principal órgão de decisão política da NATO.

colaboração no domínio ciber. O NICP reconhece a importância de trabalhar com parceiros da indústria para permitir que a Aliança atinja os objetivos da sua política de ciberdefesa (NATO, 2018).

No dia 10 de fevereiro de 2016, a NATO e a UE concluem um Acordo Técnico sobre Ciberdefesa para ajudar ambas as organizações a prevenir e responder melhor aos ciberataques. Este Acordo Técnico entre o NCIRC e a Equipa de Resposta a Emergências em Computadores da UE (CERT-EU) fornece uma estrutura para troca de informações e compartilhamento de melhores práticas entre equipas de resposta a emergências (NATO, 2018). Em 14 de junho de 2016, os ministros da Defesa concordaram em reconhecer o ciberespaço como um domínio na Cimeira de Varsóvia. Isto é um acréscimo aos domínios operacionais existentes de ar, mar e terra. Este reconhecimento não altera a missão ou mandato da NATO, que é defensivo. A Aliança também saudou os esforços realizados em outros fóruns internacionais para desenvolver normas de comportamento estatal responsável e medidas de fortalecimento da confiança para promover um ciberespaço mais transparente e estável para a comunidade internacional (NATO, 2018). Em 6 de dezembro de 2016, a NATO e a UE concordaram com uma série de mais de 40 medidas para avançar na maneira como as duas organizações trabalham juntas - incluindo combater ameaças híbridas[10], ciberdefesa e tornar o espaço comum a todos os países mais estável e seguro. Na ciberdefesa, a NATO e a UE fortalecem a sua participação mútua em exercícios e promovem a investigação, treino e partilha de informações (NATO, 2018).

No dia 16 de fevereiro de 2017, os ministros da Defesa aprovaram um Plano de Ação de Ciberdefesa atualizado, bem como um roteiro para implementar o ciberespaço como um domínio de operações (NATO, 2018). A NATO e a Finlândia intensificaram o seu compromisso com a assinatura de um Acordo-Quadro Político sobre cooperação em ciberdefesa. O acordo permitirá que a NATO e a Finlândia melhor protejam e melhorem a resiliência das suas redes (NATO, 2018). No dia 8 de novembro de 2017, os ministros da Defesa concordam relativamente à criação de um novo Centro de Operações do Ciberespaço como parte do projeto do esboço da Estrutura de Comando da NATO adaptada (NATO, 2018). Em 5 de dezembro de 2017, os ministros da NATO e da UE concordam em intensificar a cooperação entre as duas organizações em diversas áreas, incluindo a

[10] Ameaças híbridas - "*As ameaças híbridas poderão assim, neste quadro, abranger desde as campanhas mediáticas à utilização de armas químicas, biológicas, radiológicas e nucleares, passando por ciberataques contra os sistemas informáticos de infraestruturas estratégicas ou pela utilização de meios de subversão da paz social ou da ordem económica*." (Pereira, 2018, p. 11)

cibersegurança e defesa. A análise de ciberameaças e a colaboração entre equipas de resposta a incidentes é uma área de maior cooperação; outro é o intercâmbio de boas práticas sobre os aspetos do domínio ciber e as implicações da gestão de crises (NATO, 2018).

Na sequência do anúncio de 8 de novembro de 2017, os ministros da Defesa acordaram, em 14 de fevereiro de 2018, em criar o proposto Centro de Operações do Ciberespaço na Bélgica (NATO, 2018). Os líderes aliados concordam em criar um novo Centro de Operações do Ciberespaço como parte da Estrutura de Comando fortalecida da NATO. O Centro proporcionará consciência situacional e coordenação da atividade operacional da NATO no ciberespaço. Os aliados também concordam que a NATO pode aproveitar as capacidades ciber nacionais para as suas missões e operações. Por fim, os Aliados fazem um balanço de seu progresso para melhorar a resiliência nacional através do *Cyber Defense Pledge* (NATO, 2018).

1.2.2. Enquadramento da ciberdefesa no contexto Nacional

O caderno do Instituto da Defesa Nacional de 2018 intitulado de "Contributos para uma Estratégia Nacional de Ciberdefesa" contempla o enquadramento da ciberdefesa no contexto Nacional. Tendo como exemplos os casos da Geórgia e Ucrânia, onde existiu uma extensiva utilização do ciberespaço para a condução de ciberataques sendo o ciberespaço um vetor privilegiado para ações de propaganda e recrutamento. Pode-se verificar que a guerra híbrida encontrou no domínio ciber um "instrumento de ação de elevado potencial em função do custo reduzido, rapidez de atuação, sensação de anonimato e leque crescente de possíveis alvos com potencial impacto no domínio cibernético" (Santos et al., 2018, p. 33). A utilização do ciberespaço num contexto de ameaça híbrida é então perspetivada de duas formas sendo que a primeira é focada no domínio mediático de comunicação (Santos et al., 2018), e a segunda focada no domínio operacional utilizado para o combate, de modo a "complementar ou amplificar os efeitos das operações militares convencionais"(Santos et al., 2018, p. 33). Com este segundo enquadramento "importa ajustar as capacidades militares a esta nova realidade operacional, nomeadamente, dotando as Forças Armadas de mecanismos de adaptação à guerra híbrida nas suas diversas variantes, dando prioridade à melhoria do conhecimento situacional e privilegiando as áreas de prevenção e dissuasão" (Santos et al., 2018, p. 33).

1.2.3. O conceito de Ciber-resiliência

A ciber-resiliência deve ser considerada no contexto de sistemas complexos que compreendem não só os domínios físicos e da informação, mas também os domínios cognitivos e sociais (Smith, 2005). A ciber-resiliência assegura a recuperação de um sistema considerando os componentes *hardware*, *software*, e sensores que se encontram interconectados na ciber infraestrutura, como sugere a Figura 7 (Linkov & Kott, 2019). Ou seja, ciber-resiliência constitui-se como a ponte entre a sustentação das operações e o cumprimento da missão. Um sistema resiliente por sua vez é aquele que continua a oferecer um nível de desempenho aceitável mesmo quando se encontra atacado, independentemente do tipo de ataque (Hutchison & Sterbenz, 2018).

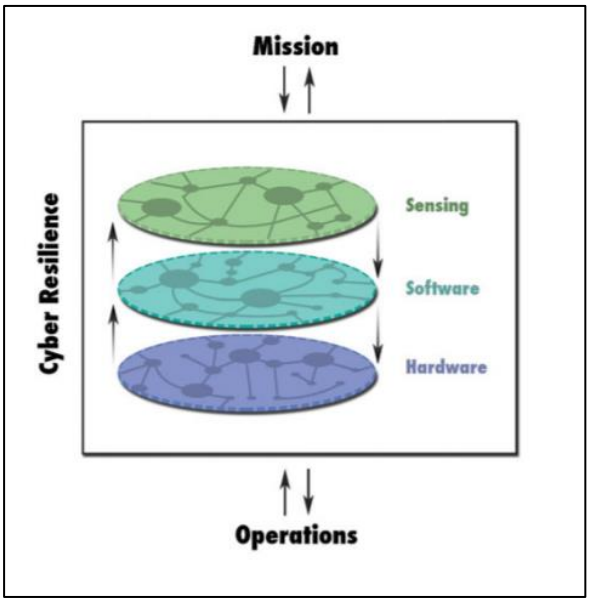

Figura 7 – Os domínios da ciber-resiliência e o seu contributo na sustentação das operações
Fonte:(Linkov & Kott, 2019)

As raízes do conceito resiliência encontram-se em diversas áreas e integram perspetivas e definições desde o domínio ecológico, social, psicológico, organizacional até às perspetivas e definições do domínio das engenharias (Florin & Linkov, 2016). A engenharia da resiliência, por exemplo, foi definida como a capacidade que os sistemas têm de antecipar e de se adaptar a uma potencial surpresa e fracasso e tem vindo a ser associada à mudança do paradigma de segurança reconhecendo que a reação do sistema é importante, uma vez que a prevenção total é utópica (Linkov & Kott, 2019). Por sua vez, a resiliência ecológica refere-se à capacidade de um sistema absorver e suportar choques, com um enfâse na persistência (Holling, 1996). Segundo Linkov e Kott (2019), a resiliência é, por vezes, usada como uma metáfora para descrever a forma como os sistemas reagem aos stresses mas que,

no entanto, a resiliência deve ser discutida de uma forma menos abrangente, separando a metáfora da ciência.

De acordo com a Academia Nacional de Ciências dos Estados Unidos resiliência define-se como a capacidade de preparar e planear para, absorver, recuperar de e ser o mais bem-sucedido possível na adaptação a eventos adversos e esta definição está a emergir como a mais usada por diversas organizações e agências governamentais (Larkin et al., 2015).

Para Ross (2018) ciber-resiliência define-se como a capacidade de antecipar, enfrentar, recuperar e por fim adaptar a condições adversas, *stresses*, ataques ou comprometimentos em sistemas que usam ou que são suportados por sistemas informáticos.

A ciber-resiliência acaba por se referir, de uma forma semelhante aos outros campos, à capacidade de um sistema recuperar ou regenerar a sua performance após um ciberataque que produza degradação no seu desempenho (Figura 8). Assumindo que dois sistemas que têm um desempenho igual, A e B, são submetidos a um impacto, resultante de um ciberataque, que leva a uma degradação equivalente do seu desempenho, a ciber-resiliência do sistema A será maior se após um determinado espaço de tempo T recuperar para um nível superior que o sistema B (Linkov & Kott, 2019).

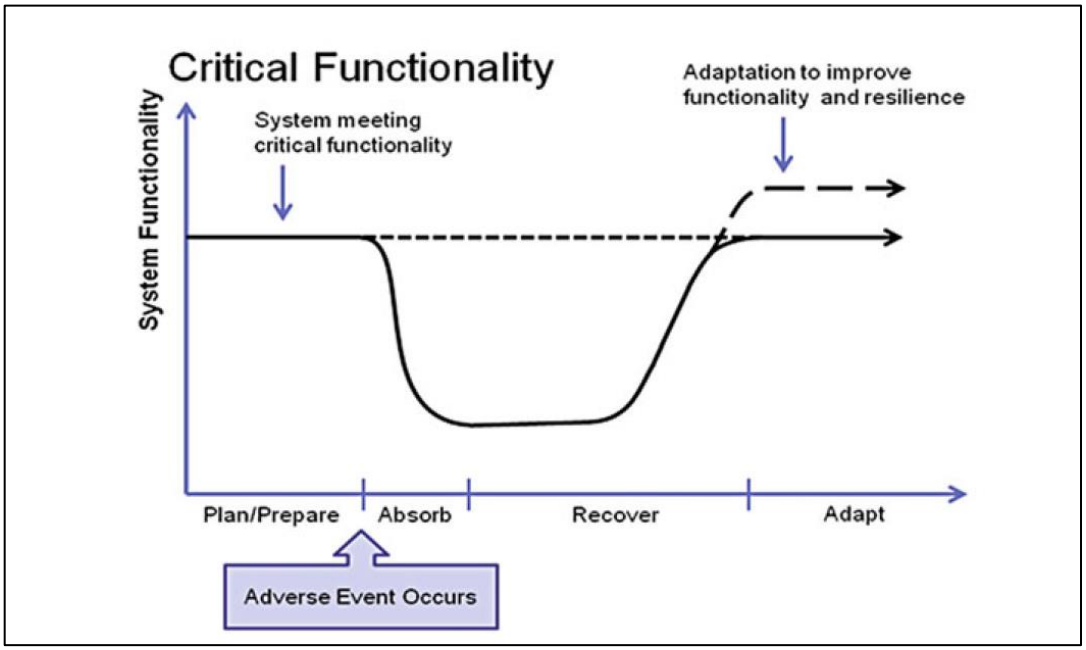

Figura 8 – Perfil de resiliência, traçando a funcionalidade crítica de um sistema ao longo do tempo
Fonte: Linkov & Kott, 2019

1.2.4. Ciber-resiliência e o ciber-risco

Risco, segundo a definição do dicionário de Oxford, refere-se a uma situação envolvendo a exposição a um perigo ou ameaça. Segundo Linkov e Kott (2019) se o risco for gerido de uma forma apropriada, o sistema alcança um estado de segurança, isto é, um estado livre de perigo ou de ameaça, ou então um estado de robustez, ou seja, tolerantes e com capacidade para fazer frente ou ultrapassar condições adversas ou testes rigorosos. Os termos segurança, robustez e risco estão interligados uma vez que estes estão focados na prevenção e na capacidade um sistema manter-se funcional com níveis aceitáveis tanto antes como após ocorrências adversas.

A ciber-resiliência difere destes conceitos uma vez que parte da premissa que o sistema é afetado e a sua funcionalidade degradada, com enfoque na velocidade de recuperação do mesmo.

Linkov e Kott (2019) definem o ciber-risco como a probabilidade que uma ocorrência não desejada aconteça juntamente com os resultados que o impacto da ocorrência implicam.

CAPÍTULO 2. METODOLOGIA

Para que uma investigação seja realizada de forma credível e com elevado grau de aceitação, esta deve assentar num método de investigação robusto, para que as questões elencadas sejam respondidas de forma estruturada.

Para Manuela Sarmento (2013), o método científico é fruto da integração de procedimentos e normas que irão resultar numa produção de conhecimento que, por sua vez, poderá ser completamente novo ou desenvolvimento, reunião ou o melhoramento de vários conhecimentos já existentes.

No que diz respeito a este trabalho de investigação o mesmo é normalizado pelas Normas de Execução Permanente Nº520/4ª e 522/1ª da Academia Militar que estabelece normas e procedimentos relativos aos Relatórios Científicos do Trabalhos de Investigação Aplicada.

O presente relatório tem como objetivo geral de investigação avaliar a ciber-resiliência do Sistema Automático de Comando e Controlo (C2) da Artilharia de Campanha, recorrendo à análise das normas de segurança e boas práticas estabelecidas internacionalmente. Sendo assim, esta investigação foi dividida em diversos objetivos específicos que contribuem para o objetivo geral, sendo estes:

- Caracterizar os sistemas de comando e controlo da Artilharia de Campanha;
- Relacionar os conceitos de ciber-resiliência e Gestão do Risco;
- Analisar as possíveis Ameaças ao Sistema Automático de Comando e Controlo no Campo de Batalha;
- Analisar as medidas de segurança no domínio “ciber”, presentes nos sistemas de comando e controlo de Artilharia de Campanha;
- Identificar e descrever as diversas normas, recomendações e procedimentos que caracterizam um sistema ciber-resiliente;
- Caracterizar as medidas necessárias à implementação de uma organização ciber-resiliente;
- Sugerir soluções para a mitigação dos problemas encontrados.

Consequentemente, através do objetivo geral enunciado anteriormente, considera-se fundamental responder à seguinte Questão Central: "Qual é o estado atual da ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha Portuguesa?". Neste sentido, para se responder à Questão Central foram levantadas as seguintes questões derivadas:

1- Como se caracteriza o Sistema Automático de Comando e Controlo da Artilharia de Campanha?
2- Qual a relação existente entre a ciber-resiliência e a gestão de risco?
3- Quais são as ameaças que o Sistema Automático de Comando e Controlo poderá enfrentar?
4- De que forma é que é possível mitigar as vulnerabilidades do Sistema Automático de Comando e Controlo?
5- Quais são as normas internacionais que deverão ser respeitadas para que um sistema seja considerado ciber-resiliente?
6- Como é que as organizações de âmbito civil gerem a sua capacidade de serem ciber-resilientes?

Com esta investigação pretende-se estudar a ciber-resiliência existente nos sistemas de C2 da Artilharia Portuguesa, aprofundando o estudo nos sistemas de C2 da Artilharia de Campanha.

Para consolidar esta investigação, a revisão bibliográfica foi um ponto central, através da análise dos mais recentes relatórios de segurança, *frameworks* sugeridas pela União Europeia e por organizações especializadas em cibersegurança, revistas e boletins de Artilharia, sendo que também foram realizadas entrevistas de carácter exploratório a diversos Oficiais do Exército que mantém/mantiveram contacto com o Sistema Automático de Comando e Controlo ou com a temática de cibersegurança.

CAPÍTULO 3. CIBER-RESILIÊNCIA EM SISTEMAS E REDES

A mudança para um paradigma completo de informação centralizada no campo de batalha tem permitido que grande parte das operações sejam possíveis ser desenvolvidas e suportadas em sistemas de comunicações em rede modernos (Kurdziel, 2014). Manter estas Redes Táticas seguras sem diminuir o seu desempenho tem sido um desafio. É necessário examinar as Redes e construir um modelo de ameaças e uma base de requisitos de cibersegurança necessários para Redes Táticas assentes em infraestruturas fixa ou móveis e/ou redes ad hoc (redes destinadas a uma determinada finalidade) (Kurdziel, 2014).

No presente capítulo será apresentado o modelo de ameaça aplicado ao SACC, de forma a verificar quais as vulnerabilidades a que este poderá estar sujeito e de que forma é que se pode mitigar as mesmas.

3.1. Modelos de Ameaça

De acordo com Kurdziel (2014), um modelo de ameaça pode ser focado no atacante, na arquitetura do sistema ou nas capacidades do sistema.

Um modelo de ameaça focado no atacante utiliza uma caracterização de potenciais adversários e, a partir daí, identificar as vulnerabilidades e potenciais modos de ataque subsequentes. A principal chave para este tipo de modelo de ameaça é a avaliação das capacidades do adversário, seus recursos e as motivações que poderão ser aplicadas para explorar uma determinada vulnerabilidade. Esta avaliação irá conduzir à identificação de quais as vulnerabilidades do sistema que poderão ser consideradas como ameaças reais. Também irá conduzir à priorização da lista de ameaças final e será o fator primário no desenvolvimento ou procura de soluções de mitigação apropriadas. Este método também permite avaliar o custo dos ataques e interrogar se, sendo assim, valerá a pena mitigar determinado tipo de vulnerabilidade. Isto é, de acordo com as limitações do adversário, se o custo computacional para este efetivar um ataque é inviável, pode-se concluir que essa vulnerabilidade não vale a pena ser mitigada.

Um modelo de ameaça focado na arquitetura do sistema examina os seus componentes para identificar as vulnerabilidades e os potenciais ataques a esses componentes. A análise inicia-se com a decomposição hierárquica do sistema nos componentes de segurança relevantes (Kurdziel, 2014). Esta decomposição poderá ser de *hardware* (componentes físicos), *software* (suporte lógico) ou funcional, dependendo das

características do sistema a analisar. O objetivo deste método é agrupar as vulnerabilidades dos componentes em classes com métodos de mitigação comuns. Assim que as vulnerabilidades sejam identificadas e categorizadas realizam-se testes de penetração, isto é, é examinada a sequência de eventos que seriam necessários para explorar uma determinada vulnerabilidade, normalmente através de árvores de ataque ou de ameaça. Os resultados desta análise são usados para determinar que vulnerabilidades transmitem maior risco e permitem que estas ameaças sejam priorizadas. Após este passo, o desenvolvimento do método de mitigação poderá ser planeado apropriadamente.

Para Kurdziel (2014), um modelo de ameaça focado nos ativos do sistema examina ativos específicos ou fontes consideradas fidedignas, ou seja, procura aumentar a segurança de um sistema e mitigar as ameaças através da implementação de mecanismos de proteção do alvo. Este tipo de processo é usado conjuntamente com uma análise ampla do sistema para identificar mecanismos de proteção para alvos com alta prioridade. Por exemplo, os dados sensíveis que são transmitidos sem fios estarão acessíveis diretamente pelo adversário e correm o risco de serem manipulados ou intercetados. A autenticação da fonte e a verificação de integridade dos dados poderão ser medidas aplicadas para defesa contra ataques de *spoofing*[11] *e* mecanismos de encriptação também poderão ser aplicados para promover a confidencialidade dos dados.

3.2. Modelo de Ameaças focado nas Redes Táticas Militares

Segundo Kurdziel (2014) a modelação de ameaças de Redes Táticas Militares tem desafios adicionais, uma vez que o adversário terá ao seu alcance capacidades avançadas no que diz respeito a ciberataques, mais recursos e objetivos mais agressivos. Para além disso, no teatro de operações o adversário poderá ter acesso completo ao espetro eletromagnético. Nesta modelação é importante prever as ameaças futuras, estar ciente de possíveis ataques de negação de serviço e, não menos importante, garantir que a missão é terminada considerando a restauração dos serviços do sistema caso este seja alvo de um ataque bem-sucedido. Posto isto, considera-se pertinente criar uma estratégia defensiva utilizando um processo construído com elementos de cada tipo de modelo de ataque.

[11] **Spoofing** – Prática fraudulenta ou maliciosa em que uma comunicação é enviada de uma fonte desconhecida disfarçada de uma fonte conhecida pelo recetor.
Traduzido de https://www.techopedia.com/definition/5398/spoofing.

Assim, para analisar os desafios que o Sistema Automático de Comando e Controlo poderá enfrentar no Campo de Batalha, iremos utilizar a metodologia de modelação de ameaças sugerida na Figura 9.

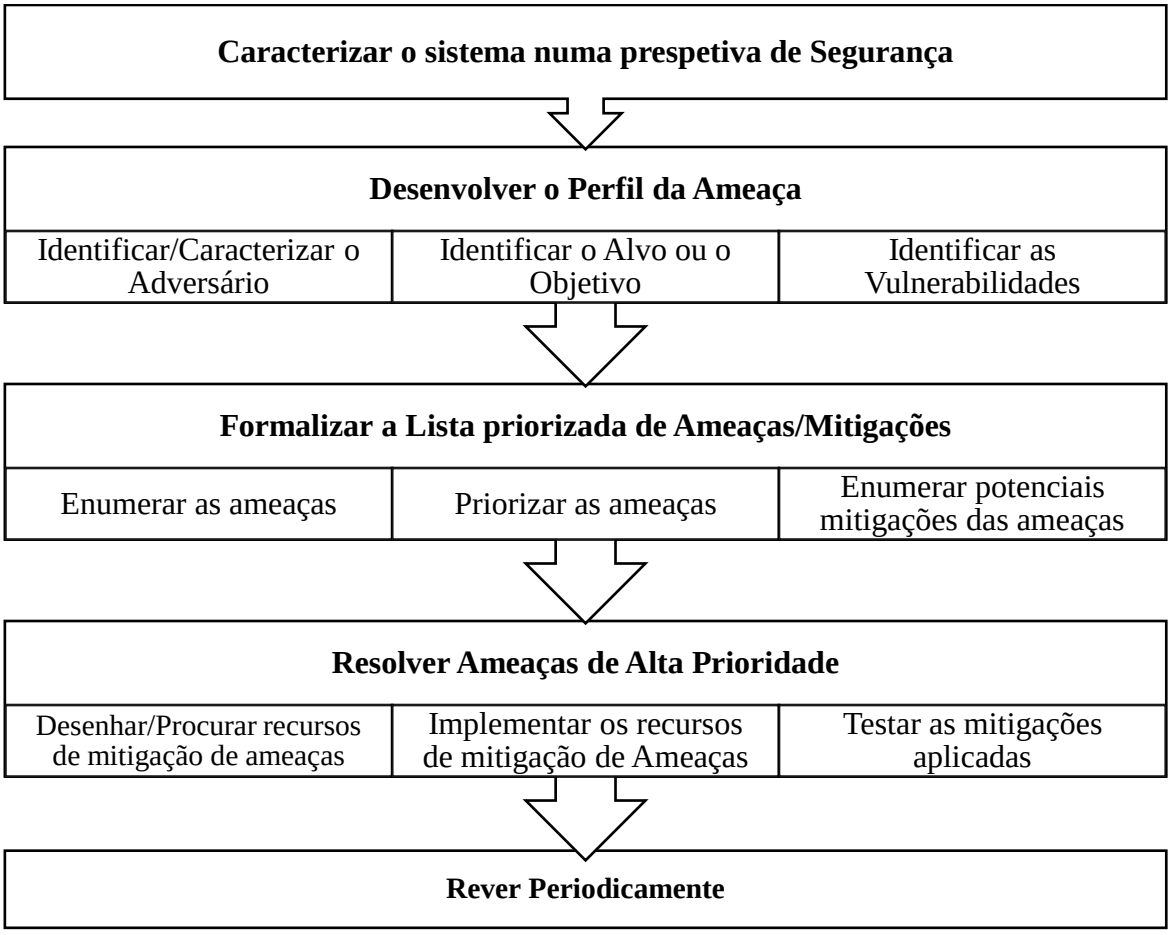

Figura 9 – Fluxo do processo do modelo de ameaça a uma rede Tática

(Adaptado de Kurdzier, 2014)

3.2.1. Caracterizar o sistema numa perspetiva de Segurança

O primeiro ponto deste processo inicia-se com a caracterização do sistema num ponto de vista de segurança.

A arquitetura de um sistema são os conceitos fundamentais ou as propriedades de um sistema no seu ambiente operacional e que inclui os seus elementos, relações e consiste também nos princípios do seu *design* e de evolução (Ross et al., 2016).

A arquitetura da segurança de um sistema mostra como é que as funções de segurança estão atribuídas nos elementos do sistema (permitindo que estes elementos sejam confiáveis); nas conexões e nos fluxos de informação que as ligações confiáveis permitem e como é que os sistemas de confiança combinam e interagem entre si e com as outras partes

do sistema de forma a que seja permitida uma capacidade de proteção específica (Ross et al., 2016).

Os recursos do sistema deverão ser identificados claramente. Por recursos do sistema, entende-se qualquer recurso que seja de valor para o adversário e para utilizadores autorizados. O propósito da segurança do sistema é proteger estes recursos. Em seguida deverá ser criada a arquitetura do sistema, que poderá ser em diagrama com texto especificando os propósitos do sistema, casos de utilização primária, ambiente em que opera e identificação dos utilizadores tipo. Por fim deverá ser realizada uma decomposição do sistema, de forma hierárquica em que primeiro o sistema deverá ser fragmentado em subsistemas relevantes relativos à segurança até ao nível de configuração de cada componente. Os pontos de entrada, a infraestrutura e os fluxos de dados deverão ser indicados e discutidos. A caracterização do sistema deverá ser detalhada o suficiente para permitir o desenvolvimento do perfil de ameaça do sistema (Kurdziel, 2014).

3.2.2. Desenvolver o perfil da ameaça

O perfil da ameaça deverá iniciar-se com a análise e caracterização do adversário (Kurdziel, 2014), sendo que esta análise deverá incluir níveis estimados de conhecimentos, capacidades financeiras, capacidade de acesso ao sistema e aos dados e recursos computacionais que o adversário poderá ter. Uma vez que dados específicos, precisos e verificáveis relativos ao adversário são difíceis de obter (Kurdziel, 2014), as suposições a fazer devem ter um carácter conservador.

De seguida, deverão ser examinados os objetivos e motivação do adversário. A previsão dos tipos de ataque que podem ser esperados poderá ser encontrada através do conhecimento dos objetivos do adversário e do valor que este poderá retirar após atingir determinado objetivo. Se o objetivo do adversário tiver um fim monetário, os ataques que tiverem um custo mais baixo serão enfatizados. Se os objetivos do adversário forem relacionados com tempo, como por exemplo o desejo de recolher informações sobre eventuais ataques que poderão ocorrer a determinada hora, também nos indica que tipo de ataques é que precisam de ser mitigados. No entanto, o objetivo do adversário poderá não se limitar a adquirir informações, mas também interromper ou reduzir a capacidade de transmissão das mesmas, através de ataques de Negação de Serviço, por exemplo.

Kurdziel considera que o sistema, na última etapa desta fase, deverá ser examinado para que potenciais vulnerabilidades sejam identificadas, uma vez que o adversário irá realizar o mesmo tipo de análise a focar os seus ataques nos componentes menos protegidos

do sistema. Este passo no processo inicia-se com a decomposição do sistema até ao nível dos seus componentes. Nesta fase, a ferramenta de modelação *"STRIDE per element"* é aplicada a cada componente. O objetivo do STRIDE é examinar as possíveis vulnerabilidades de cada componente em 6 categorias de ataque, sendo estas *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service* e *Elevation of Privilege.* Esta ferramenta irá modelar então a segurança do sistema no contexto do Sistema Automático de Comando e Controlo da Artilharia de Campanha. Assim que as vulnerabilidades são identificadas, as contramedidas apropriadas poderão ser implementadas.

Tabela 1 – Adaptação do resumo da metodologia "STRIDE por elemento" de Kurdziel

	Ameaça	Definição	Propriedade afetada	Contramedidas Padrão
S	*Spoofing Identity* – Falsificação da Identidade	O adversário imita um utilizador autorizado para alcançar um objetivo	Autenticação	• IPSec/HAIPE • Assinaturas Digitais • Códigos de autenticação por mensagem • Encriptação
T	*Tampering with Data* – Adulteração de Dados	O adversário manipula os dados para alcançar determinado objetivo	Integridade	• Encriptação • Listas de Controlo de Acessos • Assinaturas Digitais • Códigos de Autenticação por Mensagem
R	*Repudiation*	Repúdio	Não-repúdio	• Autenticação Forte • Assinatura Digital • Início de sessão seguro e monitorização
I	*Information Disclosure* – Divulgação de Informação	O adversário obtém informação de forma ilegítima	Confidencialidade	• Encriptação • Listas de Controlo de Acessos
D	*Denial of Service* – Negação de Serviço	O adversário procura perturbar o normal funcionamento do sistema	Disponibilidade	• Lista de Controlo de Acessos • Limitação de Espaço • *Design's* de grande disponibilidade
E	*Elevation of Privilege* – Elevação de Privilégios	O adversário tenta elevar os seus privilégios dentro do sistema.	Autorização	• Associação dos membros por grupos ou funções • Validação de entrada • Princípio do mínimo privilégio

3.2.3. Formalizar a Lista Priorizada de Ameaças

A mitigação de todas as vulnerabilidades é utópica em termos tecnológicos, práticos e monetários. Uma estratégia para gerir o risco é identificar os componentes críticos de um sistema que poderão sofrer falhas e, subsequentemente, fortalece-los (Linkov & Kott, 2019).

Os gráficos apresentados na Figura 10 e 11 representam o custo de diminuir o risco em sistemas ciber e a evolução da complexidade dos *softwares* no que diz respeito ao seu código-fonte. Como é possível verificar, a complexidade dos programas e componentes atuais faz com que seja difícil, se não mesmo impossível desenvolver componentes sem falhas ou detetar inserções malignas no código (DSB, 2014).

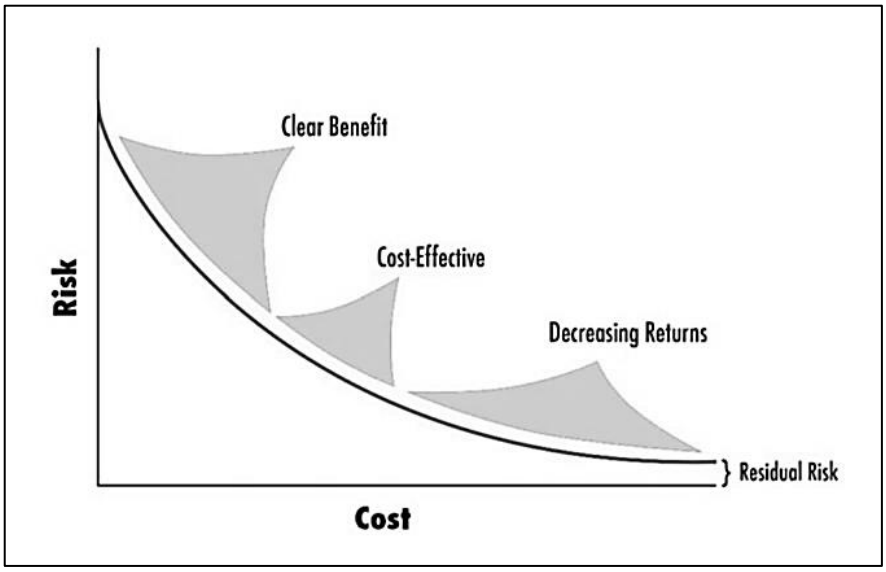

Figura 10 – Diagrama conceptual do custo de diminuição de risco em ciber-sistemas (segundo Bostick et al. 2018)

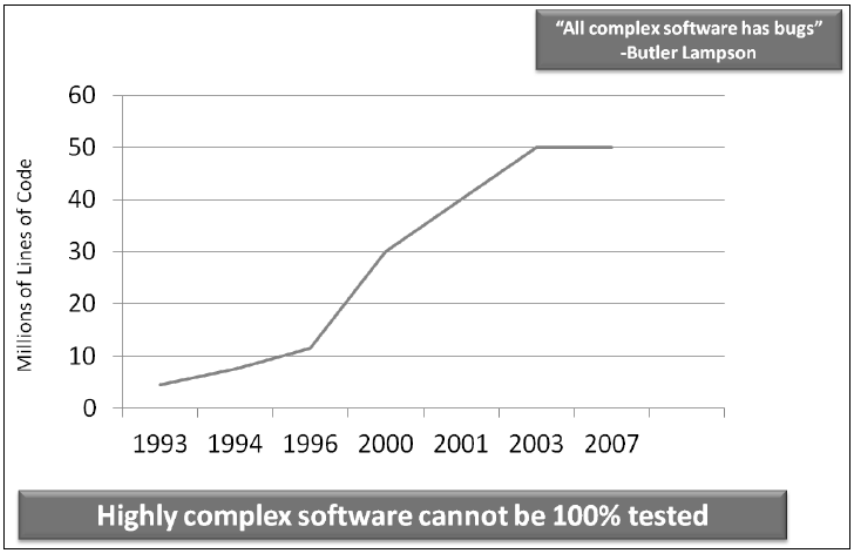

Figura 11 – Evolução do número de linhas de código-fonte dos sistemas operativos comerciais
Fonte: (DSB, 2014)

Apenas as vulnerabilidades que têm um método de ataque conhecido e que tenham grande probabilidades de serem exploradas é que são consideradas ameaças de alta prioridade. São estas vulnerabilidades que deverão ser mitigadas numa primeira fase. Para realizar a análise e classificar o risco deverá ser utilizada a ferramenta "DREAD[12]".

DREAD é um acrónimo que descreve 5 critérios[13] para avaliar as ameaças no mundo ciber:

- ***D**amage* (Dano): Segundo a *Microsoft* a avaliação dos danos que poderão resultar de um ataque à segurança é uma parte crítica da modelação de ameaças. Estes danos poderão incluir perda de dados, falha dos equipamentos, redução de performance ou qualquer medida que se aplique a um determinado dispositivo e o ambiente em que este opera.
- ***R**eproducibility* (Reprodutibilidade): Esta é a medida que quantifica o quão frequente um determinado tipo de ataque irá ter sucesso. É mais provável que uma ameaça facilmente repetida seja explorada do que uma que poderá ocorrer raramente.
- ***E**xploitability* (Explorabilidade): Esta componente avalia o esforço e o nível de conhecimento necessário para realizar determinado ataque. Uma vulnerabilidade que possa ser atacada por alguém com poucos conhecimentos tem um grande nível de explorabilidade. Um ataque que requeira pessoal com elevados níveis de conhecimentos técnicos e que tenha elevados custos associados, tem um menor nível de explorabilidade.
- ***A**ffected Users* (Utilizadores Afetados): O número de utilizadores que possa ser afetado por um ataque também é um fator importante quando avaliamos as ameaças. Um ataque que apenas afete um ou dois utilizadores poderá ser avaliado relativamente baixo nesta medida. Por outro lado, um ataque de interrompa todas as comunicações da rede, que irá afetar todos os utilizadores, será avaliado muito alto.

[12] DREAD – Ferramenta que faz parte de um sistema de avaliação de risco para ameaças de segurança a computadores desenvolvida pela *Microsoft*

[13] Informação retirada do website:
https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers acedido no dia 25 de março de 2019 às 17:20

- ***D**iscoverability* (Descoberta): Esta medida representa a probabilidade que uma ameaça tem de ser explorada. De acordo com a *Microsoft* esta medida é difícil de estimar com precisão, sendo que a modalidade de a abordar com mais segurança será assumir que todas as vulnerabilidades virão, eventualmente, ser aproveitadas e, consequentemente, permitir às outras componentes do DREAD definirem a priorização das vulnerabilidades a mitigar.

Para colocar esta ferramenta em prática, deverá ser utilizada uma tabela como a representada na Tabela 2.

Tabela 2 – Classificação *"DREAD"*

Vulnerability	D Damage	R Reproducibility	E Exploitability	A Affected users	D Discoverability	Total
V_1						
V_2						
V_3						
…						
V_n						

Kurdziel (2014) sugere que um sistema de classificação de 4 pontos é o mais indicado para ser aplicado em que 1 corresponde a “baixo”, 2 a “médio”, 3 a “alto” e 4 a “crítico”. Cada vulnerabilidade deverá ser avaliada consoante cada componente do DREAD e, por fim, deverá ser somado o total. Esse total será o que vai ditar a formalização da lista priorizada de vulnerabilidades organizada de forma descendente. Em seguida, essa lista deverá ser dividida em 4 categorias por alguém com conhecimento especializado do sistema. A primeira categoria consiste nas vulnerabilidades que representam uma ameaça agressiva e que devem ser mitigadas imediatamente. A segunda categoria consiste nas ameaças que devem ser mitigadas com menos urgência. A terceira categoria consiste nas vulnerabilidades que deverão ser monitorizadas e que, caso avancem para uma categoria de ameaça superior, deverão ser mitigadas. A quarta categoria consiste nas vulnerabilidades que não mostram ameaça e que não precisam de ser mitigadas.

3.3. Modelo de Ameaças à rede do SACC

Esta seção apresenta a uma caracterização do sistema do SACC incluindo os recursos do sistema, uma visão global da sua arquitetura e uma decomposição do sistema.

3.3.1. Recursos do sistema

De acordo com a investigação, o recurso primário do sistema é a informação transmitida por qualquer uma das redes apresentadas no esquema da Figura 5 do Capítulo 1. O tráfego consiste em toda a informação relativa ao planeamento e execução de Fogos no escalão que se estiver a trabalhar, em que no caso Português, este escalão corresponde a Brigada, e inclui todos os escalões subordinados (Chora, 2019; Feliciano, 2019) como também toda a informação corrente de operações, informações e Logística do GAC (Feliciano, 2019). Esta informação poderá ser na forma de voz ou dados. O comprometimento deste recurso é de grande valor para o adversário e será o alvo prioritário. Para Feliciano, um dos dados que é crítico para a ciber-resiliência são os próprios dados da rede SACC, uma vez que todos os sistemas (AFATDS, FOS e BCS) possuem dados da rede na sua base de dados, ou, pelo menos, possuem os dados das máquinas com quem essa máquina comunica, desde *unit reference numbers, tacfire alias,* configurações de modulação digital/analógica (protocolo *Mil-std 188-220*/*TACFIRE,* endereço IP das máquinas, velocidade de transmissão de dados, modo de encriptação de dados) (Feliciano, 2019).

Outro recurso do sistema é o funcionamento da rede em si. Os administradores e os seus utilizadores precisarão que o sistema esteja completamente disponível a toda o momento para poderem suportar as comunicações no campo de batalha, aceder aos recursos da rede, aceder às informações técnicas correspondentes aos comandos de tiro, etc. Numa primeira instância, o adversário irá colocar como alvo a informação passada no sistema, no entanto o adversário poderá aumentar a sua vantagem tática através da disrupção dos sistemas de comunicação.

3.3.2. Arquitetura do Sistema

A arquitetura da rede do SACC pode ser considerada uma *Wide Area Network (WAN)*[14] heterogénea que poderá ser montada de diversas formas, ligando os AFATDS no PC/GAC por *Local Area Network* (LAN), ligando o AFATDS ao FOS por rádio P/PRC-525 em modulação digital (com o protocolo *MilStd 188-220*), ligando o AFATDS ao BCS por rádio em modulação analógica (protocolo *TACFIRE)* ou – no extremo – ligar tudo entre si com WD1-TT em protocolo *TACFIRE* (Feliciano, 2019). Os equipamentos utilizados são robustos com vista ao Ambiente Tático em que vão ser empregues e em que os níveis de segurança do campo de batalha variam entre desafiantes a hostis. Estes equipamentos são desenhados para serem à prova de falhas e invioláveis. Os administradores dos sistemas são treinados de forma a operarem os equipamentos com vista a não introduzirem erros ou danos não intencionais, no entanto os subsistemas do SACC e o próprio rádio P/PRC 525 não são *user friendly* e para que o SACC funcione devidamente é necessário uma equipa permanentemente dedicada e a treinar no Quartel (Feliciano, 2019). Entre 2010 e 2014 os operadores do SACC, no dia a dia, entre as formaturas trabalhavam no SACC. Antes de cada exercício era realizado um ciclo de treino para garantir que tudo funcionava corretamente (Feliciano, 2019). No entanto, atualmente, devido à falta de efetivos torna-se complicado treinar os militares neste tipo de equipamentos que requerem muito treino e conhecimentos técnicos (Chora, 2019). No caso do AFATDS (Feliciano, 2019) é possível configurar o nível de privilégio que cada utilizador tem, em contraste com o BCS, FOS e GDU que não possuem tal funcionalidade mas que, no entanto, são desenhados de forma a estarem limitados à informação respetiva de cada subsistema (Chora, 2019).

Uma vez que que os utilizadores e administradores do sistema são militares, estes são sujeitos ao regulamento de disciplina militar e demais leis de âmbito militar que exigem um comportamento adequado dos mesmos. Posto isto, prossupõe-se que os administradores e utilizadores deste sistema não estão predispostos a causar dano intencional.

[14] WAN - Rede de Área Alargada

3.3.3. Caracterização do Adversário

O processo de modelação de ameaças foi aplicado à rede SACC considerando que esta é composta pelos subsistemas LAN e redes sem fios descritos na secção anterior. O perfil da ameaça é descrito nesta secção. Considera-se que o atual adversário genérico tem profundos conhecimentos no que diz respeito ao domínio ciber e que pretende tirar partido da principal vulnerabilidade do Ocidente para combater – a dependência de sistemas de comando e controlo digitais (Feliciano, 2019).

Kurdziel (2014) por sua vez considera que o atual adversário é bastante sofisticado, sendo este uma agência de informações nacional. Estas agências têm capacidades e conhecimentos de nível mundial no que diz respeito à cibersegurança. Apesar de não existirem dados concretos sobre as capacidades destas agências, assume-se que estas excedam qualquer capacidade que exista no setor público (Kurdziel, 2014). No que diz respeito à tecnologia disponível considera-se que as agências de inteligência das potências mundiais possuam tecnologia topo de gama, como por exemplo supercomputadores ou ciberarmas desenvolvidas que podem explorar vulnerabilidades não conhecidas, que até poderá não estar disponível no setor publico. Não existindo oportunidade de verificar esta informação, deverá ser assumido que o adversário tem acesso a tecnologia de computação poderosa e que tem capacidade de construir componentes à medida do necessário (Chora, 2019; Kurdziel, 2014).

Focando os alvos e objetivos do adversário, considera-se que este irá à procura de tudo o que lhe fornecer vantagem no campo de batalha. Para isso, todos os recursos do sistema descritos na secção 3.1.2.1. serão alvo. O tráfego da rede será o alvo primário (Chora, 2019; Feliciano, 2019), no entanto os mecanismos criptográficos implementados não permitam que o adversário tenha oportunidade de calcular o valor da informação até esta estar comprometida. Posto isto, toda a informação e qualquer equipamento que a processe poderá ser alvo de ataque.

Como exposto na secção 3.1.2.1. outro recurso do sistema é a funcionalidade da mesma. A segurança e disponibilidade do sistema deverá ser sempre considerada. No entanto, perante os problemas de interoperabilidade que existem entre os diversos equipamentos que constituem o SACC, o principal foco tem sido a interoperabilidade entre os mesmos, descurando na segurança. Ao utilizar o protocolo MilStd 188-220[15], a operação

[15] **MIL-STD 188-220** - Identifica procedimentos, protocolos e parâmetros a serem aplicados nos aparelhos de transferência de mensagens digitais

em SECOM-V[16] é possível entre o AFATDS e FOS, ou seja, a transmissão é segura, no entanto o funcionamento do sistema deixa de ser fiável uma vez que surgem erros nas mensagens trocadas (Feliciano, 2019; Fonseca Vicente, 2019). A quebra do sistema irá trazer ao adversário uma enorme vantagem no campo de batalha e será certamente um objetivo primário (Kurdziel, 2014), no entanto, utilizando o protocolo *TACFIRE,* caso alguma máquina na rede falhe, os FOS conseguem comunicar diretamente para os BCS, ou falhando o FOS, o OAv pode enviar a correção de tiro por voz na mesma rede e no mesmo rádio a que o FOS está ligado uma vez que em *TACFIRE* a voz sobrepõe-se aos dados, e na Artilharia os dados de tiro têm prioridade sobre tudo o resto (Feliciano, 2019).

3.3.4. Potenciais vulnerabilidades dos componentes do sistema

Na impossibilidade de testar as vulnerabilidades existentes no SACC, considera-se pertinente ilustrar as possíveis vulnerabilidades que um sistema genérico como o SACC poderá estar sujeito, como sugere a Tabela 3.

Tabela 3 – Vulnerabilidades de uma Rede Tática tipo SACC por subsistema

	Categoria da Ameaça	LAN	Rede Rádio
S	***Spoofing Identity* – Falsificação da Identidade**	• Acesso não autorizado	• Acesso não autorizado • Inexistência de seguranças físicas (Barreiras) • Equipamentos comprometidos
T	***Tampering with Data* – Adulteração de Dados**	• Acesso ao canal de Transmissão	• Acesso ao canal de transmissão de dados
R	***Repudiation***	• Vulnerabilidades nos protocolos da Rede	• Vulnerabilidades dos protocolos da rede
I	***Information Disclosure* – Divulgação de Informação**	• Acesso ao canal de transmissão	• Acesso ao canal de transmissão • Análise do fluxo do tráfego • Inexistência de Segurança Física

[16] SECOM-V Transmissão segura com Salto de Frequência

D	***Denial of Service* – Negação de Serviço**	• Erro Humano ou malícia • Código malicioso (e.g. vírus) • Limitação dos Recursos: Interfaces, memórias, banda-larga da ligação, banda-larga computacional • Gestão centralizada vulnerável • Disrupção catastrófica	• Erro Humano ou malícia • Código malicioso (e.g. vírus) • Limitação dos recursos: Interfaces, memórias, banda-larga da ligação, banda-larga computacional • Inexistência de uma gestão da rede centralizada ou gestão de segurança • Equipamentos comprometidos • Inexistência de seguranças físicas (Barreiras) • A posição, escala e topologia da Rede é dinâmica • Deteção/disrupção das ondas rádio • Disrupção catastrófica
E	***Elevation of Privilege* – Elevação de Privilégios**	• Erro Humano ou malícia • Acesso não autorizado • Vulnerabilidades dos protocolos da rede	• Erro humano ou malícia • Acesso não autorizado • Equipamentos comprometidos • Vulnerabilidades dos protocolos da rede

Adaptado de Kurdziel (2014)

Assim que as potenciais vulnerabilidades estejam identificadas, devem-se enumerar e priorizar. As vulnerabilidades com maior prioridade são consideradas ameaças. Estas ameaças deverão ser classificadas usando a ferramenta de risco "DREAD" descrita na secção 3.1.1.3. .

3.3.5. Possíveis mitigações das vulnerabilidades explanadas

Nesta secção são identificados potenciais métodos para mitigar as ameaças e vulnerabilidades consideradas nas secções anteriores. A Tabela 4 sumaria os potenciais controlos, contramedidas, políticas e procedimentos que poderão ser considerados para manter a rede do SACC segura.

Tabela 4 – Resumo de possíveis mitigações das vulnerabilidades

Subsistema	Vulnerabilidade	Mitigação
LAN	Acesso não autorizado	• Segurança física • Sistema de controlo de acessos • Redundância funcional em caso de comprometimento • Sistema de prevenção/deteção de intrusão

Rede Rádio	Acesso não autorizado	• Sistema de controlo de acessos • Sistema de prevenção/deteção de intrusão • Emissão de relatórios • Terminais seguros • Acesso respeitando o princípio do mínimo privilégio
LAN	Disrupção Catastrófica	• Plano de continuação da Missão e Recuperação de Desastres
Rede Rádio	Disrupção Catastrófica	• Plano de continuação da Missão e Recuperação de Desastres
LAN	Acesso ao canal de transmissão	• Encriptação do canal, rede fechada
Rede Rádio	Acesso ao canal de transmissão	• Encriptação do canal, rede fechada
LAN	Erro humano ou malícia	• Treino dos utilizadores • Investigação do passado dos utilizadores • Princípio do Mínimo Privilégio
LAN	Erro humano ou malícia	• Treino dos utilizadores • Sistema de prevenção/deteção de intrusão • Investigação do passado dos utilizadores • Princípio do Mínimo Privilégio
LAN	Código malicioso	• Programas de deteção de vírus • Listas de acesso autorizado • Defesa em profundidade
Rede Rádio	Código malicioso	• Programas de deteção de vírus • Listas de acesso autorizado • Defesa em profundidade • Rede fechada
Rede Rádio	Deteção/Disrupção das Ondas Rádio	• Usar baixa potência • Procedimentos rádio • Diminuir o alcance dos sinais transmitidos • Utilizar técnicas Anti-Jam (e.g. Salto de Frequência)

Adaptado de Kurdziel (2014)

Em seguida, são explicados os requisitos para possibilitar algumas das mitigações supracitadas.

a. Sistema de controlo de acessos

O acesso deverá ser restringido a quem está autorizado e a quem compete saber. O controlo de acessos assegura que o sistema mantém a confidencialidade e integridade da informação através de um controlo de acessos baseado nas funções dos utilizadores. No caso

do AFATDS este tipo de sistema poderá ser configurado, atribuindo mais ou menos privilégios consoante o utilizador que o esteja a operar (Feliciano, 2019).

b. Sistema de prevenção/deteção de intrusões

Estes sistemas permitem a combinação entre métodos baseados em análise de eventos de rede ou dos subsistemas terminais (e.g. logs), e podem usar métodos de análise com base em assinaturas (ataque conhecido) ou anomalias (comportamento desviante).

c. Encriptação do canal de transmissão

A encriptação do canal de transmissão permite que a informação enviada na rede seja cifrada de forma a proteger a sua integridade e confidencialidade. Isto irá evitar que haja informação não segura a circular em claro (sem cifra) através dos sinais eletromagnéticos.

d. Redundância Funcional

Quando possível, as operações ocorrentes na rede que sejam fundamentais deverão ser redundantes. Um AFATDS deverá conseguir assumir as funções de outro caso este seja comprometido, de forma a dar seguimento à missão. Se o tempo disponível o permitir, as secções deverão e o PCT deverão instalar e operar os equipamentos filares. No caso de os rádios não estarem disponíveis ou utilizáveis, o sistema filar é necessário. Em última instância, a missão deverá prosseguir por métodos manuais caso o SACC seja comprometido.

e. Barreiras de segurança físicas

As barreiras de segurança físicas são fundamentais para qualquer plano de segurança (Ribeiro, 2019). Os terminais do sistema deverão ser monitorizados e mantidos em segurança através de combatentes armados de forma a assegurar o sucesso da missão.

f. Ondas rádio específicas

O uso de ondas rádio específicas, nomeadamente ondas de curto alcance e ondas de baixa probabilidade de deteção/interceção melhoram a segurança da rede escondendo o funcionamento do sistema. A utilização de técnicas *Anti-jam*, como por exemplo as técnicas que empregam o salto de frequência, fazem com que seja mais difícil para o adversário quebrar as comunicações dos sistemas mesmo que o funcionamento do mesmo seja detetado.

g. Políticas de Segurança

Os sistemas de comunicação sem fios deverão incluir atualizações periódicas relativa às políticas de segurança de forma a assegurar a operação, manutenção e administração fidedigna dos sistemas.

h. Erro humano ou comportamento malicioso

O treino para a administração destes sistemas deverá ser rigoroso e os utilizadores deverão receber o mínimo privilégio possível para operarem os equipamentos. Os utilizadores deverão estar cientes das políticas de segurança e das consequências que a má utilização do equipamento poderá trazer (Ribeiro, 2019).

3.3. Síntese do capítulo e análise de resultados

Neste capítulo aplicou-se um modelo de ameaça ao SACC, referindo algumas vulnerabilidades que este poderá estar sujeito e sugerindo algumas mitigações possíveis para fazer frente a diferentes tipo de ameaças. Foi utilizado um modelo focado em Redes Táticas Militares, conceptualizado por Kurdziel. Para isso, inicialmente caracterizou-se o SACC num ponto de vista de segurança. Em seguida desenvolveu-se o perfil da ameaça, identificando/caracterizando o adversário, os seus alvos/objetivos e as vulnerabilidades que o sistema poderá conter. Numa fase final, foram sugeridas mitigações para fazer frente às vulnerabilidades explanadas no ponto anterior.

Capítulo 4. CIBER-RESILIÊNCIA EM CONTEXTO EMPRESARIAL

O ciber-risco não é algo novo, mas com o passar dos tempos as probabilidades de ser atacado aumentam a cada dia que passa (Symantec, 2014). Um incidente deixou de ser um evento único, mas sim uma campanha sustentada e persistente. A maior parte dos analistas, empresários, e visionários chegaram à mesma conclusão: não existe uma solução que seja cem por cento eficaz no que diz respeito à cibersegurança (Symantec, 2014).

Tanto a Linkov e Kott (2019) como Connelly et al. (2017) consideram que a resiliência tem quatro fases sendo estas: Planear, Absorver, Recuperar e por fim Adaptar.

A Symantec (2014) considera que no que diz respeito à perspetiva da ciber-resiliência, esta assenta nos 5 pilares que o *National Institute of Standards and Technology* (NIST) (2018) define como nucleares na sua *framework* para melhorar a cibersegurança de infraestruturas críticas, sendo estes Preparar/Identificar, Proteger, Detetar, Responder e por fim, Recuperar. Estes pilares não se destinam a formar um caminho único ou levar a um estado final desejado. Ao invés disso, estes pilares devem ser tidos em consideração e ser executadas simultânea e continuamente de forma a possibilitar uma cultura operacional que aborde o risco dinâmico de cibersegurança (NIST, 2018).

A *framework* desenhada para o incremento da cibersegurança das infraestruturas críticas proposta pelo NIST é dividida em funções, categorias, subcategorias e referências informativas que descrevem procedimentos específicos que são comuns a todos os setores das infraestruturas críticas. Esta *framework* representa um conjunto de atividades úteis à gestão de risco no domínio da cibersegurança. Posto isto, verifica-se a possibilidade de utilizar algumas destas atividades no que diz respeito ao SACC.

Para Lourenço Martins (2019), no que diz respeito à ciber-resiliência, as empresas aplicam diversos controlos presentes nas *frameworks* internacionais (e.g., ISO 27001) e nacionais (e.g., NIST 800-53) e de modelos militares (e.g., NATO) que direcionam a empresa para um caminho de resiliência. Lourenço Martins (2019) divide a resiliência em 3 grupos, sendo que o primeiro é o grupo da resiliência nos processos, o segundo consiste na resiliência no treino dos colaboradores e o terceiro, não menos importante, a resiliência nas tecnologias.

Na primeira secção deste capítulo é feita uma sistematização relativa às atividades presentes na *framework* proposta pelo NIST. Os controlos integrantes nos grupos sugeridos por Lourenço Martins incluem-se nesta *framework.* Este capítulo, nas três secções que

sucedem a primeira, irá explorar cada um dos grupos propostos por Lourenço Martins, tendo como foco relacionar as metodologias utilizadas nas empresas com o que deverá ser realizado no SACC.

4.1. Núcleo da *framework* proposta pelo NIST para incrementar a cibersegurança

O núcleo da *framework* proposta pelo NIST fornece um conjunto de atividades que permitem alcançar fins de cibersegurança específicos, e exemplos de referência de formas como alcançar esses fins (NIST, 2018). O núcleo compreende 4 elementos, sendo estes: "Funções"; "Categorias"; "Subcategorias"; "Referências informativas". A Tabela 5 faz a ligação entre as funções e as diferentes categorias propostas pelo NIST.

Tabela 5 – Relação entre as funções e categorias da framework proposta pelo NIST

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Fonte: (NIST, 2018)

4.1.1. Funções

O elemento "Funções" organiza as atividades de cibersegurança ao seu nível mais elevado. As Funções são "Identificar", "Proteger", "Detetar", "Responder" e "Recuperar". Estas ajudam uma organização a expressando a sua gestão de risco de cibersegurança organizando a informação, permitindo decisões relativas à gestão de risco, e incrementando a cibersegurança através das lições aprendidas (NIST, 2018). As Funções também se alinham com metodologias existentes que dizem respeito à gestão de incidentes e ajudam a mostrar o impacto dos investimentos na cibersegurança (NIST, 2018). As cinco Funções do núcleo da *framework* são enumeradas nas próximas subsecções.

a. Identificar

A função Identificar refere-se ao desenvolvimento da compreensão organizacional na gestão do risco da cibersegurança relativamente aos sistemas, pessoas, ativos, dados, e capacidades. As atividades desta Função são essenciais para o uso desta *framework.* Perceber o contexto do negócio, os recursos que suportam as funções críticas, e os riscos de cibersegurança relacionados permite que uma organização se foque e que priorize os seus esforços, consoante a sua estratégia de gestão de risco e necessidades de negócio. Exemplos de Categorias dentro desta função incluem: Gestão de Ativos; Ambiente do Negócio; Gestão de Risco; e Estratégias de Gestão de Risco.

b. Proteger

Esta função diz respeito ao desenvolvimento e integração apropriada de salvaguardas no sentido de assegurar a prestação dos serviços mínimos. Esta função implica a capacidade de limitar ou conter o impacto de um potencial evento de cibersegurança. Exemplos de Categorias dentro desta função incluem: Gestão de Identificação e Controlo de Acessos; Despertar de Consciências e Treino; Manutenção; Tecnologia de proteção.

c. Detetar

Desenvolver e implementar atividades apropriadas à identificação da ocorrência de eventos de cibersegurança é a terceira função apresentada. Esta função permite a descoberta de eventos de cibersegurança periodicamente. Exemplos de Categorias dentro desta função incluem: Deteção de Anomalias e Eventos; Monitorização Contínua de Segurança; Processos de Deteção.

d. Responder

A função Responder refere-se ao desenvolvimento e implementação de atividades apropriadas que entram em ação após a deteção de um evento de cibersegurança. Esta função suporta a capacidade de conter o impacto de um incidente de cibersegurança. Exemplos de Categorias dentro desta função incluem: Planeamento de Resposta; Comunicações; Análise; Mitigação; e Melhoramentos.

e. Recuperar

O desenvolvimento e implementação de atividades para manter planos de resiliência e de restaurar qualquer capacidade ou serviços que foram parados devido a um incidente de cibersegurança diz respeito à última função, Recuperar. Exemplos de Categorias dentro desta função incluem: Planeamento de recuperação; Melhoramentos; e Comunicações.

4.1.2. Categorias

São as subdivisões de cada Função em grupos de resultados de cibersegurança, ou seja, estas subdivisões estão ligadas a necessidades programáticas e atividades particulares nesta área. Exemplos de categorias incluem: Gestão de Ativos, Gestão de Identificações e Controlos de Acesso, e Processos de Deteção.

4.1.2. Subcategorias

São as subdivisões de cada Categoria correspondendo a resultados técnicos específicos e/ou atividades de gestão. Estas subcategorias fornecem um conjunto de resultados que vão apoiar a finalização dos resultados de cada Categoria. Estas subcategorias associam-se aos controlos que podem ser aplicados num sistema de forma a contribuir para a sua cibersegurança.

4.1.3. Referências Informativas

São secções específicas de documentos de normalização, práticas comuns relativas a infraestruturas críticas ou *guidelines* que ilustram um método para alcançar resultados de cada subcategoria.

4.2. Resiliência nos Processos

Para que uma empresa faça frente e supere um ataque, quem está responsável pela sua segurança deverá compreender qual é a sua postura relativamente ao risco e à segurança da mesma (Lourenço Martins, 2019; Symantec, 2014). Desta forma, a informação vital da organização deverá ser identificada exaustivamente. As infraestruturas e os sistemas de informação deverão ser testados em todas as vulnerabilidades encontradas. Sinalizar e referenciar as situações mais urgentes irá fazer com que a empresa não tenha tanta preponderância a ser alvo de ataques (Symantec, 2014). Entender o contexto de negócios, os recursos que suportam funções críticas e os riscos de cibersegurança relacionados permite que uma organização foque e priorize seus esforços, consoante a sua estratégia de gestão de risco e necessidades de negócios (NIST, 2018).

Para Lourenço Martins (2019) a ciber-resiliência nos processos passa pela realização de cópias de segurança da informação, pelo teste da recuperação dessas cópias, pela realização de planos de recuperação de dados (Center for Internet Security, 2019), isto é, permitindo que a informação esteja disponível em locais descentralizados, e pela criação de planos de continuidade de negócios (ISO, 2012; Swanson et al. , 2010).

Relativamente ao controlo de cópias de segurança do sistema de informação, o NIST (Joint Task Force Transformation Initiative, 2013) prevê um controlo – CP-9, designado de "*Information System Backup"* que sugere que a organização deverá realizar cópias de segurança ao nível do utilizador, do sistema e da documentação, incluindo documentação relacionada com a segurança, presentes no sistema de informação, de forma periódica, em que a frequência é definida pela organização consoante o tempo de recuperação e os objetivos da recuperação de informação. A organização também deverá ser responsável por proteger a confidencialidade, integridade e disponibilidade das informações das cópias de segurança (Joint Task Force Transformation Initiative, 2013; NIST, 2019). As informações das cópias de segurança deverão ser testadas de forma a verificar a confiabilidade do dispositivo onde esta está armazenada e a integridade das informações (NIST, 2019).

Transpondo este controlo para o caso do SACC, verifica-se que no que diz respeito ao AFATDS, este permite efetuar backups para recuperação do sistema num dado ponto (Fonseca Vicente, 2019) e que com um disco de reserva e uma disquete com a base de dados *backup* é somente necessário substituir o disco (Feliciano, 2019), que por sua vez é de fácil acesso (Chora, 2019). Para além disso, o AFATDS tem uma funcionalidade chamada

CONOPS[17] que pode ser pré-programada que, em caso de avaria/destruição de um dos AFATDS da rede, esta é reconfigurada de forma a continuar a operação mediante as alternativas pré-configuradas, designando uma máquina para substituição de outra temporariamente até que a anterior esteja novamente operacional (Fonseca Vicente, 2019), no entanto, este processo é complexo e não muito célere (Feliciano, 2019). No que diz respeito aos restantes equipamentos do SACC, estes não possuem esse tipo de capacidade (Feliciano, 2019).

Os planos de continuidade de negócios previstos nos relatórios ISO 22301:2012 (ISO, 2012) e NIST SP 800-34r1 (Swanson et al., 2010) concentram esforços em sustentar os processos da missão da organização enquanto esta está a ser alvo de uma dirupção de serviço (Swanson et al., 2010).

Na Artilharia, caso exista uma dirupção no SACC, a missão deverá prosseguir. Feliciano (2019) confirma que caso o FOS seja comprometido, a Missão de Tiro deverá prosseguir com o OAv a transmitir o pedido de tiro por voz. Aquando o BCS recebe as informações enviadas pelo OAv, os dados recebidos devem ser registados numa folha de papel e a coordenada do ponto de regulação deverá ser implantada na prancheta. Caso o BCS avarie, é possível continuar o tiro manualmente (Feliciano, 2019).

4.3. Resiliência no treino dos colaboradores

É tentador pensar que a ciberdefesa é um desafio técnico *a priori*, no entanto as ações dos colaboradores têm um papel preponderante no sucesso ou insucesso de uma organização (Center for Internet Security, 2019). Os colaboradores preenchem funções importantes em cada fase da implementação, construção, operação, uso e supervisão do sistema. A nova "Lei da Cibersegurança" sugere que "a cibersegurança não é só uma questão relacionada com a tecnologia; o comportamento humano é igualmente importante. Por conseguinte, dever-se-á promover…medidas simples de rotina que, quando implementadas e aplicadas com regularidade pelos cidadãos, as organizações e as empresas, minimizam a sua exposição aos riscos decorrentes de ciberameaças" (Niebler, 2019). Para que isso seja possível, é necessário que as organizações promovam o treino nesta área. Um programa de treino eficiente deverá efetuar uma abordagem holística e considerar as políticas e a tecnologia ao mesmo tempo que está a treinar os colaboradores. Não poderá ser apenas um evento anual; é um processo

[17] CONOPS – Continuidade das Operações

contínuo de melhoramento e que deverá consistir nos seguintes elementos chave (Center for Internet Security, 2019):

- O treino deverá ser específico, à medida do utilizador e focado em comportamentos e competências específicas que os colaboradores necessitam, dependendo da sua função e responsabilidade.
- O treino deverá ser realizado de forma periódica, atualizado regularmente, e a sua eficiência deverá ser medida e testada.
- Este treino irá aumentar a consciencialização e desencorajar a que existam comportamentos de risco apenas por incutir uma racionalização relativamente a bons comportamentos e competências de segurança.

Tanto Chora (2019) como Ribeiro (2019) consideram que atualmente ainda não existe uma cultura incutida no Exército para a consciencialização da importância da cibersegurança e, desta forma, não existem programas de treino para os colaboradores que operam o SACC, neste momento.

4.4. Resiliência nas tecnologias

A resiliência nas tecnologias deverá ser prevista desde o momento da aquisição de um sistema até à efetivação do uso do mesmo. Posto isto, diversos controlos deverão ser tido em conta, começando pela proteção da cadeia de fornecimento terminando em todos os controlos que deverão proteger o sistema.

As organizações devem proteger a cadeia de fornecimento dos sistema de informações e dos seus componentes, empregando uma estratégia abrangente da segurança das informações (Joint Task Force Transformation Initiative, 2013). Os sistemas de informação (incluindo os componentes que formam esses sistemas) têm que ser protegidos durante o ciclo de vida do desenvolvimento do sistema (e.g., durante a sua conceptualização, desenvolvimento, produção, empacotamento, montagem, distribuição, integração no sistema, manutenção e reforma) (Joint Task Force Transformation Initiative, 2013).

"A certificação da cibersegurança desempenha um papel importante no aumento da confiança e segurança dos produtos, serviços e processos de tecnologias de informação e comunicação" (Niebler, 2019). Tendo esta premissa em conta, constata-se que para uma tecnologia seja considerada ciber-resiliente, esta deve ser certificada e possuir mecanismos que permitam que quando for alvo de ataque, esta consegue manter um nível aceitável de

desempenho e recuperar o seu estado de funcionamento normal num curto espaço de tempo. Em Portugal, quem tem capacidade para certificar os equipamentos do Exército é o Gabinete Nacional de Segurança (Ribeiro, 2019). O processo de certificação é um processo contínuo que deverá ser renovado de 3 em 3 anos (Ribeiro, 2019). Este é um processo moroso, que implica teste de avaliação funcional e criptográfica que comprovam o grau de segurança das diferentes plataformas, assim como devem ser verificadas as atualizações de software, a robustez do mesmo. No que diz respeito aos equipamentos do SACC, uma vez que estes foram adquiridos há mais de 10 anos, não possuem qualquer tipo de certificação (Ribeiro, 2019).

4.5. Síntese do capítulo

Este capítulo pretendeu fazer uma relação entre a forma como as organizações de âmbito civil gerem a sua capacidade de serem ciber-resilientes com a forma como será possível gerir a ciber-resiliência de um sistema como o Sistema Automático de Comando e Controlo.

Inicialmente foi feita uma introdução relativamente ao núcleo da *framework* para a cibersegurança das infraestruturas críticas proposta pelo NIST. O núcleo desta *framework* é um conjunto de atividades de cibersegurança, resultados desejados e referências aplicáveis que são comuns em setores críticos de uma infraestrutura. Esta *framework* apresenta padrões, diretrizes e prátidas da industria de maneira que permita resultados de cibersegurança em toda a organização, desde o escalão mais alto até ao escalão das operações. O núcleo da *framework* consiste em cinco Funções – "Identificar", "Proteger", "Detetar", "Responder" e "Recuperar". Quando consideradas em conjunto, essas funções fornecem uma visão estratégica de alto nível relativamente ao ciclo de vida da gestão do risco de cibersegurança de uma organização. Após isso o núcleo identifica categorias e subcategorias importantes, para cada função, combinando-as com referências informativas tais como padrões, diretrizes e práticas comuns.

Em seguida, é feita uma análise aos grupos relativos à ciber-resiliência, sugeridos por Lourenço Martins – Resiliência nos Processos; Resiliência no treino dos colaboradores; Resiliência nas tecnologias. Desta forma, são apresentados alguns controlos que integram as referências informativas no núcleo da *framework* de forma a permitir caracterizar cada um dos grupos, fazendo uma ponte com o Sistema Automático de Comando e Controlo.

CONCLUSÕES E RECOMENDAÇÕES

O presente relatório, consequência do trabalho de investigação sobre a Ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha, teve como objetivo geral de investigação avaliar a ciber-resiliência do Sistema Automático de Comando e Controlo (C2) da Artilharia de Campanha propor medidas ou métodos que a elevem, recorrendo à análise das normas de segurança e boas práticas estabelecidas internacionalmente. Face a este desígnio, este relatório inicia-se com um capítulo respeitante ao enquadramento teórico da investigação, onde foi explicado o que é o SACC, como é que este é constituído e qual é que é a sua arquitetura. Numa segunda fase do primeiro capítulo foram abordados os conceitos relativos ao ciberespaço, mais concretamente o conceito de ciber-resiliência tanto em contexto nacional como internacional. Também foram definidos os conceitos de cibersegurança e ciberdefesa, realçando as suas diferenças. A última secção do primeiro capítulo destinou-se a relacionar os conceitos de ciber-resiliência e ciber-risco.

O segundo capítulo destinou-se a expor a metodologia de investigação adotada para a realização deste trabalho. Também foi enaltecido o objetivo geral da investigação e, consequentemente, os objetivos específicos que contribuem para a prossecução do mesmo. Com base no objetivo geral de investigação foi criada a questão principal a ser respondida e as suas questões derivadas.

O terceiro e o quarto capítulo são o núcleo da investigação. Podemos dividir o terceiro capítulo em duas partes. Na primeira parte foi demonstrado um modelo de ameaças explicando qual a metodologia que deve ser seguida para verificar quais as ameaças e vulnerabilidades que uma Rede Tática Militar pode estar sujeita, tendo as ferramentas STRIDE e DREAD como pilar nessa análise. Numa segunda fase foi aplicada esta metodologia ao SACC, sendo que na fase final deste capítulo foram sugeridas possíveis modalidades de ação para mitigar as vulnerabilidades apresentadas. É nesta fase do capítulo que se dá a primeira análise e discussão dos resultados obtidos. O quarto capítulo destinou-se a referir como é que as empresas no contexto civil gerem a sua capacidade de serem ciber-resilientes. Este capítulo dividiu-se em 3 subcapítulos, cada um referindo a resiliência necessária em três áreas distintas, sendo estas "resiliência nos processos", "resiliência no treino dos colaboradores" e por fim "resiliência nas tecnologias". Neste capítulo as principais referências dizem respeito às normas de padronização nacionais (americanas) e internacionais (ISO).

Com o objetivo de responder à questão central, é necessário responder às questões derivadas.

Para caracterizar o SACC podemos verificar que o este é um sistema que emprega 4 equipamentos diferentes, AFATDS, BCS, FOS e GDU-R. Este engloba 3 redes diferentes, sendo estas, "Rede de Comando e Direção de Tiro", "Redes de Tiro" e "Rede de Aquisição de Objetivos". A comunicação entre o Oficial de Apoio de Fogos da Brigada, os OAF dos Batalhões, o Oficial de Operações do GAC, o PC/PCT do GAC e os PCT é assegurada através da utilização dos rádios P/PRC-525, AFATDS e BCS. A comunicação entre o PCT de cada bateria de bocas de fogo e os seus OAv é assegurada através dos rádios P/PRC-525 e do FOS. No que diz respeito à transmissão da informação proveniente dos radares ANTPQ-36 e RATAC-S e dos sensores de meteorologia, esta é assegurada através da utilização de rádios P/PRC-525 presentes em cada uma das secções e no S2 do GAC. O S2 do GAC introduz essas informações no seu AFATDS que por sua vez está ligado por cabo ao AFATDS do S3/GAC e ao AFATDS do PC/PCT do GAC, que têm como objetivo retransmitir esses dados para os BCS presentes nas baterias de bocas de fogo.

Concluiu-se que existe uma relação entre a ciber-resiliência e a gestão de risco principalmente porque um sistema que seja ciber-resiliente irá contribuir para que uma organização/sistema, tenha menos probabilidade de sofrer um ataque no domínio ciber. Por sua vez, no sentido contrário, caso um determinado ataque não seja concretizável por parte do adversário, devido às suas limitações tecnológicas/monetárias, a mitigação da vulnerabilidade que permite esse ataque não será prioritária.

No que diz respeito às ameaças que o Sistema Automático de Comando e Controlo poderá enfrentar concluiu-se que estas poderão ser desde falsificação de identidade, adulteração de dados, a divulgação de informação, negação de serviço ou elevação de privilégios. Estas ameaças correspondem a diferentes propriedades sendo estas: autenticação, integridade, não-repúdio, confidencialidade, disponibilidade e autorização. Todas estas categorias contêm diferentes métodos de ataque disponíveis, e cada um destes métodos de ataque tem uma contramedida que deverá ser adotada pelas nossas forças. Comparando os resultados obtidos com os do estudo de Kurdziel relativamente ao Exército Americano, verifica-se uma diferença significativa de como o segundo encara a ciberdefesa comparando com as nossas forças, neste contexto de redes táticas. A maior diferença encontrada verifica-se no facto de que os militares que operam os diferentes equipamentos constituintes da rede são arduamente treinados de forma a que não cometam erros e que estejam cientes que esses erros poderão provocar vulnerabilidades em toda a rede ao invés

que no nosso caso, devido à falta de efetivos e meios, não é possível efetuar este tipo de treino. Outra diferença concreta deve-se ao facto dos componentes das redes táticas americanas serem todos interoperáveis o que não acontece no caso do SACC. Concluiu-se que esta falta de interoperabilidade faz com que o SACC seja mais vulnerável a ataques, portanto sugere-se que caso o SACC seja substituído, sejam tidos em conta tanto os requisitos operacionais que este deverá respeitar, mas também os requisitos técnicos que permitam a interoperabilidade de todos os equipamentos.

Por fim, em comparação com as modalidades adotadas no âmbito civil, no que diz respeito à forma como as organizações gerem a sua capacidade de serem ciber-resilientes, concluiu-se que a aplicação de diversos controlos presentes nas *frameworks* de segurança seguidas pelas organizações, baseadas em normas internacionais, nacionais e especiais, conduzem estas a um estado de ciber-resiliência. Verificou-se que alguns dos controlos são aplicados no que diz respeito ao SACC, mas que é possível melhorar a ciber-resiliência certificando os equipamentos constituintes e treinando os operadores e administradores dos mesmos.

Sintetizando e respondendo à questão central que motivou a realização desta investigação, conclui-se que o estado atual da ciber-resiliência do Sistema Automático de Comando e Controlo da Artilharia de Campanha encontra-se com algumas lacunas que deverão ser corrigidas. Assim, de futuro, considera-se crítico resolver os problemas de interoperabilidades atualmente presentes no SACC, que deixam o sistema vulnerável às ciberameaças. Para a resolução destes problemas propõe-se que deverá ser almejado um programa de aquisições para prolongamento da vida útil do SACC a ser estabelecido com os EUA, que permita a atualização dos equipamentos deste sistema automático de comando e controlo e que seja possível permitir a interoperabilidade destes mesmos equipamentos com os rádios em uso no Exército Português. Para tal é necessário é fundamental garantir que os diversos subsistemas do SACC operem em redes integráveis com as redes rádio de modo seguro e rápido, sem problemas de interoperabilidade. Deverá ser tido em conta que a aquisição dos equipamentos que constituem o SACC deverá ser um processo contínuo, mantendo estes equipamentos atualizados a nível de software, permitindo que estes estejam sempre na sua versão mais recente. Ao nível dos operadores e administradores dos subsistemas do SACC, estes deverão ser sujeitos a planos de formação específicos que permitam que estes não cometam erros que poderão introduzir vulnerabilidades no sistema. Também é importante que cada utilizador tenha a noção da importância da ciber-resiliência do SACC, sendo que um erro simples poderá pôr em causa toda a missão.

LIMITAÇÕES DA INVESTIGAÇÃO

Com os problemas de interoperabilidade que se têm encontrado ao longos dos anos desde a aquisição do SACC, o seu uso tem vindo a diminuir. Com isto, verificou-se que atualmente este sistema se encontra em desuso apesar das suas capacidades. Sendo assim o acesso ao grupo restrito de oficiais que lidaram/lidam com este sistema foi uma limitação da investigação. Uma vez que esta investigação diz respeito a um domínio técnico, o tempo disponibilizado para a realização da mesma foi curto, não sendo possível verificar/auditar as vulnerabilidades existentes nos equipamentos que constituem o SACC.

PROPOSTAS PARA INVESTIGAÇÕES FUTURAS

Uma vez que não foi possível verificar em concreto quais as vulnerabilidades presentes no SACC, considera-se oportuna a investigação nesta área, junto de especialistas da mesma, de forma a ser possível concluir a lista priorizada de ameaças e de vulnerabilidades a mitigar, utilizando a ferramenta DREAD.

Esta investigação e especificamente este relatório científico são o pontapé de partida para investigações no sentido do desenvolvimento duma arquitetura e dum conjunto de requisitos operacionais/funcionais de um novo SACC, contemplando e melhorando a abordagem e metodologia seguida neste trabalho, para identificação de controlos de segurança a serem implementados, no sentido de assegurar a utilização de um sistema ciber-resiliente, capaz de manter os mínimos aceitáveis de execução caso seja alvo de um ciberataque, podendo recuperar do mesmo sem danos consideráveis.

BIBLIOGRAFIA

Babiceanu, R. F., & Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry*, *104*, 47–58. https://doi.org/10.1016/j.compind.2018.10.004

Bodeau, D. (2016). *Cyber Resiliency Resource List*. (16), 10.

Bodeau, D., & Graubart, R. (2017). *Cyber Resiliency Design Principles*. (17), 98.

Bustelo, R. V. (2017). *Compatibilidade das regras contidas no Manual de Tallinn com uma estratégia eficaz de dissuasão no ciberespaço.* Instituto Universitário Militar, Pedrouços.

CCDCOE. (2009). *Manual de Tallinn* (1ª). Tallinn: Cambridge University Press.

Center for Internet Security. (2019). *CIS Controls v7.1*. East Greenbush, Nova Iorque.

Chora, J. D. C. (2019). *Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia - Entrevista ao Capitão de Artilharia Chora* [Presencial].

Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., & Linkov, I. (2017). Features of resilience. *Environment Systems and Decisions*, *37*(1), 46–50. https://doi.org/10.1007/s10669-017-9634-9

Defesa Nacional. (2017). *Despacho n.º 9762/2017*. Obtido de https://dre.pt/home/-/dre/114163969/details/maximized

DSB. (2014). *Resilient Military Systems and the Advanced Cyber Threat*.

EID. (sem data). EID - PRC - 525 Combat Net Radio - Combat Net Radio. Obtido de EID - PRC - 525 Combat Net Radio - Combat Net Radio website: http://www.eid.pt/prod/7/prc-525_combat_net_radio

Escola Prática de Artilharia. (2006). *Arquitectura do Sistema Automático de Comando e Controlo da Artilharia de Campanha* (N. 00.480.010). Região Militar Sul: Escola Prática de Artilharia.

Feliciano, E. (2013). A interoperabilidade do Sistema Automático de Comando e Controlo. *Revista de Artilharia*, (1049 a 1051), 43–63.

Feliciano, E. (2015). *Enquadramento e projetos de interesse para a Artilharia de Campanha*. (1076 a 1078), 56–71.

Feliciano, E. (2019). *Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia - Entrevista ao Major de Artilharia Feliciano* [Escrito].

Ferreira, A. (2013). Revisão das Táticas, Técnicas e Procedimentos da Bateria de Bocas de Fogo face ao Sistema Automático de Comando e Controlo. *Revista de Artilharia*, (1052 a 1054), 133–155.

Florin, M. V., & Linkov, I. (2016). *IRGC resource guide on resilience*. Obtido de irgc.epfl.ch

Fonseca Vicente, A. (2019). *Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia - Entrevista ao Major de Artilharia Vicente* [Escrito].

GAO. (2018). *WEAPON SYSTEMS CYBERSECURITY: DOD Just Beginning to Grapple with Scale of Vulnerabilities* (N. GAO-19-128).

Gómez de Ágreda, A. (2012). El ciberespacio como escenario del conflicto. Identificación de las amenazas. *El ciberespacio. Nuevo escenario de confrontación*, 167–204.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. Em *Engineering within ecological constraints*. Washington, D.C.: National Academy Press.

Hutchison, D., & Sterbenz, J. P. G. (2018). Architecture and design for resilient networked systems. *Computer Communications*, *131*, 13–21. https://doi.org/10.1016/j.comcom.2018.07.028

ISO. (2012). *Societal security - Business continuity management systems - Requirements*. Obtido de https://www.sis.se/api/document/preview/914731/

Joint Task Force Transformation Initiative. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (N. NIST SP 800-53r4). https://doi.org/10.6028/NIST.SP.800-53r4

Kott, A., Alberts, D. S., & Wang, C. (2015). Will Cybersecurity Dictate the Outcome of Future Wars? *Computer*, *48*(12), 98–101. https://doi.org/10.1109/MC.2015.359

Kurdziel, M. T. (2014, Maio 21). *Cyber threat model for tactical radio networks* (S. A. Dianat & M. D. Zoltowski, Eds.). https://doi.org/10.1117/12.2047582

Larkin, S., Fox-Lent, C., Eisenberg, D. A., Trump, B. D., Wallace, S., Chadderton, C., & Linkov, I. (2015). Benchmarking agency and organizational practices in resilience decision making. Em *Environment Systems and Decisions*: *Vol. 35(2)* (pp. 185–195).

Linkov, I., & Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. Em A. Kott & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks* (pp. 1–25). https://doi.org/10.1007/978-3-319-77492-3_1

Lourenço Martins, L. C. (2019). *Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia - Entrevista ao Tenente-Coronel de Infantaria Lourenço Martins* [Chamada].

NATO. (2011). Novas ameaças: a dimensão cibernética. Obtido de Revista da NATO - Novas ameaças: a dimensão cibernética website: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm

NATO. (2014). *Cyber Defence Taxonomy and Definitions*.

NATO. (2018). Cyber defence. Obtido 10 de Abril de 2019, de NATO - Cyber defence website: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en

Niebler, A. (2019). *«Regulamento Cibersegurança» da UE* (N. A8-0264/2018).

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (N. NIST Cybersecurity White Paper). https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2019). NVD - Control - CP - 9 - INFORMATION SYSTEM BACKUP. Obtido 23 de Abril de 2019, de https://nvd.nist.gov/800-53/Rev4/control/CP-9

Oliveira, L. M. G. de. (2014). O Comando, controlo e Comunicações na Artilharia de Campanha - O Caso do GAC/BrigMec. *Revista de Artilharia*, (1061 a 1063), 31–50.

Pereira, J. (2018). *AS AMEAÇAS HÍBRIDAS – UMA ABORDAGEM CONCEPTUAL NO QUADRO DA OTAN E DA UE*. 28.

Ribeiro, J. de O. (2019). *Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia - Entrevista ao Coronel Tirocinado de Transmissões Jorge de Oliveira Ribeiro* [Presencial].

Ross, R. (2018). *Building Cyber Resilient Systems: A National and Economic Security Imperative*. 33.

Ross, R., McEvilley, M., & Carrier Oren, J. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (N. NIST SP 800-160). https://doi.org/10.6028/NIST.SP.800-160

Santos, L. C. dos, Nunes, P. V., Ralo, J., & Mendes, C. P. (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: Instituto da Defesa Nacional.

Sarmento, M. (2013). *Metodologia Cientifica para a Elaboração, Escrita e Apresentação de Teses*. Lisboa: Universidade Lusíada de Lisboa.

Simões, A. M. L., & Dias, P. M. R. de C. D. (2007). O Treino e a Simulação o Sistema Automática de Comando e Controlo (SACC) da Artilharia de Campanha. *Boletim da Escola Prática de Artilharia*, 53–66.

Smith, E. A. (2005). *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*.

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (N. NIST SP 800-34r1). https://doi.org/10.6028/NIST.SP.800-34r1

Symantec. (2014). *The Cyber Resilience Blueprint: A New Perspective on Security*.

APÊNDICES

APÊNDICE A – Guião da Entrevista ao Major de Artilharia Alexis da Fonseca

ACADEMIA MILITAR

Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias
Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Guião de Entrevista ao Major de Artilharia Alexis da Fonseca Vicente

Lisboa, abril de 2019

Data:15-04-2019

Entrevistador: Aspirante de Artilharia Herculano Costa

Entrevistado: Alexis da Fonseca Vicente

Posto: Major

Função: ÁREA DE RECURSOS (ARREC) – Adjunto J4 - CCOM

Questões:

1- Aquando a operação do SACC, a cibersegurança é tida em conta, ou o foco principal é a interoperabilidade dos equipamentos?

2- A certificação dos equipamentos (aprovamento da NATO, por exemplo) é tida em conta? Se sim, os equipamentos utilizados no SACC foram sujeitos a essa certificação?

3- Em algum momento as vulnerabilidades dos equipamentos foram identificadas?

4- Os equipamentos que constituem o SACC possuem proteções contra ameaças?

5- Os equipamentos que constituem o SACC têm capacidade de detetar que estão a ser alvos de um ciberataque?

6- Os equipamentos que constituem o SACC têm capacidade de responder a um ciberataque? Por exemplo, autodestruição caso seja utilizado pelo adversário.

7- Caso os equipamentos que constituem o SACC sejam afetados, estes têm capacidade para recuperar a sua funcionalidade?

8- Existem alternativas caso o sistema de comando e controlo falhe que permitam a continuidade da missão?

9- O Exército fornece algum tipo de formação que sensibilize os operadores deste tipo de sistema relativamente à temática de ciberdefesa/cibersegurança?

APÊNDICE B – Guião da Entrevista ao Major de Artilharia Elton Feliciano

ACADEMIA MILITAR

Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias

Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Guião de Entrevista ao Major de Artilharia Elton Feliciano

Lisboa, abril de 2019

Data: 22Abr19

Entrevistador: Aspirante de Artilharia Herculano Costa

Entrevistado: Elton Roque Feliciano

Posto: Major de Artilharia

Função: Discente do CEM-C 2018/19

Questões:

1- Quais os ativos*(assets)* que considera presentes na rede do SACC?
2- Como caracteriza a arquitetura do SACC?
3- Os operadores dos equipamentos são treinados arduamente de forma a que se evite que sejam introduzidos erros nos equipamentos ou que causem dano não intencional?
4- No que diz respeito ao campo cibernético, como caracteriza o adversário genérico atual?
5- Aquando a operação do SACC, a cibersegurança é tida em conta, ou o foco principal é a interoperabilidade dos equipamentos?
6- A certificação dos equipamentos (aprovamento da NATO, por exemplo) é tida em conta? Se sim, os equipamentos utilizados no SACC foram sujeitos a essa certificação?
7- Em algum momento as vulnerabilidades dos equipamentos foram identificadas?
8- Os equipamentos que constituem o SACC possuem proteções contra ameaças?
9- Os equipamentos que constituem o SACC têm capacidade de detetar que estão a ser alvos de um ciberataque?
10- Os equipamentos que constituem o SACC têm capacidade de responder a um ciberataque? Por exemplo, autodestruição caso seja utilizado pelo adversário.
11- Caso os equipamentos que constituem o SACC sejam afetados, estes têm capacidade para recuperar a sua funcionalidade?
12- Existem alternativas caso o sistema de comando e controlo falhe que permitam a continuidade da missão?
13- O Exército fornece algum tipo de formação que sensibilize os operadores deste tipo de sistema relativamente à temática de ciberdefesa/cibersegurança?

APÊNDICE C – Guião da Entrevista ao Capitão de Artilharia João Duarte Caeiro Chora

ACADEMIA MILITAR

Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias

Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Guião de Entrevista ao Capitão de Artilharia João Duarte Caeiro Chora

Lisboa, abril de 2019

Data: 17Abr19

Entrevistador: Aspirante de Artilharia Herculano Costa

Entrevistado: João Duarte Caeiro Chora

Posto: Capitão de Artilharia

Função: Cmdt CSV/AgrISTAR

Questões:

1- Quais os ativos*(assets)* que considera presentes na rede do SACC?
2- Como caracteriza a arquitetura do SACC?
3- Os operadores dos equipamentos são treinados arduamente de forma a que se evite que sejam introduzidos erros nos equipamentos ou que causem dano não intencional?
4- No que diz respeito ao campo cibernético, como caracteriza o adversário genérico atual?
5- Aquando a operação do SACC, a cibersegurança é tida em conta, ou o foco principal é a interoperabilidade dos equipamentos?
6- A certificação dos equipamentos (aprovamento da NATO, por exemplo) é tida em conta? Se sim, os equipamentos utilizados no SACC foram sujeitos a essa certificação?
7- Em algum momento as vulnerabilidades dos equipamentos foram identificadas?
8- Os equipamentos que constituem o SACC possuem proteções contra ameaças?
9- Os equipamentos que constituem o SACC têm capacidade de detetar que estão a ser alvos de um ciberataque?
10- Os equipamentos que constituem o SACC têm capacidade de responder a um ciberataque? Por exemplo, autodestruição caso seja utilizado pelo adversário.
11- Caso os equipamentos que constituem o SACC sejam afetados, estes têm capacidade para recuperar a sua funcionalidade?
12- Existem alternativas caso o sistema de comando e controlo falhe que permitam a continuidade da missão?
13- O Exército fornece algum tipo de formação que sensibilize os operadores deste tipo de sistema relativamente à temática de ciberdefesa/cibersegurança?

APÊNDICE D – Guião da Entrevista ao Tenente Coronel de Infantaria José Carlos Lourenço Martins

ACADEMIA MILITAR

Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias

Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Guião de Entrevista ao Tenente-Coronel de Infantaria José Carlos Lourenço Martins

Lisboa, abril de 2019

Data: 17Abr19

Entrevistador: Aspirante de Artilharia Herculano Costa

Entrevistado: José Carlos Lourenço Martins

Posto: Tenente-Coronel de Infantaria

Função: Docente na Academia Militar

Questões:

1- No que diz respeito a redes de comunicação, quais as medidas que considera mais importantes a ter em conta para que a rede esteja segura?
2- Como é que as empresas gerem a sua capacidade de serem ciber-resilientes?
3- De que forma é que as normas de padronização são importantes no que diz respeito à ciber-resiliência?
4- Qual é a importância da certificação dos equipamentos tanto para as empresas como no exército?

APÊNDICE E – Guião da Entrevista ao Coronel Tirocinado de Transmissões Jorge de Oliveira Ribeiro

ACADEMIA MILITAR

Ciber-resiliência nos sistemas de Comando e Controlo de Artilharia de Campanha

Autor: Aspirante de Artilharia Herculano Alexandre dos Reis Sanguinete Costa

Orientador: Major de Transmissões Luís Filipe Xavier Cavaco de Mendonça Dias

Coorientador: Major de Transmissões Tiago Filipe Abreu Moura Guedes

Guião de Entrevista ao Coronel Tirocinado de Transmissões Jorge de Oliveira Ribeiro

Lisboa, abril de 2019

Data: 23Abr19

Entrevistador: Aspirante de Artilharia Herculano Costa

Entrevistado: Jorge de Oliveira Ribeiro

Posto: Coronel Tirocinado de Transmissões

Função: Subdiretor da Direção de Comunicações e Sistemas de Informação

Questões:

1. Como interliga a DCSI com propostas de projetos associados à renovação do SACC?
2. Como é feita a certificação dos sistemas/equipamentos adquiridos?
3. Como faz o enquadramento do processo de aquisição do AFATDS e lições aprendidas?