ACADEMIA MILITAR

Engenharia Social na defesa: quadro conceptual, análise de riscos e estratégias de mitigação

Aspirante de Infantaria Lourenço Alberto de Faria Viana

Trabalho de Investigação Aplicada

Mestrado Integrado em Ciências Militares na Especialidade de Infantaria

Orientador: Professor José Alberto de Jesus Borges

Júri

Presidente do Júri: Professor Auxiliar João Paulo Neto Torres
Arguente: Tenente-Coronel de Infantaria Agostinho Amaral Valente
Orientador: Professor José Alberto de Jesus Borges
Diretor de Curso: Tenente-Coronel de Infantaria Comando Roberto Martins Mariano

junho, 2025

ACADEMIA MILITAR

Engenharia Social na defesa: quadro conceptual, análise de riscos e estratégias de mitigação

Aspirante de Infantaria Lourenço Alberto de Faria Viana

Trabalho de Investigação Aplicada

Mestrado Integrado em Ciências Militares na Especialidade de Infantaria

Orientador: Professor José Alberto de Jesus Borges

Júri

Presidente do Júri: Professor Auxiliar João Paulo Neto Torres
Arguente: Tenente-Coronel de Infantaria Agostinho Amaral Valente
Orientador: Professor José Alberto de Jesus Borges
Diretor de Curso: Tenente-Coronel de Infantaria Comando Roberto Martins Mariano

junho, 2025

EPÍGRAFE

“You could spend a fortune purchasing technology and services... and your network infrastructure could still remain vulnerable to old-fashioned manipulation.”

Kevin Mitnick

DEDICATÓRIA

À minha família, amigos e camaradas,

pelo apoio constante ao longo desta caminhada.

AGRADECIMENTOS

Durante esta trajetória, muitos foram os que me auxiliaram e apoiaram. Assim, é fundamental reconhecer a todos que, de alguma forma, contribuíram para o meu sucesso, apoiando e motivando-me ao longo destes anos.

A elaboração deste trabalho representa o ponto culminante da minha trajetória na Academia Militar, mas apenas foi possível graças ao apoio de várias pessoas, às quais expresso o meu mais sincero agradecimento.

Sou grato à minha família pelo apoio incondicional e por nunca deixarem de acreditar em mim.

Quero também reconhecer o Curso General Adolfo Almeida Barbosa pela paciência e motivação em todos os momentos.

Agradeço a todos os formadores e comandantes que me acompanharam durante minha formação.

Um agradecimento especial ao meu orientador pela constante disponibilidade em todas as fases do processo.

Por fim, agradeço a todos que, de maneira direta ou indireta, contribuíram para a realização deste trabalho.

RESUMO

A Engenharia Social representa uma ameaça significativa à segurança das organizações militares, devido à sua capacidade de explorar o comportamento humano para contornar mecanismos técnicos de defesa. Este trabalho investiga o impacto desta prática no setor da defesa, com especial foco nas vulnerabilidades associadas ao fator humano e na forma como estas podem comprometer a integridade das operações militares.

A investigação seguiu uma abordagem qualitativa, de natureza exploratória e descritiva, baseada na análise documental de literatura científica, relatórios institucionais e normativos de referência. Foi construído um quadro conceptual que sistematiza os principais conceitos ligados à Engenharia Social, nomeadamente as suas técnicas mais comuns, os fatores psicológicos explorados pelos atacantes e os contextos mais suscetíveis, como o das Forças Nacionais Destacadas. Os resultados demonstram que as estruturas militares permanecem vulneráveis a ataques de Engenharia Social, sobretudo devido à escassa integração do risco humano nas doutrinas de segurança e à ausência de formação sistemática. Identificaram-se ainda medidas de mitigação eficazes, como a sensibilização contínua, a aplicação de políticas de segurança e o reforço da literacia digital.

Conclui-se que a Engenharia Social deve ser encarada como uma ameaça estrutural e transversal, exigindo uma resposta integrada que valorize o comportamento humano como elemento central da segurança da informação militar.

Palavras-chave: Engenharia Social; Segurança da Informação; Fator Humano; Ciberdefesa; Defesa Nacional.

ABSTRACT

Social Engineering represents a significant threat to the security of military organizations, due to its ability to exploit human behavior to circumvent technical defense mechanisms. This paper investigates the impact of this practice in the defense sector, with a special focus on vulnerabilities associated with the human factor and how they can compromise the integrity of military operations.

The research followed a qualitative, exploratory and descriptive approach, based on documentary analysis of scientific literature, institutional reports and reference regulations. A conceptual framework was built that systematizes the main concepts linked to Social Engineering, namely its most common techniques, the psychological factors exploited by attackers and the most susceptible contexts, such as that of the Deployed National Forces. The results show that military structures remain vulnerable to social engineering attacks, mainly due to the lack of integration of human risk into security doctrines and the absence of systematic training. Effective mitigation measures were also identified, such as continuous awareness-raising, the application of security policies and the reinforcement of digital literacy.

The conclusion is that Social Engineering must be seen as a structural and transversal threat, requiring an integrated response that values human behavior as a central element of military information security.

Keywords: Social Engineering; Information Security; Human Factor; Cyberdefense; National Defense.

ÍNDICE GERAL

ÍNDICE DE FIGURAS

INDICE DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

A	
AM	Academia Militar
C	
CENTCOM	Comando Central dos Estados Unidos
CNCS	Centro Nacional de Cibersegurança
E	
EMGFA	Estado-Maior-General das Forças Armadas
ES	Engenharia Social
EUROPOL	Agência da União Europeia para a Cooperação Policial
F	
FA	Forças Armadas
FBI	Departamento Federal de Investigação dos Estados Unidos
N	
NATO	Organização do Tratado do Atlântico Norte
NIST	Instituto Nacional de Padrões e Tecnologia
NSA	Agência de Segurança Nacional dos Estados Unidos
O	
Oe	Objetivo específico
O_G	Objetivo geral
ONU	Organização das Nações Unidas
P	
PD	Pergunta derivada
PP	Pergunta de partida
Q	
QP	Questão de Partida
U	
UE	União Europeia

INTRODUÇÃO

A segurança da informação assume, no século XXI, um papel cada vez mais determinante na preservação da soberania dos Estados e na proteção das suas infraestruturas críticas. No seio das organizações militares, esta dimensão é especialmente sensível, dada a natureza estratégica das informações tratadas e o contexto de atuação em ambientes operacionais de elevado risco. As ameaças atuais à segurança deixaram de se limitar ao uso de força convencional, sendo hoje moldadas por fenómenos complexos, entre os quais se destacam os ataques de Engenharia Social (ES).

Figura 1: Kevin Mitnick, ex-hacker e referência mundial em ES, cuja trajetória ilustra a eficácia da manipulação comportamental como vetor de ataque..
Fonte: (*Ostec Security, 2023*).

Neste cenário, a ES desponta como uma das ameaças mais eficazes e insidiosas, explorando falhas humanas — em vez de falhas tecnológicas — para obter acesso não autorizado a dados, sistemas ou instalações. É uma técnica de manipulação psicológica e comportamental que tira partido de traços como a empatia, a curiosidade, a obediência à autoridade ou a urgência emocional. Estas práticas têm vindo a ser cada vez mais utilizadas por agentes hostis, tanto em campanhas de espionagem como em operações híbridas, que integram dimensões digitais, cognitivas e humanas.

O desenvolvimento de capacidades militares no domínio da ciberdefesa e da resiliência organizacional não pode prescindir de uma análise profunda do papel do fator humano como elo vulnerável na cadeia de segurança. O estudo da ES adquire, assim, um interesse acrescido no contexto militar, porquanto os militares operam sob hierarquias

estritas, em ambientes de elevada pressão psicológica, muitas vezes com elevado grau de confiança interpessoal e acesso a informação sensível. Tais fatores são frequentemente explorados por atacantes, tornando essencial uma cultura institucional que integre o risco humano como parte do ciclo de segurança da informação.

Neste enquadramento, o presente trabalho tem como objetivo geral avaliar a ES como instrumento crítico para a segurança da organização militar, desenvolvendo um quadro conceptual de referência para compreender e reconhecer as potencialidades e os riscos envolvidos. Para tal, analisam-se os perfis típicos das vítimas, os métodos utilizados pelos atacantes, o contexto específico das Forças Nacionais Destacadas (FND) e as estratégias institucionais de mitigação adotadas ou recomendadas.

A investigação adota uma abordagem qualitativa, com base na revisão da literatura especializada, documentos oficiais, relatórios de cibersegurança e estudos de caso, de forma a proporcionar uma compreensão abrangente e aplicável ao contexto nacional. Esta escolha metodológica justifica-se não apenas pela riqueza analítica da documentação existente, mas também pelas limitações de acesso a fontes militares classificadas e pela impossibilidade de realização de entrevistas operacionais.

A temática revela-se de grande pertinência estratégica, numa altura em que o ciberespaço se consolida como domínio operativo, ao lado do ar, mar, terra e espaço, e as ameaças à segurança nacional transcendem os limites físicos. Compreender a ES permite não apenas mitigar riscos internos, mas também reforçar a postura defensiva das Forças Armadas face a campanhas de desinformação, espionagem digital e operações psicológicas.

Ao integrar a perspetiva militar com os contributos da psicologia social, da sociologia do comportamento organizacional e da segurança da informação, esta dissertação procura contribuir para o desenvolvimento de uma cultura organizacional de segurança mais resiliente e consciente do papel determinante do fator humano. Deste modo, assume-se como de extrema importância avaliar a relevância da ES na defesa, não apenas enquanto fenómeno técnico, mas sobretudo enquanto ameaça estratégica centrada no comportamento humano.

Neste contexto, torna-se essencial clarificar o problema que orienta a presente investigação. Como refere Rosado (2017), a Questão de Partida (QP) constitui o eixo estruturante do estudo, uma vez que dirige o olhar do investigador e delimita o campo de análise. Assim, formula-se a seguinte:

Qual o impacto da Engenharia Social como uma ferramenta crítica para a segurança da organização militar, considerando as suas potencialidades e os riscos envolvidos?

Esta questão procura enquadrar o fenómeno da ES no domínio da segurança organizacional militar, partindo do pressuposto de que as ameaças não se restringem ao plano técnico, mas estão fortemente enraizadas na dimensão comportamental dos indivíduos.

De forma a dar resposta a esta questão, definem-se os propósitos da investigação através dos respetivos objetivos. Defende (Fortin, 2009, p. 100) que "o objetivo de um estudo indica o porquê da investigação", sendo então estabelecido o seguinte:

Objetivo Geral (OG): Avaliar a ES como instrumento crítico para a segurança da organização militar, desenvolvendo um quadro conceptual de referência para compreender e reconhecer as potencialidades e os riscos envolvidos.

Objetivos Específicos (OE):

OE1: Desenvolver um quadro conceptual abrangente para a compreensão da ES;

OE2: Analisar os impactos da ES numa FND;

OE3: Identificar estratégias de mitigação de riscos para enfrentar as ameaças da ES.

Ao estudar esta temática, pretende-se, tendo em conta as tipologias de ataques de ES identificadas e a eficácia das medidas de mitigação implementadas, apurar se o modelo atual de proteção da informação e de sensibilização no contexto militar se revela eficaz e, idealmente, propor estratégias operacionais e formativas mais ajustadas à realidade das ameaças contemporâneas.

PARTE I – REVISÃO DE LITERATURA

CAPÍTULO 1 – REVISÃO DE LITERATURA

A ES é uma técnica com fundamentos na psicologia, utilizada para manipular indivíduos através da exploração de vulnerabilidades humanas, como a confiança, a curiosidade, o medo ou a desatenção. O seu objetivo pode variar desde a obtenção de informações confidenciais até à indução de comportamentos ou ações que comprometam a segurança de forma abrangente. Trata-se de uma abordagem sofisticada e subtil que, embora frequentemente associada a ataques à segurança da informação, também encontra aplicação em outros contextos, como o marketing, a política e a espionagem. Apesar de não depender diretamente de falhas tecnológicas, pode ser combinada com ferramentas tecnológicas para amplificar os seus efeitos. Esta prática capitaliza nas fragilidades humanas com o intuito de alcançar objetivos, muitas vezes, de natureza maliciosa. A ES pode ser definida como "a arte de enganar pessoas para obter informações confidenciais" (Mitnick & Simon, 2002).

A ES não é um conceito novo. Existe desde que os humanos existem. As suas raízes remontam a séculos atrás, onde são utilizadas técnicas de manipulação e persuasão onde já eram usadas para enganar adversários ou obter vantagens em prol do próprio bem-estar. A sua expressão foi originalmente nomeada por Karl Popper, em 1945, no contexto da Filosofia e Sociologia para descrever a tentativa de manipular e controlar o comportamento humano através de políticas sociais (Popper, 1945). No entanto, foi na década de 1980 que o termo "Engenharia Social" começou a ser associado à segurança de informação, particularmente com a ascensão dos computadores e das redes. Contudo, com a chegada da era digital, a ES evoluiu significativamente, tornando-se uma das principais ameaças à segurança cibernética. Durante as décadas de 1960 e 1970, a ES começou a ganhar especial atenção com a prática de "phone phreaking", isto é, os indivíduos manipulavam sistemas telefónicos para fazer chamadas gratuitas. A conscientização sobre este tema aumentou significativamente nas décadas de 1980 e 1990, impulsionada por hackers como Kevin Mitnick e, sendo este um artigo sobre ES, não estaria completo sem vos apresentar Kevin como um dos hackers mais famosos do mundo que mais tarde escreveu "The Art of Deception" (2002), onde era conhecido pelas suas habilidades em manipular pessoas para obter informações confidencias. Kevin tornou-se uma lenda no mundo do *hacking* devido às suas invasões em sistemas de grandes empresas de tecnologia e telecomunicações onde "*hackeou"* manipulou redes de empresas como a Nokia, a Fujitsu ou a Motorola. Esteve preso várias vezes, foi alvo de uma perseguição federal massiva e esteve ainda na lista dos mais procurados do FBI por

hacking e fraude de computadores. Após todas estas peripécias, reformou-se e passou a trabalhar como consultor de segurança cibernética o que mais tarde lhe potenciou a fundação da sua própria empresa "Mitnick Security Consulting, LLC", onde utilizou toda as suas experiências para ajudar as empresas e organizações a melhorar as suas defesas contra-ataques de ES e cibernéticos. A sua capacidade de enganar pessoas e obter acesso a informações confidenciais sem o uso de tecnologia avançada foi o que o distinguiu como um mestre em ES onde o seu legado remonta para uma lembrança contínua de que a segurança cibernética não se trata apenas de proteger máquinas, mas também de proteger as pessoas que as utilizam.

Os "agressores" atacam através de métodos não técnicos, ou seja, como uma forma de *hacking* "sem tecnologia", ao invés de explorar aquilo que são falhas nos sistemas de segurança, os "agressores" exploram falhas no comportamento humano. Granger (2001) define a ES como "qualquer ato que influencie uma pessoa a tomar uma ação que pode ou não estar nos seus melhores interesses" (Granger, 2001). Em vez de forçar o sistema, o Engenheiro Social força o utilizador, persuadindo-o a abrir portas que, em condições normais, estariam protegidas por mecanismos técnicos. A ES baseia-se em princípios psicológicos como a autoridade, a escassez, a reciprocidade, a familiaridade ou o medo, com o intuito de induzir a vítima a comportamentos automáticos e pouco críticos (Cialdini, 2001). Os atacantes exploram a tendência natural dos indivíduos para ajudar, confiar e agir rapidamente perante estímulos urgentes ou emocionais. É por isso que este tipo de ataque é muitas vezes difícil de detetar, pois a sua eficácia reside precisamente na naturalidade da resposta da vítima. Para além disso, os métodos evoluíram significativamente, acompanhando os avanços tecnológicos e os novos canais de comunicação, como redes sociais, aplicações móveis ou plataformas de mensagens instantâneas (Hadnagy, 2018).

Um dos modelos mais completos sobre a estrutura interna de um ataque de ES é o proposto por Gomes e Motta (2024), baseado nos trabalhos de Wang et al. (2021). Este modelo — representado na Figura 2— apresenta o ataque como a articulação entre dois prismas: o do atacante e o da vítima. No primeiro, o atacante define o objetivo e cria o método de ataque, que se realiza através da manipulação da ação. No segundo, a vítima possui uma vulnerabilidade humana, que é explorada para alcançar a consequência desejada. O mecanismo central do ataque reside na exploração da ação, ou seja, o espaço simbólico e comportamental onde decorre a manipulação. Esta representação reforça o carácter interativo e psicológico da ES, bem como, destaca o fator humano como elo crítico da segurança organizacional.

Figura 2: Mecanismo da Engenharia Social

Fonte: Adaptado de Wang et al. (2021), conforme apresentado em (*Gomes & Motta, 2024*).

1.1.Perfis das vítimas e alvos típicos da Engenharia Social

A eficácia da ES reside, em grande medida, na sua capacidade de adaptar o ataque ao perfil comportamental, psicológico e funcional da vítima. Os alvos são escolhidos não apenas com base no seu nível de acesso ou posição hierárquica, mas também na forma como interagem com o ambiente — seja presencialmente ou através de meios digitais. Essa distinção é essencial para compreender a amplitude das ameaças e formular estratégias de defesa adequadas a diferentes contextos organizacionais.

Os métodos utilizados pelos atacantes variam significativamente consoante o tipo de contacto estabelecido com a vítima. Como se apresenta na Figura 2, é possível distinguir duas grandes categorias de técnicas de ES: as que implicam contacto direto com o alvo (face a face ou físico) e as que se realizam sem qualquer contacto presencial, utilizando meios remotos ou digitais (Liu, Wang, Li & Chandel, 2017). Ataques com contacto direto incluem práticas como o *tailgating* — em que o atacante se faz passar por um membro da organização para aceder fisicamente a instalações — ou o *pretexting* presencial, em que se assume uma identidade falsa com autoridade reconhecida (por exemplo, auditor, técnico de manutenção ou militar superior). Já os métodos sem contacto direto, como o *phishing*, o *vishing* (via telefone) e o *smishing* (via SMS), baseiam-se no uso de canais tecnológicos para enganar a vítima à distância, explorando fatores como a urgência ou a obediência à autoridade.

A importância desta distinção ganha relevo particular no contexto militar, onde tanto os ambientes altamente hierarquizados como as missões em terreno hostil expõem os operacionais a riscos variados. Por exemplo, nas FND, a presença física em zonas urbanas

instáveis pode facilitar o uso de técnicas de contacto direto, enquanto o uso de comunicações não seguras permite a exploração remota. Reconhecer estas dinâmicas permite antecipar os pontos críticos de vulnerabilidade e definir contramedidas proporcionais à natureza da ameaça.

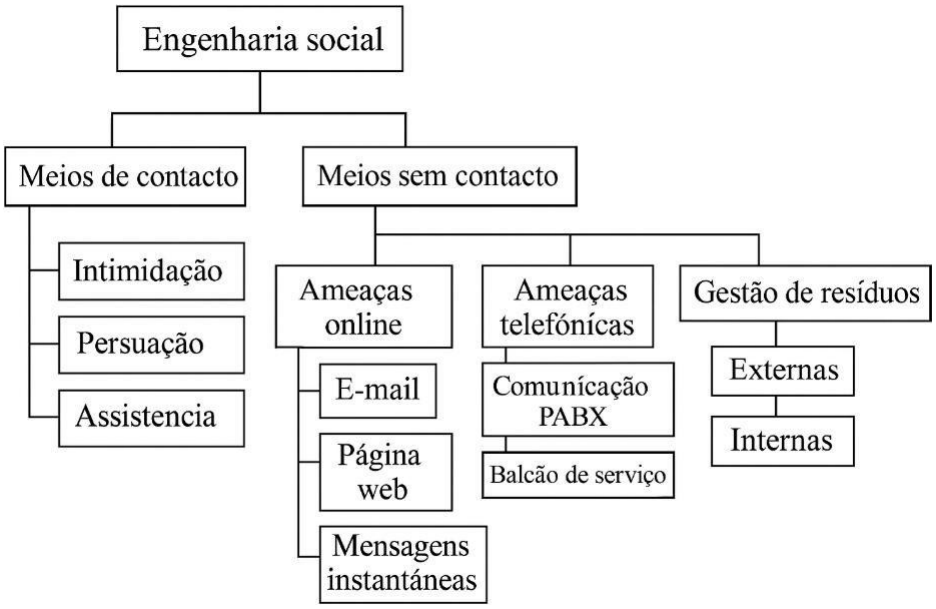

Figura 3: Classificação dos ataques de Engenharia Social com base no tipo de contacto entre o atacante e a vítima: com contacto direto e sem contacto direto.
Fonte: Adaptado de Liu, Y., Xiangyu, W., LI, T., & Chandel, a. (2017).

A Figura 3, adaptada de Liu et al. (2017) descreve a classificação dos ataques de Engenharia Social com base no tipo de contacto entre o atacante e a vítima: com contacto direto e sem contacto direto. Esta categorização reforça a noção de que não existe um perfil único de vítima, mas sim diferentes graus de exposição conforme o seu papel, rotina e canais de comunicação utilizados. Por conseguinte, torna-se necessário aprofundar a análise de vítimas genéricas e vítimas estratégicas, tal como se explorará nas subsecções seguintes.

1.2 Vítimas genéricas

Neste grupo incluem-se colaboradores de organizações que não desempenham funções críticas, mas que, por estarem ligados à rede ou ao ecossistema interno, podem funcionar como ponto de entrada para ataques mais complexos (*pivoting*). São frequentemente alvos de campanhas de *phishing* ou *baiting*, em que os atacantes recorrem a mensagens enganosas, ficheiros maliciosos ou links fraudulentos para induzir comportamentos automáticos, como o clique num link ou o download de um anexo

(Hadnagy, 2018). Estas campanhas são disseminadas em massa e aproveitam-se da rotina e da confiança excessiva no ambiente digital do trabalho.

1.3 Vítimas específicas ou estratégicas

Estas vítimas são cuidadosamente selecionadas com base no seu nível de acesso, posição hierárquica ou papel institucional. A este fenómeno chama-se *whaling* ou spear *phishing*, e visa indivíduos com acesso privilegiado a informação sensível, como oficiais superiores, responsáveis pela segurança da informação, operadores de sistemas críticos, pessoal de recursos humanos (acesso a dados pessoais) ou até familiares de militares em funções estratégicas (Clarke & Knake, 2019).

Nestes casos, o atacante pode investir semanas ou meses a estudar rotinas, redes sociais, organogramas e padrões de comportamento da vítima, de modo a construir um cenário de ataque verosímil. Esta abordagem é particularmente eficaz quando o atacante finge ser um superior hierárquico, um técnico interno ou um colaborador externo de confiança, explorando o respeito pela autoridade e a urgência na resposta — dois traços típicos das organizações militares (Mitnick & Simon, 2002).

1.4 Características comuns das vítimas

Apesar da sofisticação crescente das técnicas de ES, a sua eficácia continua profundamente dependente de vulnerabilidades humanas recorrentes. Independentemente do nível hierárquico ou da função específica, certas características pessoais, comportamentais e contextuais tornam os indivíduos particularmente suscetíveis à manipulação. Esta constatação é confirmada por diversos estudos que reconhecem o fator humano como o elo mais fraco da cadeia de segurança (Clarke & Knake, 2019; Hadnagy, 2018). As vítimas de ataques de ES, embora possam ser de qualquer perfil, partilham frequentemente traços que as tornam alvos mais prováveis. Uma das vulnerabilidades mais comuns é o baixo nível de literacia digital ou de formação em cibersegurança. Indivíduos que desconhecem práticas básicas de proteção — como verificação de remetentes, uso de senhas seguras ou políticas de acesso — estão mais propensos a ceder a pedidos fraudulentos, especialmente quando estes apelam à autoridade ou à urgência. Outro fator relevante é o excesso de confiança nos procedimentos internos e nas estruturas hierárquicas. No contexto militar, onde a cadeia de comando é profundamente enraizada na cultura organizacional, a tendência para obedecer a

ordens ou instruções sem questionamento crítico pode ser explorada por atacantes que se façam passar por superiores. Este comportamento está alinhado com os princípios de persuasão descritos por Cialdini (2001), como a autoridade e a consistência.

O isolamento funcional também representa uma fragilidade. Militares destacados em postos remotos, sentinelas ou operadores de sistemas críticos que trabalham sozinhos tendem a ser mais vulneráveis por falta de supervisão direta e ausência de apoio imediato para validação de informações suspeitas. Além disso, rotinas altamente padronizadas, como horários fixos de verificação, patrulhamento ou acesso a sistemas, facilitam a previsibilidade, que é um recurso essencial para a preparação de ataques direcionados. A exposição descuidada em redes sociais constitui outra vulnerabilidade frequentemente explorada. A partilha pública de informações como localizações, funções, nomes de colegas ou datas de missões, pode fornecer aos atacantes dados suficientes para montar ataques personalizados (*spear phishing*) ou assumir identidades falsas com alto grau de verosimilhança. Conforme Mitnick e Simon (2002) salientam, os Engenheiros Sociais são peritos em transformar detalhes aparentemente inocentes em armas de manipulação. A pressão emocional ou operacional também contribui para o sucesso destes ataques. Quando sujeitos a stress, fadiga ou prazos apertados, os indivíduos tendem a reduzir o pensamento crítico e recorrem a respostas automáticas — o que favorece decisões impulsivas e irrefletidas, como clicar num link malicioso ou fornecer credenciais por telefone. Este fenómeno é explicado pela psicologia cognitiva, que demonstra como o cérebro humano recorre a atalhos heurísticos em contextos de carga mental elevada (Kahneman, 2011). Estas características estão interligadas e raramente surgem de forma isolada. A Figura 2 ilustra este princípio, apresentando um modelo conceptual que relaciona os diferentes tipos de vulnerabilidades humanas com os mecanismos de ataque e os métodos mais frequentemente utilizados. Como se observa, vulnerabilidades cognitivas, emocionais, comportamentais e psicológicas são exploradas por táticas específicas de manipulação — como autoridade, persuasão ou exploração emocional — que, por sua vez, são operacionalizadas através de técnicas como *phishing*, *baiting*, *pretexting* ou *tailgating* (Wang, Zhu & Sun, 2021).

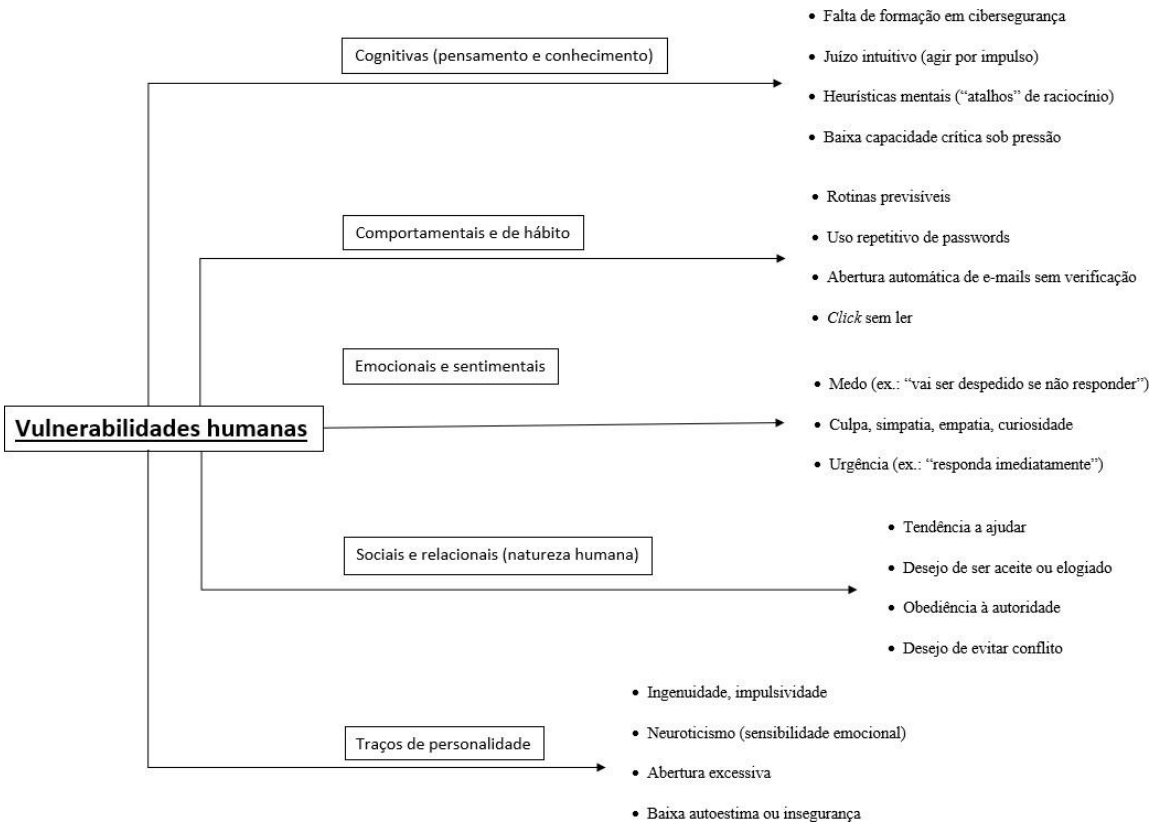

Figura 4: Modelo conceptual de ES: vulnerabilidades humanas.
Fonte: Adaptado de Wang, Z., Zhu, H. & Sun, L. (2021).

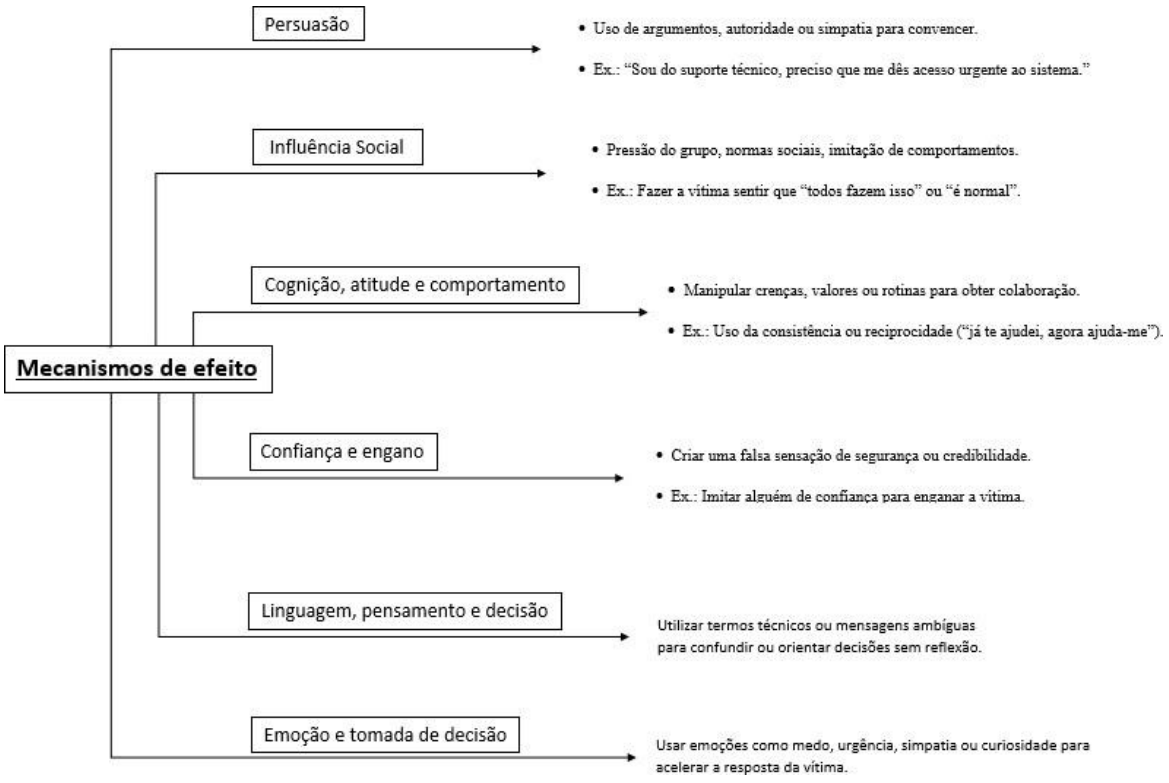

Figura 5: Modelo conceptual de ES: mecanismos de efeito.
Fonte: Adaptado de Wang, Z., Zhu, H. & Sun, L. (2021).

Este modelo, apresentado na Figura 4 e Figura 5, reforça a ideia de que a ES não depende exclusivamente de falhas tecnológicas, mas sim de padrões comportamentais previsíveis e vulnerabilidades emocionais. No caso das organizações militares, estas características devem ser cuidadosamente monitorizadas e integradas nos programas de formação e mitigação. Reforçar a capacidade de reconhecimento de sinais de manipulação e treinar respostas críticas diante de situações atípicas são medidas essenciais para transformar o fator humano — de elo mais fraco para primeira linha de defesa.

1.5 Ciclo de ataque

Para aprofundar todo este processo de ataque, é útil dissecar como um ataque de ES se desenrola e porque funciona, do ponto de vista psicológico. Em termos de ciclo de ataque, muitos autores descrevem etapas sequenciais que os atacantes seguem. Uma divisão comum identifica quatro fases principais:

1.5.1 Reconhecimento

Entende-se por Reconhecimento como as atividades de Recolha/Pesquisa de Informações. O Engenheiro Social reúne o máximo de dados sobre o alvo antes de iniciar o contacto. Isto inclui pesquisar nas redes sociais, sites oficiais, notícias e até lixo (prática conhecida como *dumpster diving*) em busca de informações que ajudem a personalizar o ataque. No contexto militar, pode significar identificar nomes de membros da unidade, cargos, rotina, familiares, locais de destacamento, etc.

1.5.2 Desenvolvimento de Relacionamento

Nesta fase, o atacante estabelece contato com a potencial vítima e procura ganhar a sua confiança. Pode ser uma interação única (por exemplo, um email convincente) ou um processo mais prolongado (por exemplo, conversas online ao longo de dias/semanas, criação de perfil falso que interage com a vítima). O pretexto criado é crucial aqui – o atacante apresenta-se como alguém com quem a vítima naturalmente cooperaria (um colega, um técnico, um conhecido, ou simplesmente alguém amigável e com interesses em comum).

1.5.3 Exploração

Uma vez obtida a confiança, o atacante explora a vítima, induzindo-a efetivamente a realizar a ação desejada. Esta é a etapa crítica em que a vítima, por exemplo, fornece a informação confidencial solicitada, clica no link malicioso, insere a *pen* USB desconhecida no computador da rede ou abre a porta de acesso ao suposto funcionário. Tudo depende do objetivo: pode ser roubo de credenciais, acesso físico, etc. O sucesso desta fase é o objetivo do atacante.

1.5.4 Encerramento

Após conseguir o que deseja, o Engenheiro Social procura encerrar a interação sem levantar suspeitas e, muitas vezes, eliminar vestígios. No mundo digital, isso pode significar apagar contas falsas, cessar comunicações repentinamente ou encerrar sessões de acesso. No mundo real, pode ser simplesmente sair rapidamente após obter acesso, ou extrair-se de uma conversa antes que a vítima perceba algo. Essa fase inclui frequentemente medidas de contrainteligência, como instruir a vítima a não contar a ninguém (sob algum pretexto) ou criar distrações para atrasar a descoberta do ataque. Em certos casos, o atacante "queima" a identidade falsa usada, desaparecendo por completo após atingir o propósito.

1.5.5 Síntese

Na primeira etapa, o atacante recolhe informações detalhadas sobre a vítima (como cargos, hábitos e redes sociais); depois, estabelece contacto direto com o alvo, ganhando a sua confiança por meios persuasivos. Numa terceira fase, induz a vítima a tomar ações desejadas — como revelar dados ou abrir acessos — culminando na última etapa, onde se concretiza o objetivo do ataque (Internos Group, 2021). Este modelo cíclico ilustra como as interações interpessoais e a exploração de princípios psicológicos podem ser sistematicamente utilizadas para comprometer a segurança da informação em ambientes organizacionais, inclusive no setor da defesa.

Figura 6: Ciclo de um ataque de ES, com quatro fases: reconhecimento, relacionamento, exploração e execução. Fonte: Adaptado de Internos Group (2021).

Este ciclo, representado na Figura 6, pode variar em duração e complexidade conforme o ataque. Alguns ataques de *phishing* em massa condensam essas etapas numa simples interação (email e clique imediato). Já ataques sofisticados contra alvos militares importantes podem envolver semanas de reconhecimento e cultivo da relação (por exemplo, um agente inimigo faz amizade online com um militar numa base destacada, trocando mensagens inocentes por algum tempo antes de fazer qualquer pedido suspeito).

1.6 Princípios psicológicos

A eficácia da ES assenta, em última instância, em princípios psicológicos universais. Estudos de psicologia social e do comportamento identificaram vários fatores de persuasão

que tornam as pessoas mais propensas a ceder a pedidos, mesmo contra melhor juízo. Um conjunto famoso de princípios é o proposto por Robert Cialdini, psicólogo comportamental, que elencou sete princípios de influência frequentemente explorados por fraudadores.

1.6.1 Reciprocidade

Tendência a querer retribuir favores. Um atacante pode oferecer algo (ajuda, um presente ou mesmo uma demonstração de camaradagem) para depois esperar que a vítima "devolva" o favor fornecendo informação ou acesso (explorando o incómodo que sentimos em ficar em dívida para com alguém).

1.6.2 Compromisso e Consistência

As pessoas tendem a manter coerência com compromissos assumidos. Um Engenheiro Social pode conseguir que a vítima diga ou faça algo inicialmente insignificante, mas que a comprometa a uma narrativa, e então, explorar esse compromisso para pedidos maiores (*foot-in-the-door*). Por exemplo, conseguir que um militar numa base preencha uma breve "pesquisa" (falsa) sobre segurança; tendo feito isso, ele pode sentir-se compelido a colaborar mais quando solicitado, para ser consistente.

1.6.3 Prova Social

Indivíduos seguem o comportamento do grupo, especialmente em situações de incerteza. Se um atacante conseguir dar a entender que "todos os colegas já aderiram" a certa iniciativa ou regra (falsa), a vítima poderá ceder por pressão de conformidade. No contexto militar hierarquizado, a ideia de que outros pares ou superiores já fazem algo pode ser um motivador potente.

1.6.4 Autoridade

Pessoas tendem a obedecer figuras de autoridade ou especialistas. Este princípio é explorado diretamente em pretextos onde o atacante finge ser alguém em posição de autoridade (um comandante, um oficial de segurança, um representante de uma instituição respeitável). A vítima, condicionada a não questionar autoridades, cumpre instruções mesmo que anômalas, por deferência.

1.6.5 Afeição/Simpatia

É mais provável dizermos "sim" a quem gostamos. Atacantes podem construir uma ligação com a vítima, demonstrando afinidades, elogios ou outros laços emocionais.

Alternativamente, usam perfis atraentes (no caso de *catfishing*, explorando atratividade romântica) para baixar as defesas do alvo. A operação de *catfishing* conduzida pelo Hamas contra soldados israelitas é exemplo disso – ao fingirem interesse romântico, criaram afeição para então explorar os soldados.

1.6.6 Escassez

Valorizamos mais aquilo que é apresentado como raro ou com disponibilidade limitada. Atacantes aplicam pressão de tempo ("última oportunidade", "urgente!") ou exclusividade ("informação confidencial, só para si") para forçar decisões rápidas, impedindo a vítima de refletir ou consultar outros. Essa urgência explorada é visível em muitos esquemas ("responda imediatamente ou perderá acesso", etc.).

1.6.7 Unidade

Princípio mais recentemente descrito, refere-se à nossa tendência de sermos influenciados por quem percebemos como pertencendo ao mesmo grupo ou identidade que nós (seja família, organização, pátria, etc.). Num contexto militar, sentimentos de camaradagem ou patriotismo podem ser explorados: um atacante que se faça passar por "companheiro de farda" ou aliado nacional poderá obter confiança extra. Como notado em análise recente, quando sentimos alguém como parte do nosso grupo, ficamos mais suscetíveis à persuasão por essa pessoa.

1.6.8 Síntese

Estes princípios frequentemente atuam em conjunto durante um ataque de ES. Por exemplo, num simples email de *phishing*, pode haver linguagem de autoridade ("Departamento de TI ordena mudança de senha imediatamente"), combinada com urgência (escassez de tempo para evitar bloqueio de conta) e talvez indicação de que "todos estão atualizando as senhas" (prova social), tudo isto para induzir o clique imediato.

Desta forma, ES constitui-se num quadro conceptual interdisciplinar, englobando tecnologia, psicologia e contexto social. A literatura assinala que a compreensão dos mecanismos psicológicos é tão importante quanto conhecer as técnicas tecnológicas envolvidas, pois a essência da ameaça reside na exploração do comportamento humano. Com esta base teórica estabelecida – definindo o que é ES, quais as suas modalidades e porque funciona – passamos a analisar como essa ameaça se manifesta no contexto militar, particularmente no caso das FND, e quais riscos concretos proporciona.

CAPÍTULO 2 – ENGENHARIA SOCIAL EM AMBIENTE MILITAR

A presença da ES no domínio militar representa uma ameaça séria, crescente, persistente, de difícil deteção e sofisticada. Ao explorar não as falhas tecnológicas, mas as vulnerabilidades humanas dentro de estruturas altamente hierarquizadas e operacionais, os ataques de ES revelam-se particularmente eficazes em contextos onde a confiança, a obediência e a rotinização de procedimentos são características funcionais. Esta realidade coloca em causa a segurança da informação, a proteção de operações sensíveis e, em casos mais graves, a própria integridade da cadeia de comando e das missões militares, visto que os ambientes militares são caracterizados por estruturas hierárquicas rígidas, confiança institucionalizada e pressão operacional onde estas técnicas podem ter consequências particularmente perigosas.

Um estudo realizado por Shahrom et al. (2021) identificou nove fatores que afetam a defesa contra-ataques de ES no ambiente militar: autoridade, reciprocidade, compromisso e consistência, difusão de responsabilidade, escassez, simpatia, consciência, prova social e confiança. Estes fatores refletem princípios psicológicos que podem ser explorados por atacantes para manipular comportamentos e decisões de membros das Forças Armadas (FA). O ambiente militar é, por natureza, um ecossistema altamente estruturado, disciplinado e orientado para a execução rápida de ordens. Estas características, que são essenciais para a eficácia operacional, constituem simultaneamente pontos de exposição a ataques de ES. Técnicas como *pretexting* (assumir uma identidade falsa), *spear phishing* (envio de comunicações fraudulentas personalizadas) ou *baiting* (oferta de dispositivos maliciosos) podem ser adaptadas a cenários militares com notável sucesso, principalmente quando visam elementos com funções administrativas, logísticas ou ligadas à tecnologia da informação (Hadnagy, 2018; Clarke & Knake, 2019).

O fator humano permanece o elo mais fraco da segurança organizacional, e no contexto das FA essa fragilidade adquire contornos críticos. De acordo com o Relatório de Riscos e Conflitos 2022 do CNCS, 43% dos incidentes reportados em Portugal estão associados a ataques de ES, com destaque para técnicas de *vishing* e *phishing* altamente direcionadas (CNCS, 2022). Ainda que o relatório não desagregue especificamente os dados relativos ao setor militar, as implicações para as FA são claras, dado o nível de sensibilidade das informações em causa e o potencial impacto estratégico de uma violação de segurança. As campanhas de desinformação, muito comuns em contextos de guerra híbrida, têm também uma componente de ES, ao manipular militares e civis através de redes sociais,

plataformas digitais e aplicações de comunicação. Em 2022, um relatório da EUROPOL identificou casos em que perfis falsos foram utilizados para estabelecer contacto com membros de FA de países europeus, simulando interesse pessoal ou profissional com o objetivo de extrair informações sobre deslocações, horários, operações ou acessos físicos a instalações (EUROPOL, 2021). Outro aspeto relevante prende-se com as operações destacadas no estrangeiro, conhecidas como FND. Nessas missões, as vulnerabilidades aumentam devido ao isolamento, à pressão das operações no terreno e à exposição a ambientes culturais e tecnológicos distintos. Nessas circunstâncias, agentes hostis — estatais ou não estatais — podem recorrer à ES para infiltrar pessoal local, explorar relações interpessoais ou manipular emoções, com o fim de recolher dados operacionais ou influenciar decisões táticas. Tal como aponta Mitnick (2002), o Engenheiro Social é "um mestre na arte de fazer as pessoas esquecerem a cautela", e isso pode ser especialmente perigoso em contextos operacionais de elevada exigência psicológica.

A presente investigação, embora ancorada numa análise conceptual e documental, não pode ser dissociada do contexto operacional concreto onde os riscos associados à ES se materializam. As FND operam frequentemente em teatros de operação marcados por instabilidade política, conflito armado, fragilidade institucional e elevada pressão psicológica. Interagem com uma multiplicidade de atores e enfrentam dinâmicas multiculturais e linguísticas, fatores que, combinados com o desgaste emocional das missões prolongadas, aumentam o risco de exposição a manipulação. A rotinização de procedimentos logísticos e operacionais oferece oportunidades de exploração por parte de agentes hostis. A quebra de vigilância psicológica, a confiança interpessoal com elementos externos ou a perceção de normalidade podem levar à partilha indevida de informação sensível. As redes sociais, por sua vez, continuam a ser uma via privilegiada para a recolha passiva de informação e campanhas de engenharia de perfil, sendo comum a utilização de perfis falsos, engenharia de género e falsos interesses românticos para obter dados operacionais. Apesar do reconhecimento da ameaça, a integração sistemática da ES nos programas de formação militar e nos manuais de segurança ainda é, em muitos países, incipiente. No caso português, embora existam doutrinas sobre segurança da informação e protocolos de ciberdefesa definidos pelo EMGFA, as medidas permanecem centradas sobretudo em aspetos técnicos, como *firewalls*, encriptação ou antivírus. A proteção contra ES continua pouco estruturada em termos de prevenção e treino sistemático.

Desta forma, torna-se imperativo que a ES seja compreendida como uma ameaça multidimensional, que requer uma resposta integrada: reforço da literacia digital, treino

baseado em simulações realistas (ex. campanhas simuladas de *phishing*), criação de canais de reporte rápido, e o desenvolvimento de uma cultura organizacional centrada na responsabilidade partilhada pela segurança. A doutrina de segurança nacional deverá, nesse sentido, evoluir no sentido de valorizar o papel do comportamento humano como componente central da defesa nacional — e não apenas como uma fragilidade residual. Reforçar as capacidades de defesa contra esta ameaça requer uma abordagem holística, que combine treino, doutrina, liderança consciente e cultura institucional de segurança.

CAPÍTULO 3 – ENGENHARIA SOCIAL NO CONTEXTO DA DEFESA

A evolução das ameaças à segurança nacional no século XXI tem evidenciado a crescente relevância de técnicas que transcendem o domínio físico, operando nos planos cognitivo e informacional. A ES, neste contexto, impõe-se como uma ferramenta crítica, empregada não apenas por cibercriminosos individuais, mas também por atores estatais e não estatais com objetivos estratégicos. A sua aplicação no setor da defesa tem vindo a aumentar, especialmente no âmbito da espionagem, sabotagem, operações psicológicas e campanhas de desinformação — todas com potencial para comprometer a integridade de estruturas militares e a eficácia operacional. Ao contrário de outras formas de intrusão cibernética que se apoiam em vulnerabilidades técnicas, a ES explora características humanas como a confiança, a autoridade, a urgência e a necessidade de pertença. A sua eficácia reside na capacidade de manipular emoções, perceções e decisões, contornando sistemas técnicos através da interação direta com os utilizadores. Como tal, representa uma ameaça assimétrica particularmente perigosa em organizações fortemente hierarquizadas e orientadas para a execução de ordens, como é o caso das Forças Armadas.

De acordo com o NATO CCDCOE (2019), a ES é frequentemente utilizada para obter acesso inicial a redes seguras, sendo vista como um vetor de ataque inicial em operações de intrusão. Este tipo de abordagem, combinada com técnicas de *spear phishing*, *pretexting* ou *watering hole*, permite infiltrar sistemas aparentemente protegidos, acedendo a informação sensível sem deixar vestígios tecnológicos evidentes. O impacto desta estratégia é exponenciado quando os alvos ocupam funções críticas em áreas como logística, comunicações, inteligência ou comando tático.

A ES é igualmente uma ferramenta central nas chamadas operações de influência — campanhas dirigidas a manipular a perceção de públicos-alvo, moldar comportamentos ou semear desconfiança entre aliados. Estas operações recorrem, com frequência, à disseminação de desinformação nas redes sociais, aproveitando algoritmos de distribuição de conteúdo e padrões de consumo emocional para amplificar mensagens falsas. Ao explorar preconceitos, divisões internas ou temas sensíveis, estas campanhas visam comprometer a coesão institucional, fragilizar o moral das tropas ou influenciar decisões políticas e estratégicas.

Exemplos práticos comprovam a eficácia da ES em contextos de defesa. O caso de Edward Snowden, antigo prestador de serviços da NSA, é paradigmático. Snowden não recorreu a sofisticadas técnicas de *hacking* para aceder a dados classificados; convenceu colegas a cederem as suas credenciais, usando argumentos credíveis e uma imagem de fiabilidade. Esta manipulação interpessoal, centrada na exploração da confiança profissional, permitiu-lhe recolher e divulgar vastas quantidades de informação sensível, com repercussões globais na segurança e reputação dos serviços de inteligência norte-americanos. Outro caso emblemático ocorreu em janeiro de 2015, quando ciberatacantes associados ao Estado Islâmico comprometeram as contas de redes sociais do Comando Central dos Estados Unidos (CENTCOM). Embora a intrusão tenha ocorrido em plataformas públicas, a credibilidade simbólica da operação — ao conseguir transmitir mensagens e propaganda usando canais oficiais — demonstrou a vulnerabilidade da perceção pública e a eficácia da ES como arma psicológica. Mais recentemente, investigações conduzidas pela EUROPOL (2021) e pela NATO identificaram padrões de ataque envolvendo perfis falsos em redes sociais, utilizados para se aproximar de militares europeus. Nesses casos, as abordagens não visavam diretamente os sistemas informáticos, mas sim o estabelecimento de relações interpessoais — por vezes de cariz afetivo ou profissional — com o intuito de obter informações sobre operações, deslocações ou acessos a instalações. Tais técnicas demonstram a capacidade adaptativa da ES ao ambiente digital contemporâneo e a sua adequação ao contexto militar, onde a partilha de rotina ou desatenção pontual podem comprometer toda uma missão.

Importa referir que, apesar do crescente reconhecimento da ameaça, a integração da ES na doutrina de segurança e defesa ainda é desigual. Em muitos países, incluindo Portugal, a resposta institucional permanece fortemente centrada na componente técnica da cibersegurança, com investimentos em encriptação, *firewalls*, antivírus e monitorização de redes. No entanto, o fator humano — o mais explorado pela ES — continua a ser o elo mais vulnerável e o menos sistematicamente abordado em termos de treino, doutrina e responsabilização. Nesse sentido, é necessário que a ES deixe de ser vista apenas como um risco complementar ou colateral e passe a integrar as dimensões nucleares da segurança da informação e da defesa nacional. Para tal, torna-se essencial reforçar a formação dos militares em literacia digital, psicologia do comportamento e análise crítica da informação. Além disso, a introdução de exercícios regulares que simulem cenários de intrusão humana e campanhas de sensibilização recorrentes deve ser institucionalizada, promovendo uma

cultura de segurança que reconheça o fator humano como parte integrante da arquitetura defensiva.

Este capítulo contribui, assim, para consolidar a perspetiva de que a ES não é apenas uma técnica isolada, mas um fenómeno estratégico com capacidade de interferir na estrutura, na operação e na decisão militar. Compreendê-la em profundidade é um requisito essencial para a formulação de políticas de defesa modernas, adaptadas a um ambiente de ameaças híbridas onde o ciberespaço e o espaço humano se interligam de forma inextricável.

CAPÍTULO 4 – QUADRO CONCEPTUAL

O quadro conceptual é uma ferramenta essencial em qualquer investigação académica, proporcionando uma base teórica que orienta todo o processo de pesquisa onde ajuda a integrar a literatura existente, identificar lacunas e clarificar os principais conceitos envolvidos. Segundo Miles e Huberman (1994), um quadro conceptual "explica, graficamente ou em narrativa, os principais elementos a serem estudados – as principais construções ou variáveis – e as relações presumidas entre elas". Isso significa que um quadro conceptual não é apenas uma coleção de conceitos, mas sim uma estrutura que mostra como os conceitos estão interligados e como contribuem para a compreensão do fenómeno em estudo. Para complementar esta definição, John Maxwell (2013) afirma que um quadro conceptual é "a rede de conceitos e relações que são desenvolvidos a partir da teoria e da literatura relevante, que guiam a investigação". Assim sendo, o quadro conceptual é essencial para orientar o investigador na formulação das hipóteses, na definição dos métodos de pesquisa e na interpretação dos resultados.

A importância de um quadro conceptual na investigação académica pode ser analisada de vários pontos. Relativamente à orientação de pesquisa, fornece uma orientação clara para a investigação, ajudando os investigadores a identificar o que deve ser estudado, as perguntas de pesquisa a serem respondias e as hipóteses a serem testadas. Serve como um mapa que guia todas as fases de pesquisa, desde a recolha de dados até à análise e interpretação dos resultados (Robson, 2011). Sem um quadro conceptual, a pesquisa pode perder o foco e direção, resultando em achados que não contribuem de maneira significativa para o conhecimento existente. Noutra vertente, um quadro conceptual eficaz integra a literatura existente de forma que os conceitos e teorias relevantes sejam destacados e relacionados ao problema de pesquisa, o que permite que os investigadores construam sobre estudos anteriores e evitem a duplicação de esforços (Miles & Huberman, 1994). Além de tudo isto, ao revisar a literatura e identificar as principais teorias e conceitos, os investigadores podem estabelecer uma base sólida para a sua pesquisa, garantindo que ela seja alinhada com o conhecimento atual e que contribua para o avanço da área. Outro fator que realça ainda mais a importância de um quadro conceptual é a identificação de lacunas. Ao explorar as relações entre conceitos e variáveis, o quadro conceptual ajuda a identificar lacunas na literatura existente e essas lacunas podem orientar a formulação de novas hipóteses e perguntas de pesquisa que contribuam para o avanço do conhecimento no campo de estudo (Maxwell, 2013). O que torna mais interessante a possibilidade de identificar

lacunas através de um quadro conceptual é que a identificação das mesmas é crucial para garantir que a pesquisa seja original e relevante, abordando questões que ainda não foram suficientemente exploradas e oferecer novas perspetivas e "insights". Outro ponto bastante positivo do fruto da realização de um quadro conceptual é a clarificação de conceitos, ou seja, a construção desta ferramenta obriga os investigadores a clarificar os conceitos chave e a definir relações entre eles. Clarificar os conceitos é essencial para evitar mal-entendidos e garantir que todos os envolvidos na pesquisa, incluindo outros investigadores e leitores, compreendam claramente o que está sendo estudado e como os diferentes elementos inter-relacionam.

Na análise da ES, um quadro conceptual ajuda a identificar os principais conceitos, bem como, principais fatores que influenciam a vulnerabilidade das pessoas aos ataques de ES. Estes fatores podem incluir características psicológicas, contextos sociais e tecnológicos, e as estratégias usadas pelos atacantes (Mitnick & Simon,2002). A integração de diferentes modelos e teorias no quadro conceptual pode fornecer uma visão abrangente da ES. Um exemplo é o modelo de influência de Cialdini (2001) que identifica seis princípios de persuasão: reciprocidade, compromisso, aprovação social, autoridade, afeição e escassez. Estes princípios podem ser integrados num quadro conceptual para analisar como os atacantes exploram as fraquezas humanas. Como exemplo prático, a reciprocidade pode ser usada em ataques de *phishing* onde o atacante oferece algo aparentemente valioso em troca de informações confidenciais. Relativamente às teorias, a teoria da dissonância cognitiva de Festinger (1957) pode ser usada para explicar como as vítimas de ES racionalizam o seu comportamento após serem enganadas. Por exemplo, uma pessoa pode justificar a cedência de informações sensíveis a um atacante por acreditar que a situação exigia tal ação, minimizando o desconforto causado pela discrepância entres as suas ações e as suas crenças.

Após a apresentação dos fundamentos teóricos e da relevância estratégica da ES em contexto militar, é imperativo sistematizar os principais conceitos que sustentam esta análise. O quadro conceptual assume, neste sentido, um papel estruturante, ao consolidar as noções essenciais que guiarão a reflexão ao longo da dissertação. Os conceitos aqui selecionados não são apenas terminológicos, mas funcionam como instrumentos analíticos com aplicabilidade prática no estudo da segurança da informação e na avaliação de risco em ambientes operacionais como o das FND.

Quadro 1: Quadro Conceptual

Conceito	Definição	Fonte
Engenharia Social	Técnica de manipulação psicológica usada para enganar indivíduos e levá-los a divulgar informações confidenciais ou realizar ações que comprometem a segurança, explorando vulnerabilidades humanas em vez de falhas tecnológicas.	Mitnick, K. D., & Simon, W. L. (2002). "The art of deception: Controlling the human element of security". Wiley.
Segurança da Informação	Preservação da confidencialidade, integridade e disponibilidade da informação, incluindo outras propriedades como autenticidade, responsabilidade, não repúdio e fiabilidade.	International Organization for Standardization. (2013). "ISO/IEC 27000: Information technology — Security techniques — Code of practice for information security controls".
Cibersegurança	Conjunto de atividades e medidas destinadas à proteção de sistemas, redes e dados no ciberespaço contra-ataques, danos ou acessos não autorizados.	Centro Nacional de Cibersegurança (CNCS). (2022). Relatório Riscos e Conflitos 2022.
Força Nacional Destacada	Contingentes militares portugueses projetados para missões internacionais sob mandatos nacionais ou de organizações como a ONU, UE ou NATO.	Ministério da Defesa Nacional. (2021). Relatório de Atividades das Forças Nacionais Destacadas. https://www.defesa.gov.pt
Phishing	Forma de ataque de ES em que o atacante envia comunicações fraudulentas que parecem legítimas, geralmente via e-mail, para enganar as vítimas e obter dados sensíveis.	Hadnagy, C. (2018). "Social Engineering: The science of human hacking" (2.ª ed.). Wiley.
Fator Humano	Elemento comportamental, psicológico e social dos indivíduos que influencia a segurança organizacional, sendo frequentemente o elo mais vulnerável nas estruturas de defesa.	Clarke, R. A., & Knake, R. K. (2019). "The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats". Penguin Press.
Mitigação de Riscos	Processo de identificação, análise e implementação de medidas que visam reduzir a probabilidade e/ou o impacto	Stallings, W., & Brown, L. (2015). "Computer

	de ameaças sobre ativos ou operações críticas.	security: Principles and practice". Pearson.
Princípios de Persuasão	Conjunto de estratégias psicológicas identificadas por Cialdini, como autoridade, escassez, prova social, reciprocidade, simpatia e compromisso, utilizadas para influenciar o comportamento das pessoas.	Cialdini, R. B. (2001). "Influence: Science and practice" (4.ª ed.). Allyn & Bacon.
Espionagem Digital	Ato de recolher secretamente informação digital, geralmente com intenções maliciosas ou políticas, através de intrusão em sistemas informáticos ou manipulação de utilizadores.	EUROPOL. (2021). "Internet Organised Crime Threat Assessment (IOCTA)".
Guerra Cognitiva	Conflito estratégico que visa explorar, influenciar ou degradar a perceção, o julgamento e a tomada de decisão dos indivíduos e grupos, recorrendo a técnicas psicológicas, manipulação de informação e controlo da narrativa.	North Atlantic Treaty Organization (NATO). (2021). "Cognitive Warfare: NATO's Sixth Operational Domain". NATO Innovation Hub.

4.1 Fundamentação do quadro conceptual

A construção do presente quadro conceptual visa sistematizar os conceitos fundamentais que sustentam a análise da ES enquanto ameaça à segurança da organização militar, com especial foco nas FND. Os dez conceitos selecionados refletem a interseção entre três dimensões estruturantes desta investigação: a dimensão técnica da cibersegurança, a dimensão humana do risco e a dimensão operacional do contexto militar.

O conceito de ES constitui o núcleo temático deste trabalho. Trata-se de uma técnica de manipulação psicológica que visa explorar vulnerabilidades humanas para aceder a informação sensível ou comprometer sistemas e infraestruturas, sem recorrer a métodos técnicos intrusivos (Mitnick & Simon, 2002). Este conceito articula-se diretamente com o de Fator Humano, o qual é amplamente reconhecido como o elo mais fraco da cadeia de segurança (Clarke & Knake, 2019), sobretudo em contextos organizacionais fortemente hierarquizados como os militares. Complementarmente, os conceitos de Segurança da Informação e Cibersegurança fornecem o enquadramento técnico e normativo da proteção de dados, redes e sistemas, sendo fundamentais para compreender os mecanismos institucionais de resposta às ameaças digitais. A segurança da informação, regulada por

normas internacionais como a ISO/IEC 27002 (ISO, 2013), define os princípios essenciais de confidencialidade, integridade e disponibilidade da informação. Já a cibersegurança foca-se na prevenção e resposta a ameaças no ciberespaço, sendo frequentemente apontada como a linha da frente contra-ataques de ES (CNCS, 2022). O conceito de *Phishing* surge como uma das manifestações mais comuns e eficazes da ES. Trata-se de uma técnica de ataque que combina engano, urgência e disfarce, muitas vezes utilizada como ponto de entrada para comprometer infraestruturas críticas. Este tipo de ataque é particularmente relevante nas FA, onde a confiança institucionalizada e a cadeia de comando são facilmente exploráveis. O conceito de FND justifica-se pela especificidade operacional deste estudo. Estas forças operam em ambientes internacionais complexos, sujeitos a diferentes culturas, tecnologias e riscos geopolíticos, o que as torna especialmente vulneráveis a tentativas de manipulação, infiltração e desinformação. A análise deste contexto operacional requer, por conseguinte, a compreensão da Espionagem Digital, entendida como o conjunto de práticas destinadas à recolha de informação sensível através de meios tecnológicos ou de ES, com fins maliciosos ou estratégicos (EUROPOL, 2021). Neste quadro, o conceito de Mitigação de Riscos assume particular importância, pois trata-se do processo que visa reduzir a probabilidade de ocorrência ou o impacto das ameaças identificadas. No âmbito da defesa, a mitigação eficaz exige uma abordagem holística que combine medidas técnicas, políticas organizacionais e treino comportamental (Stallings & Brown, 2015). A inclusão dos Princípios de Persuasão, formulados por Cialdini (2001), permite compreender os mecanismos psicológicos que sustentam os ataques de ES. Fatores como a autoridade, a reciprocidade ou a escassez são frequentemente utilizados por atacantes para induzir respostas automáticas e não críticas por parte das vítimas. Finalmente, o conceito de Guerra Cognitiva vem reforçar a leitura estratégica e contemporânea da ameaça. Ao considerar a manipulação da perceção, da tomada de decisão e da interpretação da realidade como instrumentos de conflito, este conceito insere a ES num quadro mais alargado de operações híbridas, onde a informação é usada como arma e o campo de batalha é, muitas vezes, o próprio pensamento humano (NATO, 2021).

A escolha destes conceitos decorre, assim, da sua pertinência teórica, aplicabilidade prática e valor analítico para a compreensão integrada do fenómeno da ES no setor da defesa. Em conjunto, constituem a base sobre a qual se edifica a análise dos riscos, das vulnerabilidades e das respostas institucionais estudadas ao longo desta dissertação.

4.2 Corroboração do Quadro Conceptual com base na literatura científica

O quadro conceptual desenvolvido neste estudo estrutura-se a partir de conceitos fundamentais para a compreensão da ES no domínio da segurança militar, com especial enfoque no fator humano, nas técnicas de ataque utilizadas e nas estratégias de mitigação. Para além da sua fundamentação teórica, é essencial validar empiricamente estes conceitos, demonstrando a sua pertinência com base na literatura científica recente. Neste sentido, foram selecionados dois estudos que, pela sua complementaridade, oferecem uma visão alargada e robusta da problemática em análise: Falla e Pinto (2023), no contexto lusófono, e Pujari e Hussain (2024), numa perspetiva internacional.

Um dos pilares centrais do quadro conceptual é o fator humano como elo vulnerável da segurança organizacional. Esta perspetiva é corroborada por ambos os estudos. Falla e Pinto (2023) sublinham que a ES se apoia na exploração das fragilidades humanas, frequentemente ignoradas em abordagens excessivamente técnicas. Já Pujari e Hussain (2024) aprofundam esta ideia com base em estudos comportamentais, demonstrando como viés cognitivos, complacência hierárquica e desconhecimento técnico contribuem para a elevada taxa de sucesso de ataques como o *phishing*. Esta evidência reforça a centralidade do fator humano no quadro conceptual aqui apresentado. O conceito de *phishing*, considerado uma das manifestações mais prevalentes da ES, surge como um ponto de convergência entre o quadro conceptual e os dois estudos analisados. Falla e Pinto (2023) identificam esta técnica como uma das mais utilizadas em contextos institucionais, destacando o seu caráter dissimulado e a facilidade com que engana utilizadores desatentos. Por sua vez, Pujari e Hussain (2024) analisam o impacto psicológico do *phishing*, explorando como a linguagem de urgência e a imitação de figuras de autoridade aumentam significativamente a taxa de resposta dos alvos. Ambos os estudos validam, assim, a inclusão e destaque deste conceito no presente quadro conceptual. Em relação à segurança da informação e à cibersegurança, o modelo conceptual propõe uma leitura integrada que articula normas técnicas, políticas organizacionais e elementos humanos. Esta proposta é apoiada por Falla e Pinto (2023), que advogam por uma visão holística da cibersegurança, considerando que a proteção da informação não pode ser dissociada da formação contínua dos utilizadores. Complementarmente, Pujari e Hussain (2024) defendem que as estratégias de cibersegurança mais eficazes são aquelas que incorporam princípios da psicologia comportamental, reconhecendo o papel decisivo das emoções e rotinas no comportamento do utilizador. A mitigação de riscos, apresentada no quadro conceptual como um processo

que exige formação, políticas bem definidas e tecnologias complementares, encontra respaldo direto em ambos os artigos. Falla e Pinto (2023) recomendam ações de sensibilização, treino prático e criação de protocolos de resposta rápida, enquanto Pujari e Hussain (2024) destacam a eficácia de intervenções educativas adaptadas aos perfis psicológicos dos utilizadores, complementadas por sistemas técnicos de defesa como a autenticação multifator. Finalmente, conceitos como espionagem digital e guerra cognitiva são também implicitamente validados pelos dois estudos. Falla e Pinto (2023) abordam a manipulação da informação como um vetor de intrusão que pode afetar decisões institucionais. Pujari e Hussain (2024) aprofundam este fenómeno sob a lente da engenharia comportamental, mostrando como os atacantes exploram fragilidades cognitivas para condicionar o julgamento e a perceção das vítimas. Esta análise legitima a inclusão destes conceitos mais recentes no quadro conceptual, especialmente no contexto da defesa, onde a guerra informacional e a manipulação de narrativas assumem crescente relevância.

4.3 Síntese

A correspondência entre o quadro conceptual desenvolvido e os estudos de Falla e Pinto (2023) e de Pujari e Hussain (2024) confirma a robustez, atualidade e aplicabilidade prática dos conceitos selecionados. Esta corroboração reforça a confiança no modelo proposto como instrumento analítico para compreender e enfrentar os riscos da ES no setor da defesa nacional.

CAPÍTULO 5 – ESTRATÉGIAS DE MITIGAÇÃO

Com base no quadro conceptual anteriormente definido, importa agora identificar e sistematizar as estratégias que permitam mitigar os riscos associados à ES em contexto militar. Este capítulo visa apresentar um conjunto de respostas operacionais, formativas e organizacionais, articulando a literatura especializada com recomendações normativas de entidades como o CNCS, o Instituto Nacional de Padrões e Tecnologia (NIST) e o EMGFA. A análise centrar-se-á em práticas de prevenção, deteção e resposta a ataques, tendo como pano de fundo a realidade concreta do Exército Português e das Forças Nacionais Destacadas.

A prevenção eficaz contra-ataques de ES começa com uma abordagem proativa focada na formação e sensibilização dos funcionários. A educação contínua e a conscientização são essenciais para reduzir a vulnerabilidade humana que é frequentemente o elo mais fraco na segurança da informação. Assim sendo, é essencial criar e adotar estratégias de mitigação para que estes ataques sejam menos devastadores ou até mesmo evitados. Por conseguinte, a implementação de programas de formação regulares e abrangentes ajudam os funcionários a reconhecer e responder adequadamente a tentativas de ES. Assim sendo, as organizações devem apostar em sessões de treino práticas como, por exemplo, simulações de *phishing* e outros tipos de ataques para treinar os funcionários num ambiente controlado (Hadgany,2010), realizar workshops e seminários, de modo a que abordem as últimas tendências e técnicas de ataques de ES (Mitnick & Simon, 2002) e garantir uma sensibilização contínua através de material educacional (folhetos, pósteres, manuais, cursos online, etc..).

Por outro lado, além daquilo que são as abordagens humanas, é de extrema importância garantir medidas técnicas contra estes ataques o que requer uma atualização e instauração de ferramentas tecnológicas para que possam ajudar a detetar, bloquear e mitigar tentativas de ataques. Como exemplo temos os *firewalls* que são dispositivos/softwares que monitorizam e controlam o tráfico de rede com base em regras de segurança predefinidas e atuam como uma barreira entre aquilo que são as redes internas seguras com as redes externas não confiáveis, como a internet *(*Stallings & Brown, 2015) e os Sistemas de Deteção de Intrusão (IDS) e os Sistemas de Prevenção de Intrusão (IPS), sistemas estes que monitorizam as redes e os sistemas em busca de atividades incomuns e suspeitas para que tomem medidas para impedir ataques.

5.1 IDS

Deteta atividades suspeitas e gera alertas para que os administradores de segurança possam responder a possíveis ameaças (Scarfone &Mell, 2007).

5.2 IPS

Vai além da deteção, bloqueia automaticamente o tráfico malicioso para que possa prevenir a exploração de vulnerabilidades (Scarfone & Mell, 2007).

5.3 Políticas de segurança

Para complementar todas estas medidas ainda deverão ser incrementadas e respeitadas políticas de segurança bem definidas para ajudem a estabelecer normas e diretrizes que os funcionários devem seguir para proteger a informação da organização e implementar procedimentos de verificação e autenticação.

5.3.1 Política de Uso Aceitável

Define as expectativas e responsabilidades dos funcionários em relação ao uso dos recursos de TI da empresa (ISO/IEC 27000, 2013).

5.3.2 Política de Senhas

Estabelece requisitos para a criação, utilização e renovação de senhas fortes e seguras (NIST, 2017).

5.3.3 Política de Incidentes de Segurança

Protocolo detalhado para a resposta a incidentes de segurança, incluindo procedimentos para relatar e mitigar ataques de ES (ISO/IEC 27035, 2016).

Dada a natureza insidiosa da ES – que contorna tecnologias e ataca diretamente as pessoas – as estratégias de mitigação devem necessariamente focar-se em fortalecer o "fator humano" e os processos organizacionais, sem descurar alguns auxílios tecnológicos. A mitigação efetiva envolve uma combinação de educação, políticas, práticas e tecnologias. Assim sendo, é necessário ter atenção a um conjunto de medidas, recomendadas pela literatura e por diretrizes de cibersegurança, com aplicação ao contexto militar.

5.4 Formação, consciencialização e cultura de segurança

A formação contínua de todo o pessoal, militar e civil, é unanimemente apontada como a primeira linha de defesa contra a ES. Não basta instruir uma vez; é preciso incutir uma cultura em que cada membro da organização se torne um sensor ativo contra-ameaças deste tipo. Algumas ações incluem:

5.4.1 Programas de Consciencialização Regulares

Realizar sessões periódicas de treino em segurança da informação, incluindo módulos específicos sobre ES. Estes devem cobrir os conceitos básicos, exemplos de ataques recentes e simulações práticas. Por exemplo, exercícios de *phishing simulation* podem ser conduzidos enviando emails fictícios ao pessoal para avaliar quem clica – e depois formando individualmente os que falharam no teste. Nas FA de diversos países (EUA, Reino Unido, etc.), este tipo de exercício já é rotina, administrado pelo setor de cibersegurança, para "inocular" os utilizadores contra armadilhas.

5.4.2 Destaque para Riscos em Redes Sociais

Instruir os militares (especialmente os mais jovens) sobre as armadilhas nas redes sociais. Isso inclui boas práticas de privacidade (configurações restritas, não aceitar pedidos de desconhecidos), evitar georreferenciação de posts, e proibição estrita de discutir detalhes de serviço online (OPSEC). Sessões de briefing antes de partidas em missão devem reforçar: "o inimigo está atento online tanto quanto no terreno". Muitas forças, incluindo o Exército Português, já difundem guias de *social media awareness*. Idealmente, familiares também devem ser alcançados por campanhas de sensibilização (por ex., folhetos informativos para as famílias explicando porque não se deve postar datas de partida/chegada ou detalhes das missões dos seus entes queridos).

5.4.3 Cultura de Zero-Trust (Confiança Zero)

Promover ativamente uma mentalidade em que desconfiar é saudável em contexto de segurança. Os militares devem sentir-se empoderados para verificar identidades e ordens sem receio de ofender. Por exemplo, ensinar: se receber um telefonema incomum pedindo informações, é correto dizer "vou retornar a chamada pelos canais oficiais"; se um civil tenta entrar consigo num recinto reservado, deve-se cortês, mas firmemente verificar credenciais e acompanhar à segurança se necessário. Essa cultura também envolve não penalizar quem

reporta falsos alarmes – antes premiar a vigilância. Quanto mais olhos atentos, menos espaço para um atacante se insinuar.

5.4.4 Lições Aprendidas e Divulgação de Incidentes

Sempre que houver uma tentativa (real ou simulada) de ES, partilhar internamente as lições. Por exemplo, se num teste de *phishing* 30% clicaram num anexo falso, divulgar esse número e explicar o que podia ter acontecido. Se um militar notou um perfil falso no Facebook tentando adicioná-lo e reportou, elogiar o ato e avisar os demais para bloquearem o perfil. A transparência sobre incidentes (resguardando segredos quando necessário) ajuda a tornar o perigo concreto e não algo meramente teórico.

Conforme observado por Azzolin (2017), a conscientização do público interno é indispensável e deve ser tratada como parte das políticas de segurança da informação nas organizações. O autor reforça a necessidade de educar continuamente os militares para reconhecerem sinais de ES e adotarem postura proativa de segurança.

5.5 Políticas de segurança da informação e procedimentos operacionais

Além da formação individual, é essencial que a organização disponha de regras claras e procedimentos que reduzam as oportunidades para o Engenheiro Social e orientem a resposta adequada quando uma tentativa ocorre.

5.5.1 Política de Comunicação e Uso de Dispositivos

Estabelecer normas que regulem o que é permitido em termos de comunicações pessoais e profissionais, especialmente em teatros de operações. Por exemplo, pode-se determinar que smartphones pessoais não acedam à rede interna da base, que certos períodos antes de operações sensíveis haja blackout de comunicações pessoais (para evitar fugas acidentais), e que todos os dispositivos pessoais dos militares sejam cadastrados e monitorizados quanto a comportamentos anómalos (sem invadir privacidade injustificadamente, mas com sensores de deteção de *malware* atualizados). Uma clara política de redes sociais deve instruir o que se pode ou não divulgar (muitos exércitos adotam listas de “não postar”: fardas, locais, datas, etc.). Essas políticas, para terem eficácia, devem ser reforçadas por liderança – ou seja, comandantes e oficiais superiores dando o exemplo e cobrando cumprimento.

5.6 Procedimentos de Verificação de Identidade

Implementar e treinar procedimentos formais para verificar identidades quer em comunicações, quer presencialmente. No campo das comunicações: usar autenticação *multifator* e códigos de desafio para ordens críticas transmitidas (por exemplo, se receber um email de ordem urgente, validar através de um código ou chamada pré-combinada). A UE recomenda insistentemente o uso de autenticação *multifator* como barreira adicional contra acesso indevido.

5.6.1 Nas interações presenciais

Instituir crachás e passes para áreas restritas e a regra de que visitantes (mesmo que supostos VIP ou aliados) devem ser sempre escoltados. Minimizar exceções ad hoc.

5.6.2 Segregação de Privilégios e Informação

Adotar o princípio do *need-to-know* e *least privilege* de forma rigorosa. Se cada elemento só tem acesso à informação estritamente necessária para as suas funções, reduz-se o impacto caso alguém seja enganado. Por exemplo, um soldado raso não deveria conseguir aceder a planos estratégicos – logo, mesmo que caia num *phishing*, o dano é contido. Estruturar as redes e bases de dados de forma segmentada, limitando também a possibilidade de movimento lateral de um eventual intruso.

5.6.3 Políticas de Relato e Reação

Deve ficar estipulado que qualquer tentativa ou suspeita de ES seja reportada imediatamente aos oficiais de segurança/cadeia de comando, sem punição pela vítima ter sido visada. Uma cultura em que o militar sinta confiança em dizer "acho que fui alvo de um esquema" é essencial para resposta rápida. Os procedimentos devem incluir: isolar máquinas possivelmente comprometidas, informar o restante pessoal se necessário (ex.: se houve emails falsos circulando, avisar todos para apagar), e acionar investigação pela contrainteligência ou ciberdefesa. De acordo com diretrizes internacionais, "qualquer incidente suspeito deve ser comunicado de imediato ao departamento responsável, a fim de serem tomadas providências" – este conselho, extraído de uma publicação acadêmica, alinha-se com as melhores práticas de gestão de incidentes.

5.6.4 Testes de Segurança e Auditorias

Incorporar nos exercícios militares componentes de ES (por ex., incluir cenários de *insider threat* em exercícios de proteção de força). Adicionalmente, realizar auditorias periódicas de conformidade: verificar, por exemplo, se não há *pendrives* USB conectadas indevidamente, se terminais foram deixados desbloqueados, ou se pessoal de sentinela está cumprindo as verificações de credencial. Estas auditorias simulam o olhar de um potencial atacante identificando portas abertas.

Em suma, as políticas formam o arcabouço que reduz a chance do erro humano e prevê um plano de contingência para quando algo falha. Documentos oficiais, como normativas de ciberdefesa, tipicamente incluem secções dedicadas a "medidas de proteção do elemento humano" e enfatizam o desenvolvimento de protocolos robustos contra manipulação social (ver, e.g., Portaria Normativa n.º 3.010/MD do Ministério da Defesa do Brasil, 2014, que incorpora ES como ameaça à doutrina de defesa cibernética).

5.7 Medidas técnicas de apoio

Embora a ES contorne a tecnologia, há ferramentas e configurações tecnológicas que podem ajudar a prevenir ou limitar os danos desses ataques:

5.7.1 Filtragem e Detecção de Phishing

Utilização de sistemas de filtragem de emails e mensagens que identifiquem spam, *phishing* conhecido e anexos suspeitos antes de chegarem ao utilizador. Soluções de Secure Email Gateway podem bloquear grande parte de emails forjados. No entanto, reconhece-se que ataques direcionados sofisticados podem iludir filtros, então não se pode depender unicamente deles.

5.7.2 Autenticação Multifator (AMF)

Conforme já mencionado, a AMF (por exemplo, uso de *token* ou app além da senha) impede que a simples obtenção de credenciais via ES seja suficiente para aceder a sistemas críticos.

As FA devem implementar AMF em todos os acessos remotos e serviços sensíveis (email, VPN, etc.). Assim, mesmo que um soldado revele inadvertidamente a sua senha, o atacante não conseguirá fazer o login sem o segundo fator (que pode ser um cartão físico ou código no telemóvel do militar – telemóvel esse que, se estiver comprometido por *malware*, seria problemático, mas idealmente o segundo fator deve ser hardware seguro).

5.7.3 Limitação de Dispositivos e Mídias

Controlar portas USB e leitores de mídia nos equipamentos militares – por exemplo, através de políticas de grupo que desativem auto-execução de dispositivos externos e registem qualquer cópia de dados para *pendrives*. Caso um atacante entregue uma "isca" USB (*baiting*), esta não deveria infetar automaticamente o sistema quando ligada. Além disso, usar criptografia de dados nos dispositivos torna menos proveitoso para um atacante obter um laptop ou *pen* extraviados.

5.7.4 Monitorização e Inteligência de Ameaças

Equipas de ciberdefesa podem empregar ferramentas de monitorização de menções à força militar em fontes abertas (OSINT) e nas redes sociais. Se houver um aumento repentino de perfis tentando adicionar membros da unidade, ou se *phishing* similares forem reportados em outro país contra forças aliadas, essas informações devem ser rapidamente comunicadas. Estar a par das táticas emergentes (por ex., uso de *deepfakes* de voz para imitar comandantes em telefonemas – algo já demonstrado em ambiente empresarial) permite atualizar o treino e alertar o pessoal. A integração de fontes de inteligência, inclusive da comunidade de INFOSEC civil, ajuda a antecipar novas formas de ataque social.

5.7.5 Resposta a Incidentes e Backup

Do ponto de vista técnico, caso um ataque concretize e cause dano (ex.: encriptação de dados após um *malware* entrar via ES), é fundamental ter *backups* atualizados e planos de recuperação. Isso não previne o ataque inicial, mas mitiga o impacto, permitindo restaurar sistemas sem ceder a extorsões. Da mesma forma, se credenciais forem roubadas, procedimentos de *reset* geral de senhas e invalidação de sessões devem estar prontos para execução imediata.

Vale destacar o programa ASED (Active Social Engineering Defense) da DARPA (EUA), que investiga formas automatizadas de identificar e interromper interações de ES em tempo real. Embora numa fase experimental, projetos assim indicam que no futuro poderemos ter assistentes de IA que alertam um utilizador se, por exemplo, o email que acabou de ler tem características de *phishing*, ou se a pessoa que lhe telefona está a mentir (com base em padrões de voz). Enquanto essas tecnologias não amadurecem, prevalece a dependência no julgamento humano treinado, apoiado pelos controles básicos referidos.

5.8 Medidas específicas para forças destacadas

Algumas medidas de mitigação merecem destaque especial quando se trata de contingentes em missão fora do país, acumulando elementos das categorias acima:

5.8.1 Briefing e De-briefing de Segurança:

Antes do destacamento, realizar um briefing abrangente de forma a cobrir ameaças de ES específicas da área de operações. Incluir informações de inteligência sobre possíveis tentativas de aproximação por parte de serviços estrangeiros ou grupos hostis, modus operandi esperados (por ex., "sabe-se que na região tal, espiões costumam investigar hábitos nos bares locais"). Após o retorno da missão, fazer de-briefing para recolher eventuais experiências de tentativas de ES enfrentadas, aprendendo com o terreno.

5.8.1..1 Rotação de Procedimentos e Códigos

Em ambientes de alto risco, variar regularmente procedimentos que possam ser conhecidos pelo inimigo. Por exemplo, mudar códigos de autenticação de comunicações com maior frequência, alterar rotas de patrulha (já se faz taticamente) mas também alterar rotinas de acesso – se os agressores aprendem que certo oficial verifica emails todas as noites às 22h, podem escolher esse horário para ataques; variações aleatórias podem frustrar essas observações. Essencialmente, não dar margem para que o inimigo explore padrões humanos estáveis.

5.8.1..2 Contrainteligência Ativa

Empregar pessoal de contrainteligência para eles mesmos, testarem a força destacada. Isso vai além do *red teaming* técnico – agentes podem simular abordagens sociais (tentar ligar para a base fingindo ser do comando, ou enviar questionários falsos de ONG aos militares). O objetivo não é "enganar por enganar", mas identificar quem poderia sucumbir e reforçar a formação nesses pontos fracos. Em missões críticas, por vezes destacam-se oficiais de segurança cuja função é observar o comportamento dos próprios militares, aconselhando-os se notam, por exemplo, alguém a falar demais com estranhos fora do perímetro.

5.8.1..3 Limpeza digital e OPSEC rigoroso

Orientar militares a "limpar" a sua pegada digital antes de partirem – rever definições de privacidade, remover dados sensíveis ou pessoais excessivos online, e durante a missão manter-se discretos. Alguns contingentes chegam a proibir o uso de certos aplicativos conhecidos por falta de segurança. Embora isso possa afetar o moral (pois limita contato com família), equilibra-se definindo canais alternativos seguros para comunicação pessoal (por ex., uma sala de internet controlada na base com monitoração).

5.8.2 Coordenação Multinacional

Em forças combinadas (por ex., NATO), partilhar informações sobre tentativas de ES entre países. Se um contingente italiano notar civis suspeitos tentando coletar dados, o contingente português deve ser alertado. Estabelecer pontos focais para troca de inteligência sobre ameaças humanas.

5.8.3 Síntese

Ao implementar estas estratégias, espera-se reduzir significativamente o risco de sucesso das tentativas de ES. Azzolin (2017) concluiu que a síntese de medidas preventivas adequadas ao meio militar – incluindo políticas de segurança robustas e conscientização – contribui de forma decisiva para proteger o ativo informação e a própria força. Do mesmo modo, as diretrizes do Conselho da UE sobre cibersegurança salientam que "o conhecimento é a sua defesa" e recomendam práticas como pensar antes de clicar, proteger informações pessoais e verificar identidades em contactos inesperados.

As estratégias aqui apresentadas demonstram que a resposta à ES não se limita à implementação de soluções técnicas, mas exige uma abordagem integrada, que combine a formação contínua, a consciencialização institucional, a normalização de procedimentos e o reforço da vigilância comportamental. Com esta sistematização concluída, abre-se caminho para a análise crítica dos resultados obtidos, bem como para a reflexão final sobre os contributos e limitações do estudo, a serem abordados nas conclusões.

PARTE II – ENQUADRAMENTO METODOLÓGICO E RESULTADOS

CAPÍTULO 6 – METODOLOGIA, MÉTODOS E MATERIAIS

A metodologia deste estudo foi elaborada para proporcionar uma análise abrangente e detalhada sobre a ES, utilizando uma abordagem qualitativa. Esta escolha metodológica justifica-se pela natureza exploratória do tema e pela necessidade de compreender as nuances e implicações associadas às práticas de ES em diversos contextos. A investigação segue, portanto, uma abordagem qualitativa, essencial para explorar em profundidade os fenómenos relacionados com a ES, nomeadamente no contexto das Forças Armadas e da segurança nacional. Segundo Creswell (2013), a pesquisa qualitativa é apropriada para estudos que procuram compreender significados, experiências e processos complexos, especialmente em áreas onde o comportamento humano e os contextos sociais desempenham um papel crucial. Esta abordagem permite uma análise detalhada das técnicas de ES e dos seus impactos, tanto a nível individual como organizacional. Tendo em conta que a Engenharia Social atua primariamente sobre o fator humano, e muitas vezes sem deixar vestígios técnicos mensuráveis, torna-se fundamental compreender os processos subjetivos que envolvem manipulação, perceção de risco e resposta organizacional.

A recolha de dados foi realizada através de uma revisão bibliográfica exaustiva, centrada numa análise documental e crítica. Esta incluiu artigos académicos, livros, relatórios técnicos, estudos de caso, doutrina militar e documentação emitida por organismos especializados em cibersegurança, defesa e inteligência, como o CNCS, a NATO, a EUROPOL e EMGFA. A seleção dos materiais obedeceu a critérios de atualidade (prioridade a publicações pós-2015), relevância temática, autoridade da fonte e aplicabilidade ao contexto militar português. Autores de referência como Mitnick e Simon (2002), Hadnagy (2018), Clarke e Knake (2019) foram particularmente relevantes para compreender os fundamentos técnicos e psicológicos da ES. Paralelamente, foram incorporadas análises sobre operações militares contemporâneas, com destaque para os riscos enfrentados por em cenários de elevada complexidade operacional e cultural. O cruzamento entre fontes académicas e institucionais permitiu construir um quadro conceptual robusto e alinhado com a realidade operacional das forças militares.

O método de análise adotado foi a análise de conteúdo qualitativa, aplicado às fontes recolhidas. Este processo permitiu identificar padrões, estratégias, vulnerabilidades e medidas de mitigação documentadas em diversos contextos. A triangulação de fontes — académicas, normativas e operacionais — visou garantir uma abordagem rigorosa e multidimensional, reforçando a validade da análise realizada. A construção do quadro conceptual e dos eixos temáticos da investigação derivou da categorização temática progressiva das fontes analisadas.

A investigação seguiu três eixos analíticos principais: (1) a conceptualização da ES enquanto fenómeno estratégico; (2) a análise da sua aplicação no setor da defesa, com particular incidência nas FND; e (3) a avaliação crítica das respostas institucionais existentes, em termos de prevenção e mitigação. Estes eixos guiaram a organização dos capítulos e a resposta articulada aos objetivos e à pergunta de partida. Não foram utilizados instrumentos quantitativos nem foram realizados inquéritos, entrevistas ou observação direta, por razões éticas, de segurança institucional e pela própria natureza do fenómeno estudado. A ausência de trabalho empírico direto foi colmatada por uma análise sistemática e crítica das fontes disponíveis, respeitando os princípios de fiabilidade, coerência e densidade interpretativa.

Por fim, os materiais analisados foram tratados à luz dos princípios éticos da investigação científica, assegurando o respeito pelas fontes e a transparência das interpretações apresentadas. A metodologia adotada revelou-se adequada aos objetivos da investigação, permitindo uma compreensão aprofundada da ES no domínio militar e sustentando as recomendações propostas nos capítulos finais.

CAPÍTULO 7 – DISCUSSÃO CRÍTICA

A complexidade crescente dos conflitos contemporâneos, caracterizados por uma fusão entre ameaças físicas, cibernéticas e cognitivas, exige das forças militares uma postura adaptativa que reconheça o papel central da segurança da informação e, especialmente, do fator humano. Neste contexto, a ES emerge como um desafio transversal à doutrina, à formação e à operação das FA, sendo simultaneamente uma ameaça invisível e profundamente eficaz. Esta dissertação permitiu desenvolver um quadro conceptual centrado nos principais riscos associados à ES, nas suas técnicas de execução e nas respostas institucionais possíveis.

A análise crítica dos resultados obtidos confronta os modelos teóricos da cibersegurança, os contributos da psicologia organizacional e os dados documentais com as realidades institucionais. Verifica-se, por exemplo, uma dissonância significativa entre a sofisticação crescente das táticas de ES utilizadas por atores hostis e o grau de preparação das estruturas militares para as reconhecer e mitigar. Esta lacuna revela uma assimetria de enfoque: enquanto os investimentos em tecnologias de defesa cibernética se intensificam, a vertente comportamental e humana continua a ser negligenciada ou tratada de forma secundária. Tal constatação é reforçada por autores como Hadnagy (2018) e Cybenko (2015), que sublinham a importância de integrar o risco humano como um pilar estrutural da segurança. O papel das FND constitui, dentro desta análise, um ponto especialmente sensível. Estas unidades operam em contextos multiculturais, de elevada ambiguidade e sob pressão constante, tornando-as vulneráveis a ataques baseados em manipulação interpessoal. Tais interações podem parecer inofensivas — em redes sociais, em conversas informais ou em abordagens no terreno — mas muitas vezes escondem operações sofisticadas de recolha de informação ou influência cognitiva (EUROPOL, 2021; CNCS, 2022). As redes sociais, em particular, surgem como vetor privilegiado para este tipo de ações, precedendo frequentemente operações de espionagem ou campanhas de desinformação.

A investigação evidencia ainda um défice persistente de articulação entre os princípios da segurança da informação e a formação operacional quotidiana. Em muitos contextos militares, a cibersegurança continua a ser percecionada como responsabilidade exclusiva de técnicos ou especialistas. No entanto, os dados analisados apontam para o comportamento diário — o clique num link, a partilha inadvertida de informações, o uso de aplicações pouco seguras — como elementos-chave na vulnerabilidade organizacional. Neste sentido, a ES não é apenas uma técnica isolada: é um fenómeno cultural, enraizado

em normas tácitas, perceções de risco distorcidas e rotinas institucionais. Outro ponto crítico identificado prende-se com a ausência de um quadro legal e normativo que aborde especificamente a ES em ambiente militar. A falta de codificação normativa compromete a capacidade de prevenção e reação, dificultando a responsabilização e o tratamento disciplinar de incidentes. A doutrina de cibersegurança militar tem evoluído no plano técnico, mas continua a deixar lacunas no plano humano — precisamente aquele que os agentes de ES mais exploram. Importa sublinhar que, embora esta investigação não tenha recorrido a fontes empíricas diretas — como entrevistas ou observação participante — a triangulação de fontes académicas, normativas e operacionais permitiu construir um modelo teórico com aplicabilidade real. A ausência de dados internos sobre a realidade das FAP em matéria de ES justifica-se por limitações éticas e institucionais, mas não invalida o valor analítico do quadro conceptual desenvolvido. Este oferece uma base sólida para futuras investigações empíricas e práticas doutrinárias.

Assim, os resultados obtidos sugerem a necessidade de uma transformação organizacional profunda: a ES só poderá ser enfrentada de forma eficaz se for reconhecida como uma ameaça estrutural e transversal. Tal transformação requer liderança, pedagogia institucional, revisão sistemática de processos e institucionalização de práticas de formação contínua. Programas de consciencialização, simulações realistas de intrusão social e campanhas internas de sensibilização devem ser integradas como parte da cultura de segurança.

O principal contributo desta investigação reside, portanto, na capacidade de articular um modelo teórico robusto com implicações práticas, reforçando a ideia de que a segurança da informação, no setor da defesa, começa no comportamento humano. O fator humano deve deixar de ser o elo mais fraco e passar a ser compreendido como a primeira linha de defesa.

CAPÍTULO 8- CONCLUSÕES

A presente investigação procurou compreender o impacto da ES como uma ferramenta crítica para a segurança das organizações militares, com particular incidência no desenvolvimento de um quadro conceptual, na análise de riscos operacionais e na identificação de medidas de mitigação. Com base numa abordagem qualitativa e numa revisão bibliográfica e documental rigorosa, foi possível obter resultados que respondem de forma coerente às perguntas de partida e aos objetivos delineados.

O quadro conceptual construído, sustentado em autores como Mitnick e Simon (2002), Hadnagy (2018), Clarke e Knake (2019), Cialdini (2001) e o National Research Council (2010), permitiu clarificar os principais conceitos associados à ES no contexto militar. Destacam-se nesta análise as técnicas mais comuns (como *phishing*, *pretexting*, *baiting*), os vetores de manipulação psicológica (autoridade, reciprocidade, escassez, prova social e compromisso) e as vulnerabilidades humanas (confiança excessiva, curiosidade, falta de formação, stress operacional). Esta estrutura analítica revelou a interdependência entre fatores técnicos e comportamentais, realçando que a ES não é apenas uma ameaça externa, mas um risco interno profundamente enraizado nas rotinas e estruturas hierárquicas. A compreensão aprofundada deste fenómeno revelou que as organizações militares apresentam características que podem, inadvertidamente, potenciar ataques de ES: a disciplina hierárquica, o espírito de camaradagem, a comunicação tácita e a presunção de segurança no meio interno. Estas dinâmicas são exploradas por agentes maliciosos através de técnicas que induzem o erro humano ou a partilha indevida de dados sensíveis. A perceção de que o perigo provém apenas de fora da estrutura militar constitui, por si só, uma vulnerabilidade crítica.

No que respeita à sua utilização como ameaça contra FND, identificou-se que a ES representa um risco crescente para a segurança da informação e para a estabilidade operacional. Este risco é particularmente acentuado em cenários de missão onde o contacto com populações locais, forças aliadas e entidades civis pode abrir espaço a interações informais não controladas. Fontes como o CNCS (2022), a NATO Innovation Hub (2021) e a EUROPOL (2021) documentam situações onde dados operacionais foram comprometidos por via de interações sociais aparentemente inofensivas. As redes sociais, por sua vez, continuam a ser uma via privilegiada para a recolha passiva de informação por parte de agentes hostis, podendo mesmo preceder operações mais complexas de espionagem digital ou influência cognitiva. Em muitos casos, os militares destacados são alvos de campanhas

de desinformação, perfis falsos e mensagens manipuladoras, frequentemente disseminadas através de plataformas abertas. A ausência de protocolos uniformes de resposta a incidentes de ES no contexto das FND agrava a situação, permitindo que tentativas de recolha de dados ou manipulação de perceções não sejam imediatamente reconhecidas como ameaças. O impacto operacional pode traduzir-se no compromisso da localização de unidades, exposição de cronogramas de missão e degradação da moral das tropas.

A investigação permitiu identificar um conjunto de boas práticas com base em fontes especializadas, que apontam para três eixos fundamentais de atuação. O primeiro é a formação contínua com simulações realistas de ES, incluindo *red teaming* e testes de penetração baseados em engenharia psicológica. O segundo é a implementação de regras rígidas de partilha de informação, aplicando o princípio do menor privilégio e a verificação cruzada de ordens e pedidos atípicos. E por último, o envolvimento das famílias dos militares em campanhas de consciencialização e educação digital, com vista a reduzir a exposição de dados sensíveis nas redes sociais. Estas práticas devem ser integradas numa cultura organizacional de segurança, sustentada em liderança ativa e envolvimento institucional.

As recomendações emergentes desta investigação incidem sobre a necessidade urgente de integrar sistematicamente a ES nos programas de formação militar, desde os cursos de praça até à formação de altos quadros. A elaboração de um manual de contra Engenharia Social adaptado ao contexto das FND, bem como a criação de equipas especializadas de resposta a incidentes de natureza humana, constituem passos fundamentais para a mitigação deste tipo de risco. Além disso, propõe-se o reforço da articulação entre as estruturas de ciberdefesa e os comandos operacionais, assegurando que as ameaças comportamentais são tratadas com o mesmo rigor das vulnerabilidades técnicas.

Contudo, reconhecem-se limitações metodológicas relevantes. A não realização entrevistas e recolha de testemunhos operacionais limitou a riqueza empírica da análise. O acesso condicionado a documentos classificados restringiu a valoração de casos práticos, e a dependência de fontes secundárias implica um desafio constante de validação e triangulação. Estas limitações, embora justificáveis no contexto da investigação, apontam para a necessidade de estudos complementares com abordagem empírica, nomeadamente entrevistas estruturadas com militares em funções operacionais.

Respondendo à questão de investigação "Qual o impacto da ES como ferramenta crítica para a segurança da organização militar, considerando as suas potencialidades e os riscos envolvidos?", conclui-se que se trata de uma ameaça efetiva, persistente e subestimada, cuja eficácia reside na exploração sistemática do comportamento humano e das

fragilidades psicológicas inerentes ao contexto militar. A ES revela-se como uma vulnerabilidade transversal à estrutura castrense, e a sua compreensão é fundamental para o reforço das políticas de segurança e da resiliência institucional.

Em conformidade, foram alcançados todos os objetivos delineados: foi construído um quadro conceptual robusto, analisado o impacto operacional da ES em contextos militares, e identificadas medidas concretas de mitigação adaptadas à realidade das Forças Armadas Portuguesas. Esta investigação oferece, assim, um contributo sólido para a doutrina de segurança militar e para a promoção de uma abordagem holística e integrada à proteção da informação e à defesa contra-ameaças baseadas no fator humano.

REFERÊNCIAS BIBLIOGRÁFICAS

Azzolin, M. M. (2017). Ataques de Engenharia Social: Medidas preventivas para a segurança da informação. *O Comunicante*, 7(3), 56–64. Publicação da Revista do Exército Brasileiro.

BBC News. (2020, 16 de julho). Twitter hack: What went wrong and why it matters. *BBC*. https://www.bbc.com/news/technology-53425822

Centro Nacional de Cibersegurança. (2022). *Relatório riscos e conflitos 2022 – Observatório de Cibersegurança*. https://www.cncs.gov.pt

Cialdini, R. B. (2001). *Influence: Science and practice* (4.ª ed.). Allyn & Bacon.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3.ª ed.). SAGE Publications.

Cybenko, G. (2015). Cognitive hacking: A battle for the human mind. IEEE Security & Privacy Magazine, 13(3), 58–60. https://doi.org/10.1109/MSP.2015.61

EUROPOL. (2021). *Internet organised crime threat assessment (IOCTA)*. https://www.europol.europa.eu

Falla, D. A. A., & Pinto, G. S. (2023). Engenharia Social e a importância da cibersegurança na atualidade. Interface Tecnológica, 20(2), 58–65. https://revista.fatectq.edu.br/interfacetecnologica/article/download/1759/940/7427

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford University Press.

Gomes, R. C., & Motta, M. M. S. (2024). Framework contrainteligente para ataques de Engenharia Social. *REAVI – Revista de Educação, Artes e Letras, 10*(1), 101–123. https://doi.org/10.36489/reavi.v10i1.29516

Granger, S. (2001). Social engineering fundamentals, Part I: Hacker tactics. *SecurityFocus*. https://www.securityfocus.com/infocus/1527

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Wiley.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2.ª ed.). Wiley.

International Organization for Standardization. (2013). *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls.*

International Organization for Standardization. (2016). *ISO/IEC 27035: Information technology – Security techniques – Information security incident management*.

Internos Group. (2021). *Social engineering attack cycle*. https://www.internosgroup.com/blog/social-engineering-attack-cycle/

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid*. SANS Industrial Control Systems.

Liu, Y., Wang, X., Li, T., & Chandel, A. (2017). *Understanding social engineering techniques in cyber security*. Proceedings of the 2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1–8. https://doi.org/10.23919/CYBERSEC.2017.8074862

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3.ª ed.). SAGE Publications.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2.ª ed.). SAGE Publications.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2011). *Ghost in the wires: My adventures as the world's most wanted hacker*. Little, Brown and Company.

NATO Cooperative Cyber Defence Centre of Excellence. (2019). *Social engineering attacks and defences: A framework for assessing risk and mitigation*. https://ccdcoe.org

National Institute of Standards and Technology. (2017). *Digital identity guidelines* (SP 800-63B). https://doi.org/10.6028/.SP.800-63b

Pujari, S. R., & Hussain, M. A. (2024). Human factor in cybersecurity: Behavioral insights into phishing and social engineering attacks. Nanotechnology Perceptions, 20(S15), 630–642. https://doi.org/10.62441/nano-ntp.vi.3556

Robson, C. (2011). *Real world research* (3.ª ed.). Wiley.

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (SP 800-94). National Institute of Standards and Technology.

Shahrom, M. F., Maarop, N., Samy, G. N., & Hassan, N. H. (2021). A pilot analysis of factors affecting defense against social engineering attacks in the armed forces environment. *Open International Journal of Informatics*, 9(1), 53–64. https://doi.org/10.11113/oiji2021.9n1.28

Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice.* Pearson.

Symantec. (2019). *Internet security threat report* (Vol. 24). https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-24

Wang, Z., Zhu, H., & Sun, L. (2021). *Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods*. *Journal of Cybersecurity and Information Integrity*, 3(2), 45–62. https://doi.org/10.1016/j.jcsi.2021.03.007

Verizon. (2020). *2020 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/