ACADEMIA DA FORÇA AÉREA

O Impacto das Redes Sociais nas Operações Militares

David Miguel Dorotea Muleta

Aspirante a Oficial-Aluno/Piloto-Aviador 137724-J

Dissertação para obtenção do Grau de Mestre em

Aeronáutica Militar, na Especialidade de Piloto-Aviador

Júri

Presidente:	Coronel Joaquim José Carvalheira Baptista Veloso
Orientador:	Professor Doutor Paulo Cardoso do Amaral
Coorientador:	Major Paulo Jorge Rodrigues Mineiro
Vogal:	Tenente-Coronel Paulo Jorge Machado Dias Gonçalves

Sintra, março de 2015

Página intencionalmente deixada em branco

ACADEMIA DA FORÇA AÉREA

O Impacto das Redes Sociais nas Operações Militares

David Miguel Dorotea Muleta

Aspirante a Oficial-Aluno/Piloto-Aviador 137724-J

Dissertação para obtenção do Grau de Mestre em

Aeronáutica Militar, na Especialidade de Piloto-Aviador

Júri

Presidente:	Coronel Joaquim José Carvalheira Baptista Veloso
Orientador:	Professor Doutor Paulo Cardoso do Amaral
Coorientador:	Major Paulo Jorge Rodrigues Mineiro
Vogal:	Tenente-Coronel Paulo Jorge Machado Dias Gonçalves

ISBN:

Sintra, março de 2015

Este trabalho foi elaborado com finalidade essencialmente escolar, durante a frequência do Curso de Pilotagem Aeronáutica cumulativamente com a atividade escolar normal. As opiniões do autor, expressas com total liberdade académica, reportam-se ao período em que foram escritas, mas podem não representar doutrina sustentada pela Academia da Força Aérea.

Agradecimentos

Assim encerro mais uma etapa e subo mais um degrau da grande escada académica a que me propus subir, voluntária e orgulhosamente. Encontro-me agora um pouco mais próximo de materializar este longo sonho, que voa comigo desde pequeno, ser piloto militar ao serviço do meu país. O que no início era uma nuvem inatingível, começo agora a observá-la de perto e anseio o dia de a poder tocar.

A Academia da Força Aérea Portuguesa deu-me a generosa oportunidade de alcançar esse sonho, o que significou profundas mudanças na minha vida. Nesta casa tenho aprendido e crescido. Aprendi a conhecer-me a mim próprio e a valorizar as pequenas coisas da vida, que agora têm outro significado, outro simbolismo e outra virtude. Em cada fase aprendi novas lições e conquistei novas metas. Cada fase foi conquistada com entrega, dedicação, orgulho e esperança de concretizar um sonho de criança e aquilo que parecia inalcançável foi pouco a pouco, página a página, alcançado. Conquistei assim mais um desafio, graças a mim e a todos os que me apoiaram. Sem esses, nada disto seria possível e a eles quero agradecer.

Reservo o primeiro agradecimento à minha família. Apoiaram-me em todas as fases e a força que demonstram nas barreiras que ultrapassam (e que juntos ultrapassamos), resulta na minha motivação, força e empenho. Tenho de facto uma família maravilhosa: um Pai invencível, uma Mãe líder e empenhada, uns Irmãos dedicados e uma namorada tão militar quanto eu, por ter tanta força e compreensão. A todos os que ultrapassam comigo cada meta, Obrigado.

Gostaria de dedicar um enorme agradecimento ao Professor Doutor Paulo Amaral, um excelente profissional, que me transmitiu conhecimentos essenciais e orientou para a concretização deste objetivo.

Deixo também um especial e muito generoso agradecimento ao Major Paulo Mineiro, que me enquadrou, motivou e ajudou incansavelmente. Muito Obrigado.

A todos os militares que demonstraram interesse no meu tema e prontificaram-se a ajudar, deixo também um Obrigado, pois sem cada um de vós, este conteúdo não seria possível.

Aos meus camaradas de curso e a todos os meus amigos, Obrigado pela força e motivação.

Página intencionalmente deixada em branco

Resumo

Esta dissertação tem como objetivo determinar de que forma a utilização de Redes Sociais em Operações Militares, quer pela Força Aérea Portuguesa, quer pelos seus militares, pode influenciar essas operações.

Neste trabalho, presume-se que as Redes Sociais são um ponto de encontro fundamental para a comunicação entre as pessoas. No âmbito militar, este pressuposto concretiza-se em considerar que a Guerra de Informação ocorre todos os dias de forma silenciosa e que uma "simples" publicação pode resultar em mudanças significativas para os militares e familiares, bem como determinar o desenvolvimento das operações militares.

Para analisar a influência das Redes Sociais nas Operações Militares, foi consultada bibliografia diversa e concernente à Força Aérea Portuguesa e a outras organizações congéneres. Concomitantemente procedeu-se quer à realização de entrevistas a militares da Força Aérea Portuguesa com conhecimentos e expertise nos assuntos abordados, quer ainda à realização de um inquérito junto dos militares que participaram em missões internacionais a partir do ano de 2012. Todos estes instrumentos permitiram evidenciar a existência de potencialidades e de perigos no uso de Redes Sociais em Operações Militares.

Concluiu-se pois, que as Operações Militares são potenciadas pelas capacidades das Redes Sociais, nomeadamente na aquisição de *Situational Awareness* e ainda que a falta de capacitação dos militares nesta área de missão comporta riscos, coletivos e individuais, o que poderá obrigar a Força Aérea Portuguesa a tomar medidas preventivas.

Palavras-chave: Redes Sociais, Operações Militares, Força Aérea Portuguesa, Guerra de Informação, *Situational Awareness*.

Abstract

This dissertation aims to determine how the use of Social Networks (SN) in military operations, either by the Portuguese Air Force (PAF), or by the military personnel, can influence these operations.

In this dissertation, it is assumed that the SN are a vital meeting point for communication between people. Under the military, this assumption is to consider that the Information Warfare occurs every day, silently, and that a "simple" publication may result in significant changes to the soldiers, relatives and for the progress of operations and also that, these publications, may enhance or harm the military operations.

To analyze the influence of social networks on military operations, diverse literature was consulted, concerning the PAF and other organizations. Concurrently was the realization of interviews to the PAF's military personnel with knowledge and expertise in the subjects addressed, and also, was carried out a survey among the military who participated in international missions from the year 2012. All these instruments have allowed evidence the existence of potentials and dangers in using SN in military operations.

Finally, it was concluded that the military operations are enhanced by the capabilities of the SN, in particular in the acquisition of Situational Awareness, but also concluded that the lack of military awareness about the SN dangers, entails collective and individuals risks, which may force the PAF to take preventive measures.

Keywords: Social Networks, Military Operations, Portuguese Air Force, Information Warfare, Situational Awareness.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Abreviaturas e Símbolos

C2 – Comando e Controlo

CAO – Civil Affairs Operations

DoD – Department of Defense

DON – Department of the Navy

DOTAF – Department of the Air Force

EMFA – Estado-Maior da Força Aérea Portuguesa.

FA – Força Aérea Portuguesa

FRI – Força de Reação Imediata

GI – Guerra de Informação

INFOPS – Information Operations

INTEL – Intelligence

NEPS - Notas de Execução Permanente

NSA – National Security Agency

OP – Opinião Pública

OPMIL – Operações Militares

OPSEC – Operations Security

ORDOPS – Ordens de Operações

OSINT – Open-Source Intelligence

RS – Redes Sociais

RSFA – Redes Sociais da Força Aérea Portuguesa

PSYOPS – Psychological Operations

RP – Relações Públicas

SA – Situational Awareness

TIC – Tecnologias de Informação e Comunicação

► – Este símbolo surge ao longo do desenvolvimento do trabalho e remete para a "Análise dos inquéritos (Anexo B)".

Página intencionalmente deixada em branco

Glossário

Blog – Diário mantido na Internet através de sistemas de publicação de fácil utilização.

Briefar – Esta palavra é usada diversas vezes neste trabalho para designar a ação de dar um briefing ou receber (“ser briefado”).

Briefing – Reunião onde se dão informações e instruções. No âmbito desta dissertação, entende-se como sendo um Briefing militar, onde o tópico de discussão são as Operações Militares.

Chat – É uma sessão de conversação entre duas ou mais pessoas na Internet, que pode ocorrer em *websites* dedicados ao Chat (como é o caso do mIRC) ou pode ocorrer através das plataformas de Redes Sociais (como é o caso do Facebook).

Convencional – Refere-se à comunicação, reportagens e noticiários televisivos.

Download – Cópia de informação de uma fonte central para um dispositivo periférico.

Forças amigas – Refere-se às próprias forças militares ou às forças militares dos aliados.

Guerra de Maomé – A “guerra de Maomé” é a expressão usada para designar a revolta do povo muçulmano contra a profanação do profeta Maomé.

Intranet – Rede ou *website* próprio de uma organização. É acessível apenas a membros autorizados.

Jamming – Visa negar as comunicações, bloqueando o sinal das mesmas, perda de informação e consequentemente afeta a tomada de decisão devido ao comprometimento da *Intelligence*.

Malware – *Software* desenhado para infetar um dispositivo eletrónico.

Mensagens Instantâneas – Também conhecido como *Instant messaging*, é um método popular de comunicação pela Internet através das sessões de *chat*.

Moral dos Militares – Para efeitos do estudo em causa assume-se como definição de “Moral” a vontade e coragem para servir a instituição militar e que pode ser incrementada por sentimentos de orgulho, bem-estar e confiança na instituição militar.

NEPS – Notas de Execução Permanente. É um documento promulgado pelo Comando Aéreo.

Online – Significa estar ligado a um servidor na Internet, o que permite interagir com esse servidor.

Opinião Pública – Representa o conjunto de opiniões partilhadas pela população, acerca de determinado assunto (por exemplo: política, economia, questões sociais e militares). A Opinião Pública é amplamente disseminada pelos meios de comunicação (por exemplo: as Redes Sociais).

ORDOPS – Ordens de Operações. É um documento promulgado pelo Comando Aéreo.

Post – Publicação nas Redes Sociais.

Preocupação Hierárquica – Por preocupação hierárquica entende-se como a preocupação das hierarquias competentes para criação das Ordens de Operações e outros documentos que devam refletir a adequada integração das RS nas Operações Militares.

Redes Sociais – São entendidas como Redes Sociais, as plataformas ou *websites* que permitem aos *users* socializarem através de diversas funcionalidades.

Selfies – É um estrangeirismo que designa uma fotografia tirada ao próprio.

Software – Conjunto de meios não materiais que servem para o tratamento automático da informação e permitem a ligação entre o homem e o dispositivo eletrónico.

Tweet – Publicação no Twitter.

Twitterer – Utilizador da plataforma Twitter.

Twitterverse – Universo de ferramentas associadas ao Twitter.

User – *Users* ou usuários é o nome dado aos utilizadores de uma Rede Social ou da Internet no seu sentido amplo do termo.

Viral – Refere-se a posts das Redes Sociais que pela sua natureza e conteúdo atraem milhões de pessoas.

Voice over IP (VoIP) – Significa *Voice Over Internet Protocol* e consiste numa ligação telefónica através da Internet em vez de ser através das linhas telefónicas

Website – É uma página ou um conjunto de páginas programadas que são executadas através de um Browser (Internet Explorer por exemplo). A cada página é atribuído um endereço WWW.

1. Introdução

"Estamos numa guerra e mais de metade desta guerra é disputada no campo de batalha que são os média." - Ayman al-Zawahiri, Julho de 2005

Neste capítulo dá-se a conhecer ao leitor qual é o tema tratado nesta dissertação, a importância que pode ter face ao contexto atual ao nível das Operações Militares (OPMIL) da Força Aérea Portuguesa (FA) relacionadas com as Redes Sociais (RS). É apresentado o objetivo e a origem do estudo em causa, a questão de partida e as questões derivadas, a metodologia e a estrutura que define esta dissertação.

1.1. Contextualização

No dia 29 de Dezembro de 1972 Edward Lorenz (meteorologista e matemático) deu nome ao tema da sua apresentação com a célebre e mítica questão acerca da imprevisibilidade da meteorologia: "O bater de asas de uma borboleta no Brasil pode provocar um tornado no Texas?" (Lorenz, 1972).

Atualmente retratada em músicas, filmes, livros, jogos, religiões e textos filosóficos, a ideia de Lorenz disseminou-se pela sociedade, com uma noção clara: uma pequena causa pode gerar enormes consequências (Ghys, 2012).

Ora, é esta realidade que nos serve para contextualizar o tema com o efeito borboleta de Lorenz, pois os média[1] são uma plataforma potenciadora deste efeito.

Vejamos. A 30 de Setembro de 2005 o jornal dinamarquês Jyllands-Posten, publicou uma série de *cartoons* onde caricaturava o profeta Maomé como um terrorista (BBC NEWS, 2006). Mais tarde, segundo a mesma fonte, o jornal egípcio Al-Fagr republica esses desenhos e descreve-os como um insulto aos muçulmanos e uma bomba de racismo. Consequentemente, os embaixadores de 10 países islâmicos mostram a indignação dos muçulmanos ao primeiro-ministro dinamarquês. Ainda assim, diversos jornais viriam a publicar novamente os *cartoons,* nos seguintes países: Alemanha, Itália, Espanha e França (BBC NEWS, 2006), entre os quais a revista satírica Charlie Hebdo (HA; SLATER, 2015).

[1] Segundo o Priberam [2013b], os média são todos os suportes de difusão de informação, onde se inclui a Internet.

Segundo a BBC News (2006), a revolta do povo muçulmano foi crescendo e culminou num ataque às embaixadas da Dinamarca e Noruega situadas em Damasco, Beirute e Teerão e às embaixadas Inglesas e Alemãs no Irão tendo morrido mais de 37 pessoas em 13 dias no mundo muçulmano (BBC NEWS, 2006). Em 2010, a "guerra de Maomé"[2] saltou para as RS, de acordo com Walsh (2010), levando a autoridade de telecomunicações do Paquistão a bloquear indefinidamente os acessos locais ao Facebook, em resposta a uma competição levada a cabo por um "grupo" nessa RS, que encorajava os *users* a publicarem desenhos do profeta Maomé, tendo como objetivo a "discussão livre da brutalidade dos radicalismos do Islão". Foram também bloqueados os acessos a um vídeo que mostrava a violência dos militares paquistaneses contra civis (Walsh, 2010). Ha e Slater (2015) referem que Charlie Hebdo continuou a publicar *cartoons* de diversas figuras, onde se incluía Maomé e sátiras aos *jihadistas*[3], resultando num ataque em 2011 com uma bomba incendiária às instalações e várias ameaças de morte que se mantiveram até 2015 (HA; SLATER, 2015). Não terminando por aqui, a "guerra de Maomé" culminou recentemente no assassinato de 17 pessoas (dos quais 8 jornalistas e 3 polícias) nas instalações do Charlie Hebdo, na rua e num supermercado (BBC NEWS, 2015).

Estes casos demonstram bem que pequenas causas podem gerar enormes consequências em todo o mundo. E é um pressuposto que hoje ganha maior relevo com a Internet e as RS, já que, segundo Castells (2004), a Internet está enraizada em todos os aspetos da vida das pessoas (Castells, 2004).

O enorme sucesso da Internet deve-se à capacidade de transmitir informação a todo o mundo desprezando grandezas físicas como a distância e a localização geográfica (PASTOR-SATORRAS; VESPIGNANI, 2004). Segundo um *website* de informações estatísticas, o número de utilizadores da Internet aumentou cerca de 10 vezes no espaço de 14 anos (estatísticas de 1999 a 2013). Segundo o mesmo, no início de 2015 existiam cerca de 3 mil milhões de utilizadores da Internet em todo o mundo, face a um total de população mundial de mais de 7 mil milhões, o que representa cerca de 40% da população mundial (ILS, [2015]).

Vivemos atualmente numa era onde a comunicação através da tecnologia digital prevalece na sociedade (RYAN; JONES, 2009) e uma das primeiras provas disso

[2] A "guerra de Maomé" é a expressão usada para designar a revolta do povo muçulmano contra a profanação do profeta Maomé.

[3] Segundo Zalman [2015], são indivíduos que acreditam que todos os Muçulmanos devem ser governados pelo Estado Islâmico e justificam as suas ações violentas nesta causa.

remonta a 1997. Segundo Boyd e Ellison (2007) foi nesta data que a primeira RS reconhecida, abriu portas para que milhões de pessoas comunicassem entre si. "SixDegrees.com" era o nome do *website* que se identificava como uma ferramenta para ajudar as pessoas a comunicarem mais facilmente. Em 2000 terminou o sucesso desta RS (BOYD; ELLISON, 2007) e deu lugar a que outras alcançassem o sucesso.

Foi o caso do YouTube, Facebook (que surgiram em 2005) e Twitter (que surgiu em 2006) (BOYD; ELLISON, 2007). As RS vieram igualmente a transformar a periodicidade com que as notícias são disseminadas. Deixou de haver tempo, passou a haver o "agora" (Baillie, 2014). As RS passaram também a ser uma ferramenta de revolução a que os protestantes recorrem para disseminar a informação, vejam-se os protestos árabes de 2011 (subcapítulo 4.5). Não há dúvida de que as RS emergiram tornando-se na forma de comunicação dominante na sociedade do século XXI (KASE et. al., 2014).

1.2. Motivação

"(…) a excelência suprema consiste em quebrar a resistência do inimigo sem combater" (Sun Tzu, 2009)

Com este trabalho o investigador pretende aprender e dar a conhecer ao leitor de que forma é que a FA está integrada no universo das RS, nomeadamente, aprender: se as RS são consideradas como uma potencialidade, na FA e fora da mesma; de que forma essas potencialidades podem ser aproveitadas para as operações; se existem riscos associados ao seu uso, se na FA existe consciência de alguns dos riscos e o que é feito no sentido de os minimizar. Neste sentido, o investigador sendo militar da FA, encontra motivação em estudar os tópicos supracitados e ajudar a instituição a reconhecer a importância do estudo das RS.

Ora, e seguindo o JP 2-0 (2007), a informação tem um valor maior quando molda ou contribui para o processo de tomada de decisão dos comandantes, pois fornece bons elementos para compreender o que poderá acontecer no futuro (JP 2-0, 2007). Tendo em conta que grande parte da comunicação atual é feita pelas RS, parte-se do pressuposto que interessa à FA como "uma organização ágil, flexível e inovadora" (FA, [2015]), explorar as potencialidades das RS para as OPMIL, nomeadamente a aquisição de *Situational Awareness* (SA) e *Intelligence* (INTEL).

"*By 'intelligence' we mean every sort of information about the enemy and his country: the basis, in short, of our own plans and operations*." Clausewitz, 1832 (2006).

1.3. Âmbito e Objetivo

Esta dissertação centra-se na análise do uso das RS, tanto pela FA, tanto pelos seus militares. O Objetivo é perceber como essa utilização poderá influenciar as OPMIL da FA. Consideram-se no âmbito deste trabalho OPMIL, as operações relacionadas com a segurança cooperativa ou com a segurança humana.

Assim, iremos estudar a forma como as RS podem potenciar o SA e incrementar ações de INTEL, favorecendo as OPMIL. Por outro lado procuraremos identificar a forma como o uso das RS pode facilitar a compreensão da Opinião Pública (OP) acerca das missões em curso. Finalmente iremos analisar como os militares usam as RS e como essa prática pode trazer riscos acrescidos às OPMIL. Todas as tarefas mencionadas surgem com a finalidade de responder à questão de partida do trabalho:

As Operações Militares da Força Aérea Portuguesa são potenciadas pelo uso das Redes Sociais?

Adicionalmente, procura-se também responder às seguintes questões:

–Q1. O uso de Redes Sociais em Operações Militares permite capacitar os militares com um melhor *Situational Awareness*?

–Q2. As Redes Sociais são plataformas potenciadoras da motivação dos militares envolvidos em Operações Militares?

–Q3. A utilização das Redes Sociais no contexto das Operações Militares tem influência na Opinião Pública?

–Q4. O uso de Redes Sociais incrementa o risco das quebras de segurança no âmbito da atividade militar?

Da problemática em estudo ressaltam conceitos que enformam esta investigação e constituem o modelo de análise na Tabela C-1 (Anexo C). Estes conceitos foram relacionados como constituintes das hipóteses que se apresentam de seguida.

- Relacionado com a Q1:

Hipótese 1 – O uso das Redes Sociais nas missões, permite capacitar os militares com um melhor *Situational Awareness*.

- Relacionado com a Q2:

Hipótese 2.1 – O uso das Redes Sociais pelos militares é um fator de motivação durante as Operações Militares.

Hipótese 2.2 – O uso efetivo das Redes Sociais da Força Aérea Portuguesa para divulgar as missões motiva e moraliza os militares destacados e contribui para a tranquilidade das suas famílias.

- Relacionado com a Q3:

Hipótese 3 – O uso das Redes Sociais, de forma individual e institucional, para potenciar a imagem da Força Aérea Portuguesa, influencia positivamente a Opinião Pública acerca das Operações Militares.

- Relacionado com a Q4:

Hipótese 4.1 – O uso de Redes Sociais durante as missões representa um risco de quebras de segurança, pondo em perigo as Operações Militares.

Hipótese 4.2 – A Força Aérea Portuguesa tem a preocupação devida em consciencializar os militares que ingressam nas Operações Militares, acerca do uso das Redes Sociais.

Hipótese 4.3 – Não está divulgada na Força Aérea Portuguesa informação sobre os perigos do uso das Redes Sociais.

1.4. Metodologia

Os objetivos desta dissertação serão alcançados recorrendo a uma metodologia de trabalho definida por uma sequência lógica e dividida em três fases: Rutura, Construção e Verificação (QUIVY; CAMPENHOUT, 1998).

Na Rutura, o objetivo é que o investigador esteja livre de influências, rompendo "com os preconceitos e as falsas evidências". É nesta fase que o investigador apresenta diversas questões que deverão ser respondidas, sendo esse o objetivo principal da dissertação. Essas questões dividem-se por ordem de importância, em grupos distintos mas complementares, assumindo as seguintes formas: Questão de Partida - que no fundo é a tese a defender. Esta é a questão que orienta o trabalho de investigação e à qual o investigador terá que conseguir responder; Questões Derivadas - são questões definidas pelo investigador cujas respostas irão sustentar a resposta à questão de investigação (Questão de Partida). Ainda nesta matéria, importa referir que cada pergunta

dará origem a uma hipótese, e o propósito da investigação é validar ou refutar as mesmas e desta forma responder às questões.

O objetivo da Construção é conduzir o investigador a uma “experimentação válida” pela formulação organizada de um mapa de ideias e conceitos que possibilitem explicar os fenómenos em estudo, elaborar o plano de pesquisa, saber quais os caminhos a seguir e as consequências que se devem esperar. O modelo de análise é parte integrante desta fase, onde o investigador se propõe a organizar o modelo de construção da dissertação, definindo os conceitos basilares em que a dissertação se insere, as dimensões associadas aos conceitos e a metodologia para validar cada uma das dimensões. Cada dimensão corresponde ao conhecimento literário que o investigador pretende adquirir e que irá enformar o trabalho.

A Verificação é a fase última e conclusiva da dissertação, onde por meio da investigação, serão validadas ou refutadas as hipóteses, que por sua vez responderão positiva ou negativamente às questões derivadas. Apuradas as conclusões intermédias por cada questão derivada respondida, o investigador fará a análise das mesmas e poderá concluir finalmente a Tese, respondendo à Pergunta de Partida no último dos capítulos, a "Conclusão". Fazendo a suma deste parágrafo, na Verificação, o investigador garante uma resposta à dissertação baseada nos factos que a sustentam.

As três fases da metodologia são constituídas por uma sucessão de operações, em permanente interação, e que estão divididas em seis etapas:

Etapa 1 – Pergunta de Partida: é uma pergunta que representa o fio condutor do estudo e exprime o que o investigador procura “saber, elucidar, compreender melhor”.

Etapa 2 – Exploração: leituras e entrevistas: nesta etapa, a leitura tem o objetivo reunir os conhecimentos relativos ao problema em estudo e as entrevistas conduzem à descoberta de aspetos importantes para o trabalho e moldam o campo de investigação das leituras.

Etapa 3 – Problemática: explorar as leituras e entrevistas e fazer um balanço. E depois confrontar as diferentes perspetivas possíveis que relacionam o estudo com a realidade. No fundo, é a abordagem que permite tratar o problema formulado pela questão de partida.

Etapa 4 – Construção do modelo de análise: consiste em construir e selecionar conceitos que se vão procurar validar através de indicadores de forma a conseguir dar resposta à questão partida.

Etapa 5 - Análise das informações: consiste em verificar e confrontar a informação, obtida pela observação, com as hipóteses formuladas, podendo as hipóteses ser refutadas ou não.

Etapa 6 – Conclusões: esta etapa compreende uma análise das linhas gerais seguidas pelo investigador, uma apresentação dos "contributos para o conhecimento originados pelo trabalho" e as considerações finais.

1.5. Panorâmica Geral da Dissertação

Esta dissertação encontra-se dividida em 8 capítulos organizados de forma coerente, possibilitando ao leitor a perceção da importância do estudo em causa.

O primeiro capítulo é a "Introdução", onde o investigador situa o trabalho no contexto das RS e apresenta os objetivos do estudo.

O segundo capítulo, a "Revisão de Literatura" conduz o leitor a uma contextualização conceptual, importante para a compreensão de toda a teoria que envolve o presente trabalho. Neste capítulo são abordados os conceitos teóricos que servem de base sustentadora ao estudo.

Do terceiro ao sétimo capítulo, o investigador faz o aproveitamento dos conceitos abordados na "Revisão de Literatura", bem como a análise do inquérito realizado e das entrevistas, de forma a sustentar a resposta ao objetivo do trabalho.

Finalmente, o oitavo capítulo, designado por "Conclusão e Recomendações", é onde o investigador faz a síntese do trabalho e tece as conclusões obtidas, a partir da solidificação de toda a investigação. Respondendo assim às questões derivadas e à questão de partida espelhadas no subcapítulo 1.3. Neste capítulo, o investigador aproveita ainda para recomendar estudos futuros que se relacionem com a temática em causa.

Página intencionalmente deixada em branco

2. Revisão de Literatura

Considera-se a leitura e compreensão deste capítulo de elevada importância no seio desta dissertação, na medida em que os conceitos e definições abordados são os pilares nos quais a mesma se sustenta. Toda a base teórica aqui compilada e fundamentada tem como função orientar o leitor para conceitos da Guerra de Informação aplicados à temática em causa.

2.1. A Evolução da Guerra

Segundo Waltz (1998), desde a Segunda Guerra Mundial, o aumento e melhoramento constante dos meios de obtenção, processamento e disseminação da informação fez acelerar a importância da informação no seio da guerra, de pelo menos 3 formas. Em primeiro lugar refere que as tecnologias de INTEL[4], vigilância e reconhecimento, têm vindo a aumentar a distância à qual os adversários podem ser observados e seguidos, aumentando assim o alcance a que as forças podem atuar. Em segundo lugar, menciona que as tecnologias de computação e comunicação que suportam as funções de comando e controlo (C2) foram responsáveis pelo aumento da velocidade de transmissão da informação para os órgãos de comando, bem como o aumento da frequência com que as operações podem ocorrer. Em terceiro lugar, e continuando a seguir Waltz (1998), surge a integração das tecnologias de informação no armamento, aumentando a precisão das trocas de informação e a letalidade dessas armas. As tecnologias de informação são um meio precioso para a obtenção de *Tactical Intelligence* ao mesmo tempo que se elimina as capacidades adversárias de inteligência e de aquisição de alvos (Waltz, 1998).

Diversos analistas reconhecem que os conflitos militares têm vindo a sofrer modificações significativas, evoluindo da destruição física massiva até à destruição precisa e destruição não física, recorrendo às tecnologias de informação que permitem ganho de INTEL (Waltz, 1998).

[4] Falamos em *Intelligence* (ou INTEL) quando adquirimos as mais variadas informações, e associamo-las a outras informações já previamente adquiridas acerca do ambiente operacional e do adversário em si (JP 2-0, 2007)

2.2. Transformações da Guerra

O desenvolvimento da tecnologia é responsável por gerar rápidas alterações na forma como a produção de riqueza e o poder bélico influenciam a ordem mundial, como refere Toffler (1993). Continuando a seguir o mesmo autor, vemos que o mundo está hoje dividido em nações com diferentes estados de desenvolvimento e maturidade, classificando-se assim cada nação quanto ao seu foco de riqueza e poder como: pré moderna (agricultura), moderna (industrial) ou pós moderna (informação). Em termos quantitativos não discretos e comparando os diferentes estados de desenvolvimento classificados anteriormente, são poucas as nações com capacidades pós modernas, isto é, com a capacidade de produção de riqueza e poder através do domínio da informação, enquanto as restantes nações são definidas pelas suas capacidades pré modernas (baseadas na agricultura) ou capacidades modernas (industriais) (Toffler, 1993).

Assim, na era pós moderna, a informação é o recurso central para a produção de riqueza e poder. Essa produção de riqueza é baseada no domínio da informação, ou seja, na criação de conhecimento e na produção baseada nesse mesmo conhecimento (Toffler, 1993).

As tecnologias de informação têm o potencial de alterar as estruturas das nações, que atualmente são definidas por fronteiras físicas que protegem propriedades reais. Na era pós-moderna, ocorre a transição da propriedade real para a propriedade do conhecimento e da informação. Por consequência, o papel dos estados-nação terá menor significância e a forma como os conflitos bélicos serão travados ao nível da informação sofrerá alterações (Waltz, 1998).

2.3. Informação

Desde sempre, a informação assumiu um papel fundamental na guerra e hoje em dia é um fator crítico para o sucesso militar e a tendência é que se torne cada vez mais importante no futuro (Jessop, 2007). A informação está associada aos processos, às pessoas e às tecnologias e quando é transformada em conhecimento adquire valor intelectual (Dinis, 2004), chamado de *Intelligence* por Waltz (1998).

Para os comandantes, a informação é crucial para que possam exercer a sua função primordial, comandar. Esta permite que o ciclo de decisão-execução funcione corretamente e sirva de guia às ações das forças para que consigam atingir os objetivos das OPMIL. A recolha das informações relevantes, o seu processamento e

disseminação é a chave para fornecer SA a toda a força, criando assim oportunidades para que se cumpra a missão (FM 100-6, 1996).

A era da informação na qual vivemos atualmente está a transformar todas as OPMIL devido ao aumento da quantidade e qualidade da informação que é fornecida aos comandantes. Um comandante que domine a informação, que consiga observar o campo de batalha, analisar eventos e disseminar a informação, tem em sua posse uma poderosa vantagem sobre o adversário, que pode mesmo ser decisiva (DOTAF, 1995). Segundo Waltz (1998) a informação é hoje uma arma de guerra muito valiosa e é um fator crítico para a vigilância, avaliação das situações e alternativas, estratégia e interpretação dos riscos para a tomada de decisão. Os melhores na guerra são os que analisam a informação possibilitando a presciência (Waltz, 1998).

2.4. Guerra de Informação

Segundo Kopp (2008), a Guerra de Informação (GI) como área doutrinada é muito recente, contando apenas com duas décadas de existência. No entanto, a prática e obtenção dos seus efeitos contam já com centenas de anos (Kopp, 2008)

Segundo o *Department of the Air Force* (DOTAF, 1995), a GI é definida como sendo qualquer ação de negação, exploração, corrupção ou de destruição da informação e processos da informação do adversário, ao mesmo tempo que se garante a própria proteção contra esse tipo de ações e são exploradas as próprias atividades militares (DOTAF, 1995). Waltz (1998) descreve essas ações:

Ações de destruição ou negação - visam causar a perda de dados ou o atraso da partilha dos mesmos, ou até mesmo a destruição dos serviços que tratam e partilham esses dados. São exemplos de contramedidas de destruição ou negação: o *jamming*, a sobrecarga de informação, ou a destruição eletromagnética ou física das conexões ou dos processadores (Waltz, 1998);

Ações de corrupção - assumem diversas formas, servindo os objetivos de substituir, inserir ou remover informações ou os próprios serviços. Este tipo de contramedidas inclui por exemplo, a disseminação de vírus em computadores e em bases de dados (Waltz, 1998);

Ações de exploração - são cumpridas de duas formas: a nível externo, tendo por base a observação visual; ou a nível interno, para conquistar o acesso a informação interna ou aos serviços depois de anular os serviços de segurança. Ambas as formas

de exploração têm como objetivo conseguir ter acesso a informações consideradas confidenciais (Waltz, 1998).

A GI é “irregular” quando o foco das operações (a população) e propósitos estratégicos visam conquistar, controlar ou influenciar a população, bem como o seu suporte através da política, métodos psicológicos e económicos (JP 1, 2007).

Segundo o mesmo documento, a GI pode manifestar-se de variadas formas e até na combinação entre elas, nas quais se incluem insurgência, terrorismo, operações de informação (desinformação, propaganda, entre outros), atividades criminosas organizadas (como o tráfico de droga), ataques e invasões (JP 1, 2007).

Continuando com o mesmo autor, quem pratica as diferentes formas de GI, sejam Estados ou grupos armados, têm o objetivo de comprometer a legitimidade e credibilidade dos adversários e isolá-los, física e psicologicamente da população. Procuram ainda, simultaneamente, reforçar a própria legitimidade e credibilidade para exercer autoridade sobre a mesma. As operações de GI focam-se na subversão, atrito e exaustão do adversário, enfraquecendo e corroendo o seu poder, influência e vontade de exercer autoridade política sobre a população (JP 1, 2007).

2.4.1. Guerra de Informação Pessoal

Hoje em dia a maior parte das pessoas tem pouco controlo sobre as informações armazenadas que às próprias dizem respeito, sejam essas informações verdadeiras ou falsas (Schwartau, 1994).

2.4.2. Guerra de Informação Corporativa

Segundo Haeni (1997), esta classe da GI ficou mais conhecida a partir da Guerra Fria onde ações de espionagem foram executadas com o propósito de alcançar a superioridade de informação face à nação adversária (Haeni, 1997).

Continuando com Haeni (1997), no ambiente altamente competitivo que hoje se vive em redor das organizações, tanto as corporações como os estados participam neste tipo de ações de espionagem e em ações de desinformação (Haeni, 1997).

2.4.3. Guerra de Informação Global

Haeni (1997) inclui nesta classe de GI a ação de roubar informações secretas e utilizá-las contra os adversários, num cenário de conflito entre indústrias, organizações globais de economia ou países inteiros ou estados (Haeni, 1997).

2.5. A informação nas Operações Militares

Para compreender a importância e influência da informação nas OPMIL, dão-se a conhecer os domínios definidos por Alberts (2001) e Waltz (1998):

2.5.1. Domínio Físico

Corresponde ao lugar onde existe o cenário que as forças pretendem influenciar. Este é composto por terra, mar, ar e espaço, sendo estes quatro ambientes que as ações militares ocorrem. No domínio físico estão montadas as plataformas e as redes de comunicações que interligam todos os elementos dessa força (ALBERTS et al., 2001).

Neste domínio ocorrem ataques físicos às infraestruturas que tratam a informação, às linhas de comunicação e aos computadores, que tanto podem ser destruídos como furtados, visando sempre influenciar a informação (WALTZ, 1998).

2.5.2. Domínio da Informação

É neste domínio que a informação habita e é nele que é criada, manipulada e partilhada. A existência deste domínio é importante para os combatentes, por permitir a transmissão de informações entre forças, bem como a execução de C2 por parte dos comandantes. É neste domínio que comunicamos uns com os outros, e por isso é fundamental que seja defendido (ALBERTS et al., 2001)

2.5.3. Domínio Cognitivo

É o domínio da mente, onde a perceção, consciência, compreensão, as crenças e valores residem. É nele que as decisões são tomadas com base no raciocínio e compreensão (ALBERTS et al., 2001). Este domínio comporta diversos fatores que influenciam o resultado dos conflitos: a liderança, a moral, a coesão, o treino e experiência, o SA e a OP (ALBERTS et al., 2001). Waltz (1998) acrescenta que é onde têm lugar os ataques à mente humana, exercendo influência através de propaganda, desinformação e outras que sirvam o mesmo propósito (Waltz, 1998).

Situational Awareness – Habita no domínio cognitivo e significa estar consciente e atento ao que nos rodeia. É uma capacidade que resulta da interação entre o conhecimento prévio e a perceção da realidade (ALBERTS et al., 2001).

2.6. Intelligence

Falamos em INTEL quando adquirimos as mais variadas informações, e as associamos a outras informações previamente adquiridas acerca do ambiente operacional e do adversário em si (JP 2-0, 2007). A INTEL difere da informação por

duas razões: permite a previsão de situações e circunstâncias futuras e permite distinguir as diferenças entre cada caminho de ação para que a melhor decisão seja tomada (JP 2-0, 2007).

2.6.1. Open-Source Intelligence

Segundo Richelson (2008), a Open-Source Intelligence (OSINT) consiste na INTEL adquirida a partir de fontes públicas como as RS e envolve a aquisição legal (ou seja, informação não classificada) de qualquer material transmitido de forma verbal, por escrito ou em formato eletrónico. Nestes incluem-se os jornais, revistas, noticiários, transmissões na rádio, televisão e diversos conteúdos disseminados na Internet (Richelson, 2008), entre os quais as RS.

2.7. Superioridade de Informação

A superioridade de informação pode ser definida como a aplicação de um conjunto de ações de obtenção, processamento e difusão de informações, ao mesmo tempo que se impede que o adversário faça o mesmo, constituindo assim uma vantagem informacional (JP 3-13, 2012). A força que tiver conseguido maior vantagem no domínio da informação, é quem detém a superioridade de informação, sendo que essa vantagem pode ser obtida através do efeito surpresa (ALBERTS et al., 2001).

2.8. Operações de Informação

As operações de informação (INFOPS) consistem no emprego de capacidades nas operações que visem influenciar, romper e corromper decisões do adversário ou direcioná-las a favor das tropas amigas (JP 1-02, 2010).

Já a NATO[5], define as INFOPS como as funções focadas no ambiente de informação, que consistem em analisar, planear, avaliar e integrar atividades desse ambiente, que possam afetar a moral, o raciocínio, compreensão e as capacidades dos adversários. Visam ainda dotar o comando de avaliações do ambiente de informação, bem como de mecanismos para planear e coordenar atividades que visem alcançar efeitos na informação, que sirvam de suporte aos objetivos operacionais (MC 422/4, 2012).

Segundo o Departamento do Exército Americano, as INFOPS ocorrem continuamente dentro do ambiente de informação militar, afetando o adversário e

[5] NATO refere-se à North Atlantic Treaty Organization. Consiste numa aliança entre vários países, com o propósito de salvaguardar a liberdade e segurança dos seus 28 membros (atualmente) (NATO, [2015]).

protegendo as capacidades das forças amigas de recolher informação, processá-la e direcioná-la para o ganho de vantagens em todas as OPMIL (FM 100-6, 1996).

Waltz (1998) divide as INFOPS em:

Operações Psicológicas (PSYOPS) - recorrem à informação para influenciar o raciocínio e perceção psicológica do adversário, como por exemplo: através de ataques de informação e deceção (Waltz, 1998);

Deceção Militar - é utilizada para enganar o adversário das intenções e/ou capacidades das forças amigas. Para o efeito, podem ser efetuados ataques físicos, eletrónicos e ataques de informação (Waltz, 1998).

Destruição Física - pretende eliminar alvos físicos, como infraestruturas, computadores, comunicações, fontes de energia e armas (Waltz, 1998).

Guerra Eletrónica - Neste âmbito, são efetuados ataques no espetro eletromagnético por forma a negar as informações que deveriam chegar aos sensores eletrónicos do adversário (Waltz, 1998).

Ataque à informação - através de meios não físicos, provocam efeitos que não são visíveis na entidade física onde está armazenada a informação. Estes ataques corrompem diretamente as bases de informação do adversário (Waltz, 1998).

Medidas de Segurança - visa impedir que o adversário conheça as capacidades e intenções das forças amigas, através da proteção das fontes de informação e dos processos. Para tal, são desenvolvidos serviços de segurança de computadores e da comunicação (Waltz, 1998).

Na Figura 1, o documento FM 100-6 (1996), sintetiza e simplifica os componentes das operações de informação. No centro da imagem, situam-se os três componentes das operações de informação que estão interrelacionados: as operações, os sistemas de informação e as informações de cariz relevante e INTEL.

As atividades das INFOPS encontram-se integradas numa dimensão maior de operações, que engloba o ambiente de informação global (FM 100-6, 1996).

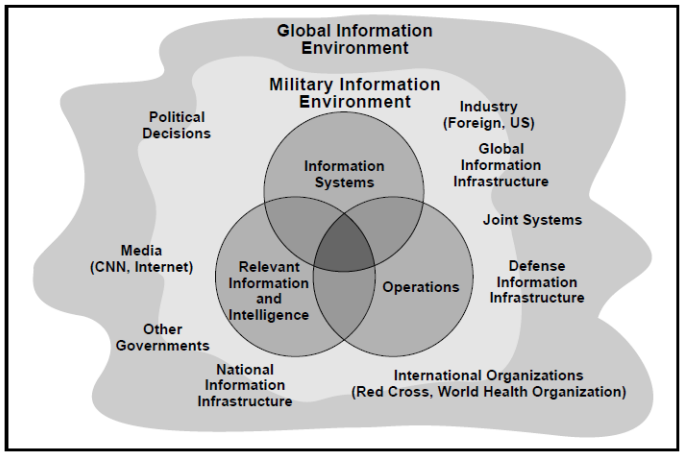


Figura 1 - Operações de Informação (FM 100-6, 1996).

2.9. Engenharia Social

Segundo ENISA (2008), a Engenharia Social compreende as técnicas aplicadas por um agente informático que visam aproveitar e explorar as fraquezas humanas e manipular as pessoas por forma a ultrapassar as barreiras de segurança. Este tipo de ataques consistem em convencer a(s) vitima(s) a fazerem determinadas ações contra a segurança e a divulgarem informações confidenciais. Segundo o mesmo autor, constituem um sério problema de segurança, na medida em que os *users*[6], são geralmente mais fáceis de manipular do que as tecnologias, no sentido de ultrapassar as barreiras de segurança (ENISA, 2008). Segundo o RFA 390-6, "a engenharia social consiste no conjunto de práticas usadas para obter acesso a informação ou aos sistemas que a processem, por meio de engano ou exploração da confiança das pessoas. Apenas uma formação de segurança adequada e contínua poderá preparar os utilizadores para lidar com quebras suspeitas de protocolo e procedimentos" (RFA390-6, 2011).

2.10. Information Security

A Information Security (INFOSEC) consiste na aplicação de medidas que protegem as informações processadas, armazenadas ou transmitidas pelos sistemas de informações e comunicações, contra a perda de confidencialidade, integridade ou

[6] *Users* ou usuários é o nome dado aos utilizadores de uma Rede Social ou da Internet no seu sentido amplo do termo.

disponibilidade, acidental ou intencional e visa ainda prevenir as perdas de integridade ou disponibilidade dos próprios sistemas (NATO, 2010).

2.11. Public Affairs Operations

Segundo o FM 100-6 (1996), a maior parte das OPMIL são conduzidas debaixo do olhar crítico e minucioso do público, que observa atentamente as informações disseminadas através dos média, acabando por funcionar como um grande fórum de debate público onde se possibilitam as análises e críticas dos objetivos, ações e conquistas dos militares. O impacto que os média têm no mundo e no planeamento e decisão política, estratégica e operacional, pode resultar tanto no sucesso das missões como no seu fracasso (FM 100-6, 1996).

Segundo o mesmo, quando comparado com o passado, a informação é hoje processada e transmitida quase em tempo real e para um público muito mais abrangente. Como tal, surge a necessidade da existência de militares, com a função de acompanhar a perceção que o público tem das OPMIL e face ao exposto, disseminar informações claras e objetivas acerca das OPMIL para o público (FM 100-6, 1996).

Ainda segundo o mesmo documento, os comandantes deverão saber usar as relações públicas (RP) como uma vantagem. Também os subordinados devem ser informados sobre o que devem fazer para que seja cumprida a missão, considerando para o efeito a influência que as RP têm no seu cumprimento. Desta forma, poderão combater mais facilmente os efeitos que a propaganda e desinformação exercida pelo adversário possa ter nas suas mentes (FM 100-6, 1996).

2.12. Relações Públicas Estratégicas

A velocidade a que as comunicações se processam pela internet é enorme (Kelleher, 2007), a partilha de informações ocorre quase em tempo real e é uma capacidade que representa tanto uma vantagem como uma vulnerabilidade (JP 3-13, 2012). Kelleher (2007) refere que as relações públicas estratégicas têm por base o planeamento, ação e a comunicação que são resultados de estudos de casos no âmbito das RP e da avaliação dos efeitos (Kelleher, 2007).

Num ambiente tão imprevisível e mutável como a internet, as organizações têm que conseguir responder rapidamente às situações que se lhes apresentam e quanto melhor for o planeamento estratégico, mais bem preparada estará a organização para

se adaptar à velocidade da informação *online* e responder aos desafios impostos pelo ambiente da informação (Kelleher, 2007).

2.13. Propaganda

Segundo Williams (2010), a propaganda tem como objetivo influenciar emoções, causas e o raciocínio, recorrendo à persuasão. Pode atuar como PSYOPS e através da internet ou outros média, resultando em impactos sociais e organizacionais. Refere ainda que para além de poder ser uma vantagem também pode representar um elevado risco e ameaça para as organizações dada a facilidade com que a informação pode ser manipulada para denegrir um alvo (Williams, 2010). Também Bernays (1928) descreve a propaganda como uma forma de manipulação consciente e inteligente dos hábitos e opiniões das pessoas (Bernays, 1928).

2.14. Sistemas de Informação e Comunicações

Segundo o RFA 390-6, os Sistemas de Informação e Comunicações (SIC) têm como funções o armazenamento, processamento e transmissão de informação. No âmbito da FA, alguns destes sistemas representam uma importância crítica para o cumprimento da missão e possuem, em diferentes graus, vulnerabilidades a ameaças que poderão ser concretizadas por diferentes agentes (internos ou externos) (RFA390-6, 2011). Os SIC contemplam um conjunto de componentes que trabalham em conjunto para a recolha, recuperação, processamento, armazenamento e distribuição de informações, com o intuito de facilitar o planeamento, controlo, coordenação, análise e decisão nas organizações (LAUDON; LAUDON, 1999).

2.15. Tecnologias de Informação e Comunicações

"O crescimento explosivo das tecnologias de informação e comunicações (TIC) e a sua penetração global têm especial incidência na comunidade militar, dada a elevada complexidade dos sistemas e equipamentos que utiliza e da dispersão geográfica em que opera, tornando-a um alvo especialmente apetecível pela sua visibilidade internacional e pela gravidade das consequências que podem resultar num "ciberataque" (RFA390-6, 2011). As TIC permitem o acesso à informação através das telecomunicações, onde se inclui a Internet, telemóveis e outros meios de comunicação (TechTerms, 2010). Atualmente, as TIC permitem a comunicação em tempo real através de diversos serviços como mensagens instantâneas, *voice over IP*

(VoIP), videochamadas e as RS onde as pessoas comunicam regularmente (TechTerms, 2010).

2.16. Web 2.0

O termo Web 2.0 surgiu inicialmente com Darcy DiNucci em 1999 (Ammunition, [2007]) e foi depois popularizado por Tim O'Reilly em 2004 na primeira conferência acerca da Web 2.0. Esta é a evolução da web 1.0 e foi uma transformação tão significativa que muitas empresas colapsaram por não terem acompanhado a evolução para a web 2.0 (O'Reilly, 2005).

Segundo o mesmo, na web 1.0, os *websites* caraterizam-se pela comunicação unidirecional, em que o *user* se limitava a receber a informação que os programadores dos *websites* publicam, pois para o fazer, são necessários conhecimentos técnicos (O'Reilly, 2005). Em 1.0 a comunicação é feita do programador para o *user*, ou seja, "eu publico, tu lês, eu forneço" (Carrera, 2009:39). Segundo O'Reilly (2005), com a evolução para a Web 2.0, o *user* passou a ter um papel dinâmico nos *websites*, onde foram incorporadas funções de edição e passaram a funcionar como aplicações ou programas que podem ser atualizados a partir de qualquer computador e utilizador. Desta forma, os *users* passaram a contribuir para o conteúdo dos *websites* (O'Reilly, 2005) onde a comunicação passou a ser bidirecional e partilhada, ou seja "Nós publicamos, nós lemos, nós partilhamos" (Carrera, 2009:39). E foi neste ambiente que cresceram as RS.

2.16.1. Redes Sociais

As RS são plataformas que habitam na Internet e que permitem aos *users*: construir um perfil de caráter público ou privado; gerir listas de pessoas com quem tencionam conectar-se; visualizar e percorrer a própria lista de conexões e a lista de conexões de cada pessoa dentro desse sistema (BOYD; ELLISON, 2007). Permitem ainda a partilha de interesses, experiências, informações que podem ser partilhadas e respondidas por outros e também ver, partilhar e responder às publicações dos outros *users* (NSA, [2009]). Segundo o mesmo, as RS permitem vários métodos de interação através de aplicações associadas como jogos, mapas interativos onde constam os locais visitados pelos *users*, ferramentas de mensagem privadas com vídeo ou através das publicações de fotografias, vídeo e/ou texto. Muitas RS permitem também que os *users* acedam às contas por telemóvel com acesso à Internet a partir

de qualquer parte do mundo e atualizar o perfil, fazer publicações com ou sem identificação geográfica entre outras opções (NSA, [2009]).

Segundo o RFA 390-6 (2011), as RS são um fenómeno transversal a toda a sociedade onde as pessoas e as organizações se expõem. “São o campo de excelência para a aplicação de técnicas de engenharia social e a propagação de *malware*, como revelam os constantes ataques a estas plataformas[7] com a quebra das *passwords* de acesso e a divulgação e análise das informações e dos detalhes pessoais dos utilizadores (RFA390-6, 2011).

[7] O relatório anual da Symantec sobre ameaças à segurança na Internet revela um aumento significativo dos mesmos (81% dos ataques são de engenharia social e malware) (Symantec, 2013).

3. Identificação e capacidades das Redes Sociais

Este capítulo tem como foco principal dar a conhecer ao leitor algumas plataformas de RS que pelas suas caraterísticas podem potenciar as OPMIL. As RS abordadas serão o Facebook, o YouTube e o Twitter.

3.1. Facebook

O DoD[8] considera o Facebook a derradeira ferramenta das RS uma vez que combina os elementos das outras RS como o Twitter e o YouTube. O Facebook é atualmente uma necessidade para os negócios *online*, *blogs*, RP, jogos de computador, partilha de fotografias e vídeo e atividade social (DOD, [2015a]) Esta plataforma tinha em janeiro de 2015, o maior número de contas ativas em todo o mundo, contando com mais de um mil milhão (Statista, [2015a]).

No Facebook os *users* são identificados por um perfil que criaram. Na página do perfil é possível ver os amigos e os amigos em comum, informações, gostos (por livros, grupos, músicas, filmes, personalidades e tudo o que se possa imaginar), locais frequentados, atividades recentes, fotografias, vídeos, grupos em que o *user* esteja registado, o contacto e morada do *user* (se este tiver disponibilizado) e o mural (onde constam as publicações ou *posts* que tenham sido feitas no perfil, pelo próprio ou por terceiros e que podem ser diretamente comentadas, fazer "Gosto" ou partilhar) (Wisegeek, [2015a]). Cada elemento referido pode ser visto em maior detalhe se clicado, podendo obter-se mais informações. Os *users* também podem fazer (clicar em) "Gosto" quando gostam de uma publicação no Facebook (Wisegeek, [2015a]).

Os *users* têm a possibilidade de procurar por grupos de interesse, amigos ou qualquer pessoa que esteja registada no Facebook e ver o perfil da mesma, se este for público. Caso contrário, se for um perfil privado, significa que só as pessoas que o *user* autorize podem ver o seu perfil. Nesse sentido, um *user* que queira ver um perfil ou um grupo privado terá que enviar um pedido de amizade ou enviar um pedido de acesso ao grupo, respetivamente. A procura por pessoas pode ser feita procurando por um endereço eletrónico, por escola, universidade, trabalho ou escrevendo o nome da pessoa ou a localidade em que vive (ou melhor, a que tem registada no Facebook). No âmbito da pesquisa, à semelhança do Twitter é possível a criação de *hashtags*

[8] DOD refere-se ao Departamento de Defesa dos Estados Unidos da América (U.S. *Department of Defense*).

para ir diretamente à página de interesse, como será explicado no subcapítulo 3.3 (exemplo de *hashtag*: #JeSuisCharlie) (Facebook, [2015]).

A caraterística mais popular do Facebook é a publicação (*post*) de fotografias, que podem ser carregadas e publicadas diretamente por telemóvel, câmara ou computador, entre outras formas possíveis. É possível publicar fotografias, vídeo e texto, no próprio perfil, no perfil de outras pessoas ou em grupos. Os *users* têm a possibilidade de estabelecer privacidade nas publicações que as vejam apenas quem se quer (Facebook, [2015])

O Facebook conta também com serviço de mensagens privadas, e é possível enviar uma mensagem a qualquer pessoa, esteja ou não no núcleo de amigos do *user*. Na secção do *chat* é possível visualizar todos os amigos que se encontram *online* (ou seja, todos os estão conectados ao Facebook e declaram-se como "disponível") (Facebook, [2015]).

Como se pode verificar, o Facebook é uma plataforma multifacetada que disponibiliza inúmeras ferramentas, de fácil utilização, e que permite a difusão instantânea de informação sobre formas variadas: texto, imagem e vídeo.

3.2. YouTube

Segundo o DOD ([2015a]) o YouTube é o *website* de partilha de vídeo por excelência. Nesta RS, os *users* podem publicar e partilhar vídeos que vão desde as notícias online amadoras até vídeos de música. Podem criar respostas a vídeos (colocando a hiperligação num comentário a um vídeo), comentar vídeos e classificá-los. O YouTube transformou os vídeos *online* num fenómeno social (DOD, [2015a]).

Esta RS conta com milhares de milhões de utilizadores e disponibiliza um "fórum onde as pessoas podem interagir, informar e inspirar outras pessoas em todo o mundo (…)" (YouTube, [2015a]).

Como se verifica, esta RS permite a difusão de vídeos, que podem ser editados, legendados e trabalhados para depois serem publicados de forma *online*. Para além disso, o YouTube permite a publicação de vídeos ao vivo e em direto. Esta vantagem acresce à simplicidade de uso e torna-o como uma ferramenta de eleição para a disseminação do *Awareness*.

3.3. Twitter

O Twitter conta com cerca de 284 milhões de contas ativas por mês (Socialbakers, [2015]) e segundo o DoD ([2015a]) é uma RS bastante distinta das outras, na medida em que é uma plataforma de *microblog*, ou seja, permite criação de mensagens com apenas 140 caracteres. O objetivo é que as mensagens sejam rápidas e claras, sejam elas acerca de notícias do dia ou partilha de fotografias. O DoD ([2015a]) acrescenta ainda que o Twitter está desenhado para ser muito sensível ao tempo, na medida em que as informações são disseminadas em tempo quase real. Aliás, muitas notícias são hoje disseminadas em primeira mão através dos *tweets*, i.e. mensagens (ou *posts*) que os *users* (ou *twitterers*) criam no Twitter, ou ainda através de *retweet* (partilhar um *tweet* que outro *user* fez) (DOD, [2015a]). Estes *tweets* podem ser feitos através do próprio Twitter, através de mensagens de texto SMS, mensagens instantâneas, correio eletrónico, ou através de *websites* e aplicações (ferramentas) associadas ao Twitter (Beal, 2010).

PSimões (2015) [9] refere que ao contrário do Facebook, o Twitter é uma RS muito mais aberta, no sentido de que em seu redor existem inúmeras ferramentas que são possíveis interligar para os mais variados fins. Todas essas ferramentas habitam num universo digital, o *twitterverse* (ver a Figura 2). Estas aplicações permitem as mais variadas funções, como agendar *tweets*, elaborar estatísticas de *tweets*, manipular várias páginas de diferentes RS, pesquisar por palavras-chave, visualizar mapas de *tweets* geolocalizados, estudar as ações de um determinado *twitterer* (ou seja, como esse *user* usou o Twitter em determinado período de tempo) entre outras milhares de funções. Ainda segundo o mesmo, é possível extrair diversas informações de cada *tweet,* como: quem o publicou, onde, quando, a partir de que tipo de equipamento (por vezes conseguindo-se até saber a marca e modelo do equipamento que publicou), com que aplicação foi publicado, entre outras informações (PSimões, 2015).

O Twitter é uma plataforma na qual as pessoas publicam aquilo que fazem em determinado momento. Devido ao facto de ser uma plataforma de *microblogging*, em 140 caracteres torna-se difícil fazer algo mais do que dizer exata e sucintamente o que se pretende (Wisegeek, [2015b]).

[9] O Major Paulo Simões está colocado na Divisão de Recursos e é investigador na área das RS. É também um orador convidado em várias conferências internacionais onde palestrou sobre o uso das plataformas de RS.

Os *users* têm um perfil que podem tornar privado ou público e atualizar de variadas formas, podem fazê-lo diretamente através do *website* do Twitter, ou por mensagem através de correio eletrónico ou através de diversas aplicações (Wisegeek, [2015b]). Os *users* podem ainda "seguir" outros *users* para serem notificados das atualizações. São muitas as pessoas que atualizam os perfis hora a hora, transformando o Twitter numa RS com informação bastante atualizada. São também muitas as pessoas que sentem a necessidade de estarem constantemente a atualizar o perfil e a pesquisar os perfis de outros *twitterers*. Ainda segundo o mesmo, no Twitter existem grupos privados ou públicos, que várias vezes são criados para cobrir eventos reais em tempo real, com *tweets* em tempo real (Wisegeek, [2015b]).

A utilização dos *hashtags* é uma forma dos *users* organizarem os seus *tweets* para os motores de busca do Twitter. Os *hashtags* ajudam outros *users* a encontrarem *tweets* que lhes interessem quando pesquisam no Twitter. Não são mais do que um título curto que define o *tweet* e é feito como no exemplo: #títulocurto (Beal, 2013).

Como se verifica, o Twitter sendo uma plataforma de *microblogging* e com inúmeras ferramentas associadas, é uma potente plataforma de disseminação de informação em tempo real.

Figura 2 - *Twitterverse* de Brian Solis e JESS3 (Solis, 2011)

4. As Redes Sociais e o Situational Awareness

No capítulo anterior analisámos as potencialidades das RS, nomeadamente do Facebook, YouTube e Twitter. Vimos que estas redes possuem milhões de utilizadores ativos e diferentes formas de produzir e disseminar informação. Iremos agora abordar as RS como uma ferramenta com potencialidades ao nível do ganho de SA. Para isso daremos a conhecer diferentes realidades onde é possível usar as RS com essa vantagem, nomeadamente: apoio à população, causas humanitárias, controlo epidémico, causas políticas e sociais, e por fim as OPMIL e a importância das RS neste âmbito.

4.1. Introdução à temática

Através das RS podemos almejar uma vantagem operacional face ao adversário, nomeadamente a obtenção de um SA em tempo quase real. Esta vantagem consiste em recolher e agrupar informações obtidas ao nível das RS e interpretá-las de forma a conseguir antecipar futuros eventos (OMAND; BARTLETT; MILLER, 2012).

As pessoas continuam a abraçar as novas tecnologias e nesse sentido o uso das RS irá aumentar. À medida que a popularidade das RS aumenta, um nº significativo de pessoas irá escolher as RS como fonte de informação principal (Lindsay, 2011) e também como meio de transmissão de informação. Segundo Kase (et al. 2014), uma importante característica das RS no que concerne à disseminação de informação é que cada *post* resulta numa transmissão mundial de gigantescas quantidades de informação pública que passa a estar disponível a todos (KASE et. al., 2014). As estatísticas acerca do Twitter e Facebook são surpreendentes, na medida em que, por dia, são feitos mais de 500 milhões de *tweets* no Twitter e existem, neste momento, mais de 1 340 000 000 contas ativas no Facebook (Socialbakers, 2015a, 2015b). As RS conduziram a um crescimento exponencial da velocidade de difusão de informação e alcance (KASE et. al., 2014).

A análise do tráfego das RS pode potenciar a capacidade de previsão de certos acontecimentos, aumentando a rapidez com que se identificam eventos emergentes, impulsionando desta forma o SA que, por vezes pode ser mais rapidamente adquirido através das RS do que pelas fontes de informação tradicional (OMAND; BARTLETT; MILLER, 2012). Extrapolando para as OPMIL, também neste universo podem ser obtidas informações importantes autonomamente, por parte dos militares destacados,

muito antes de essa informação chegar pelas fontes oficiais, nomeadamente pelas equipas de INTEL. Segundo Gonçalves (2015)[10], um dos problemas vividos em operações no Afeganistão era a desatualização da informação, referindo que "a informação social desatualiza-se muito rapidamente (…) apenas duas vezes por dia era enviado aos militares das Nações Unidas reportes de informação pelo que, as pessoas tinham que explorar as RS no sentido de encontrar mais informação que lhes fosse útil" (Gonçalves, 2015).

"É incrível a informação atual que se obtém em tempo quase real a partir das RS" (Gonçalves, 2015) seja num cenário de conflitos, seja num cenário de catástrofe ou de emergência, onde a informação quer-se de forma rápida, precisa e atual, tal como veremos adiante.

As RS são atualizadas por todas as pessoas desse sistema, resultando na vantagem de ter informação extremamente atualizada e precisa (Gonçalves, 2015). Mais, recorrendo às vantagens da geolocalização (processo incorporado nos equipamentos *Smartphone*, por exemplo) poderíamos ter a capacidade de mapear todos os eventos violentos e caracterizá-los por ordem de probabilidade de acontecimento, através da análise de *tweets* geolocalizados, por exemplo. Facilitando assim o ganho de SA e que se poderia converter numa resposta mais rápida, efetiva e ágil contra as ameaças (OMAND; BARTLETT; MILLER, 2012).

As particularidades das RS fazem delas um mundo atrativo dentro de um gigantesco universo chamado Internet. Nesse mundo, caraterizado pela variedade de ambientes, uns pacíficos e outros hostis, habitam todos os dias mais de 800 milhões de *users* no Facebook (Socialbakers, 2015b), sendo esta plataforma apenas uma entre tantas outras que os habitantes exploram para satisfazer as suas necessidades. Segundo Sedra (2013), as pessoas e as organizações confiam cada vez mais nas RS para aumentar os níveis de *Awareness*. As notícias espalham-se rapidamente através das publicações de vídeos, *tweets* e comentários no Facebook, dando lugar a uma nova geração de jornalistas: os cidadãos jornalistas. Graças à proliferação dos telemóveis com câmara e acesso imediato às RS, qualquer cidadão pode desempenhar a função de jornalista e disseminar ao vivo uma dada ocorrência (Sedra,

[10] O Tenente-Coronel Paulo Gonçalves é Chefe da Repartição de Planeamento Operacional e Doutrina e desempenhou funções como Military Liaison Officer no Afeganistão durante 2 anos. Participou em missões da NATO, da União Europeia e das Nações Unidas. Enquanto esteve no Afeganistão, foi conselheiro das Nações Unidas e geria grandes quantidades de informação. Uma das ferramentas que utilizou para a gestão de informação foram as RS.

2013). Estatísticas demonstram que atualmente, cerca de 80% dos *users* de Facebook e Twitter acedem às contas maioritariamente por telemóvel (Socialbakers, 2015a, 2015b).

Sedra (2013) refere que cada vez mais pessoas são convertidas a fazer jornalismo amador, saltando para as ruas e publicando nas RS os acontecimentos em tempo real. A revolução no Egipto mostrou claramente como as novas tecnologias coligadas às RS se podem transformar radicalmente, deixando de ser um meio de entretenimento para ser uma poderosa ferramenta para o ativismo politico e uma fonte primária de informação e SA, permitindo compreender o que se passa num dado local sem sair de casa ou do local de trabalho (Sedra, 2013). Em OPMIL, tal assume uma importância acrescida, pois tal como refere Gonçalves (2015), no contexto de operações num cenário hostil, a pessoa mais importante para a segurança coletiva e individual, executa o seu trabalho atrás de um computador na procura de informações críticas nas RS (Gonçalves, 2015).

As RS têm um elevado potencial de disseminação de informação e é importante que os comandantes da FA tenham esta consciência para que, face a um evento crítico, seja em operações internacionais ou em território nacional, tenham a capacidade de responder rapidamente, interpretando as informações dispostas nas RS e reconhecendo as consequências que certas informações podem ter para atuarem em conformidade. Por exemplo, segundo o OTCPA (2011), a situação que se viveu em 2009 na base militar dos Estados Unidos da América (EUA) é demonstrativo da rapidez e capacidade de disseminação das notícias e informação ao nível das RS. Serve o mesmo exemplo para o alerta e tomada de consciência dos comandantes acerca das potencialidades das RS (OTCPA, 2011).

Caso Estudo: Fort Hood Shootings, 2009

No dia 5 de Novembro de 2009, um militar Americano atacou com armas de fogo outros militares da base, resultando num cenário sangrento. O evento em Fort Hood, uma base militar do Texas, resultou em 13 mortos e 30 feridos depois de um ataque levado a cabo pelo Major Nidal Malik Hasan, um psiquiatra que estava prestes a ser destacado para uma missão (KENNEDY; MOORE, 2009).

Imediatamente após o tiroteio, as pessoas conectaram-se à Internet à procura de informação nas RS, nomeadamente no Twitter e Facebook e até os órgãos mediáticos estavam conscientes que a informação mais atualizada acerca do evento estava a ser despejada nas RS (OTCPA, 2011). No entanto, veio a revelar-se que

muita dessa informação não passava de especulação. Segundo a mesma fonte, nas horas que se seguiram, foram dadas conferências de imprensa com o objetivo de esclarecer certas informações não confirmadas que estavam a circular nas RS. Cada vez mais comandantes nos EUA estão conscientes desta realidade e encaram a necessidade de ter uma ferramenta dinâmica inserida nas RS, destinada a comunicar com o público durante situações críticas como esta (OTCPA, 2011).

Vejamos então, em que medida as RS se encontram enraizadas na Sociedade da Informação[11] e de que forma potenciam o SA em diferentes cenários.

4.2. Catástrofes e Emergências Sociais

Um estudo efetuado pela Cruz Vermelha Americana em 2009 demonstrou que as RS são a 4ª fonte mais popular no que toca a encontrar informações acerca das situações de emergência. O estudo indica ainda que, um em cada cinco *users,* publicam relatos de vítimas de situações de emergência (ARC, 2010).

As RS são um contributo para o SA em situações de emergência, como as catástrofes naturais por exemplo. Segundo (Palen, 2008), as RS são frequentemente utilizadas com o intuito de disseminar alertas acerca de áreas ou situações potencialmente perigosas, dar a conhecer às pessoas mais chegadas em que condições se vive num local afetado e ainda para angariar fundos em prol dessas localidades afetadas por catástrofes. Segundo o mesmo, as RS podem ser usadas como uma ferramenta de gestão de emergências, com as seguintes funções: efetuar alertas de emergência – o que potencia o SA global; receber pedidos de assistência por parte das vítimas; monitorizar as ações e *posts* dos *users* potenciando assim o SA – o que permite que as equipas de socorro atuem mais eficazmente; estimar os danos sofridos na localidade, através da visualização das imagens e vídeos que os *users* publicam nas RS acerca do mesmo evento (Palen, 2008).

Por exemplo, durante um tiroteio na universidade Virginia Tech, que ocorreu em 2007, os alertas pela internet foram disseminados em primeiro lugar pelos estudantes e fontes não oficiais (Palen, 2008).

Não há dúvidas de que as RS têm uma função importante durante as situações de emergência, tal como se verificou na atuação por parte dos militares do exército

[11] "Sociedade da Informação" foi um conceito abordado e desenvolvido por vários autores como Castells (2000) e é também reconhecida na "Terceira Vaga" de Toffler (1980).

dos EUA que, face aos tiroteios em Fort Hood, usaram o Twitter para ir atualizando as pessoas acerca da situação (Beizer, 2009).

Segundo Scott Testa, um professor especialista em RS, as RS têm ruído, que pode ser abafado através das publicações. O mesmo refere que depois do tiroteio surgiram reportes de ocorrência que careciam de confirmação ou que conflituavam com outros reportes e o Twitter foi como um filtro usado para confirmar ou refutar as histórias que pairavam sobre os acontecimentos (Beizer, 2009).

4.2.1. Ruído de Informação

O ruído das RS não potencia o SA, antes pelo contrário, segundo Gonçalves (2015) um dos perigos das RS é a má informação que circula (entenda-se ruído). Ainda assim, comparando as RS com os órgãos de comunicação convencionais, nomeadamente os média televisivos, as RS conseguem ter informação mais atual, num espaço de tempo muito reduzido, dando origem a atualizações praticamente em tempo real. Continuando a seguir Gonçalves (2015), apesar do elevado ruído existente nas RS, o número de testemunhas reais dispostas a relatar os acontecimentos é igualmente elevado (Gonçalves, 2015) (denominados cidadãos jornalistas por Sedra (2013).

Passemos aos números. No início de 2012, os EUA tinham uma população de cerca de 313 milhões (USCB, [2015]). Desses, cerca de 57 600 profissionais trabalhavam nas áreas da comunicação mediática, onde se incluem os repórteres televisivos (USBLS, 2014). Ou seja, cerca de 0,02% da população dos EUA. Por outro lado, dentro da população dos EUA, existiam em 2012 cerca de 143,4 milhões de *users* de Facebook (Statista, [2015b]), dos quais 97,8% acederam ao Facebook por telemóvel em 2012 (Statista, [2015c]). O que significa que cerca de 140,2 milhões de Americanos, acediam ao Facebook através de telemóvel, isto é, cerca de 45% da população dos EUA.

Na Tabela 1, comparam-se as estatísticas:

Tabela 1 - Relação entre a quantidade de jornalistas profissionais e potenciais cidadãos jornalistas.

	EUA, 2012			
	População Total	Jornalistas profissionais	Potenciais cidadãos jornalistas	Diferença
Numeração Cardinal	313 372 918	57 600	140 200 000	140 142 400
%	100%	0,02%	45%	44,98%

Se assumirmos a perspetiva de Sedra (2013) no que concerne ao conceito de cidadão jornalista, podemos concluir que o cidadão jornalista é qualquer cidadão com a capacidade de relatar e/ou gravar um evento (nos formatos de vídeo, fotografia e/ou áudio) em tempo real e disseminá-lo através das RS, como o Facebook, em tempo quase real. Veja-se um exemplo de cidadão jornalista mencionado por Sedra (2013), Sharif Abdel Kouddous.

Foi nesta base que a Tabela 1 foi construída, com o objetivo de demonstrar a diferença entre as duas dimensões, jornalistas profissionais vs. cidadãos jornalistas e com isso concluir que, num universo tão desproporcional, é natural que existam imensas informações falsas, o que não invalida que existam também muitas informações verdadeiras e importantes. Aliás, Gonçalves (2015) refere, com base na experiência em OPMIL da FA, que as pessoas respeitam muito o que é dito nas RS e por uma questão de segurança global e individual, os cidadãos têm interesse em publicar informações fidedignas que potenciem o SA de todos (Gonçalves, 2015).

Ainda assim, o universo dos cidadãos jornalistas de 2012 poderá não ter sido tão grande quanto os 140 milhões enunciados e por essa razão se classificam como potenciais cidadãos jornalistas, o que significa que, mesmo não tendo a oportunidade de presenciar um evento e publicá-lo nas RS, são cidadãos que a qualquer momento o poderão fazer por 2 razões:

- Possuem telemóvel com acesso ao Facebook, podendo publicar;
- Poderão a qualquer momento presenciar um evento, gravá-lo e publicá-lo e/ou relatá-lo.

Um outro exemplo do referido surgiu no decorrer dos incêndios no Estado da Califórnia em 2007 (Palen, 2008). As pessoas que habitavam na região afetada recorreram às RS para obterem o máximo de informação acerca dos fogos, já que as notícias televisivas eram generalistas e muitas vezes incorretas. Através da análise das informações que circulavam nas RS era possível desenhar o mapa dos acontecimentos (onde constavam estradas fechadas, focos de incêndio e posições de abrigos) (Palen, 2008). Neste incidente, os fóruns onde se discutiam os acontecimentos foram vistos como fontes de informação espantosamente fiáveis onde as pessoas partilhavam e recolhiam informação extremamente atualizada e precisa (Palen, 2008).

As RS podem ser usadas para alertar quando uma emergência ocorre, monitorizando o fluxo de informação que provém de diferentes fontes durante um

incidente. Essa monitorização é feita através da identificação, processamento e compreensão dos elementos críticos de uma dada situação (Lindsay, 2011). A obtenção de SA em tempo quase real, imediatamente depois dos eventos ocorrerem, pode ajudar a perceber onde estão as pessoas, assistir as vítimas e alertar as pessoas para as mudanças no cenário e novas ameaças que surjam (Lindsay, 2011).

Esta possibilidade de usar a Internet em situações de emergência coloca de parte os problemas criados pela saturação das linhas telefónicas que muitas vezes impede a assistência a quem necessita urgentemente. Esta capacidade é extremamente potenciada pela evolução exponencial que a tecnologia ao nível das telecomunicações tem sofrido, nomeadamente no que concerne ao uso dos *Smartphones*, que hoje em dia são em muitas partes do mundo, uma tecnologia acessível a todos e muito difundida (DAWSON; HILL; BANK, 2013). A propósito, quando em missão no Afeganistão, Gonçalves (2015) observou este fenómeno, a banalização dos *Smartphones*. Notando que, até quem vivia em condições precárias e nas zonas mais remotas, tinha um bom telemóvel capaz de aceder à Internet e com câmara de fotografar/filmar. Diz ainda que, cerca de 80% dos afegãos são analfabetos mas têm telemóveis e sabem telefonar e gravar vídeos ou fotografar. Ainda que não se consiga aceder à Internet, é possível comunicar por chamada telefónica, o que significa que todas as informações pertinentes se sabem graças à proliferação dos telemóveis, tornando a rede social afegã muito potente no que concerne ao ganho de SA (Gonçalves, 2015). Neste sentido, também EC (2015) afirma que no Afeganistão, o acesso à Internet é quase geral, possuído por todos, considerando que poucos têm televisão mas muitos têm Internet (EC, 2015).

Este tipo de avanços e acessibilidade tecnológica facilita o acesso imediato às fontes de informação, nomeadamente às RS, ou ainda, em situações de emergência, a assistência em locais exatos, por vezes do desconhecimento do próprio utilizador (através dos programas de geolocalização dos *Smartphones*) (DAWSON; HILL; BANK, 2013).

4.3. Causas Humanitárias

Um objetivo pessoal ou de um pequeno grupo pode tornar-se num objetivo mundial, recorrendo à força das RS. Prova disso, foi o objetivo do ator americano Ashton Kutcher e de uma ONG sem fins lucrativos que consistiu em travar as mortes em África disseminando SA global em prol de um problema específico numa região

desse continente: a malária no Senegal (RYAN; JONES, 2011). Para tal, o ator, lançou um desafio à CNN: uma corrida no Twitter cuja meta seria alcançada quando o primeiro atingisse 1 milhão de seguidores. Ashton comprometeu-se a oferecer 10 000 redes mosquiteiras se atingisse primeiro a meta, o que veio a acontecer. Para além dessa doação, a CNN, alguns dos *twitterati* (*twitterers* famosos), bem como outros *twitterers* acresceram ao nº de redes oferecidas. Segundo a mesma fonte, devido ao *Awareness* implementado no Twitter, foram doadas no total desta campanha 89724 redes sendo o custo de arranque da mesma $0 (RYAN; JONES, 2011). Para além disso, outras vantagens se obtiveram a partir do Twitter:

- Milhões de *twitterers* aprenderam acerca da malária e como ajudar;
- O perfil @malarianomore teve um aumento de 10 000% de seguidores;
- O *website* malarianomore.org teve mais visitas em 1 mês do que em 1 ano.
- Doações de *twitterers* e dos *twitterati* permitiram alcançar as 10 000 redes que Ashton se comprometeu a oferecer e ainda alcançar $500 000.
- E ainda, foram oferecidas redes por parte de indivíduos atentos à causa no Twitter, de 42 países diferentes (RYAN; JONES, 2011).

4.4. Rastreio epidémico

O interesse pelas RS tem crescido em todo o mundo nos últimos anos, em todos os Âmbitos incluindo a área da saúde. As RS como o Facebook, Twitter, YouTube e blogs têm demonstrado a sua efetividade ao nível da disseminação de conhecimento e educação médica, podendo vir a servir para fazer bio vigilância, rastreando epidemias antes que as mesmas se alastrem pela população (ROSMAN et al., 2014).

Nos conflitos vividos na Síria, as RS foram usadas para documentar e também para disseminar conhecimento e *Awareness* entre os intervenientes no conflito armado (ROSMAN et al., 2014). O conflito na Síria tem sido único pois tem tido cobertura quase em tempo real através das RS. Pela primeira vez, foi diagnosticado através das RS um conjunto de sintomas clínicos provocados por envenenamento pelo agente nervoso Sarin (ROSMAN et al., 2014). Obama (2013) afirmou: “O mundo viu milhares de vídeos, imagens de telemóveis e relatos nas RS sobre o ataque” que encheu hospitais com pessoas envenenas por gás venenoso (Obama, 2013)

As RS têm surgido como uma fonte de conhecimento situacional, que pode ser valiosa em cenários onde não existe acesso direto e imediato às vítimas, como por exemplo: zonas de Guerra e de catástrofes naturais (ROSMAN et al., 2014).

4.5. Ferramenta de revolução

As RS no mundo Árabe têm sido usadas ao máximo para informar, mobilizar e aumentar o *Awareness* acerca de direitos humanos, corrupção e democracia. Funcionaram como catalisador para as revoluções no Irão, Egipto e Líbia (ALI; FAHMY, 2013). O papel principal das RS no Irão era aumentar o *Awareness* para a situação social e política que se vivia na região, dando conhecimento mundial e chamando a atenção dos órgãos mediáticos internacionais. Refere ainda que, à semelhança do que aconteceu no Irão, também no Egipto a influência das RS foi impressionante, mas neste caso ao nível do Facebook, sendo depois apelidada de "Facebook *Revolution*" (ALI; FAHMY, 2013).

4.5.1. Na Líbia

Na Líbia, *users* das RS bem como grupos ativistas serviram-se das plataformas Youtube, Twitter e Facebook, para demonstrar ao mundo a violência implementada pelo regime (Human Rights Watch, 2011), gerando uma onda de apoio mundial à intervenção de forças militares naquele país (Aday, 2012). Devido ao incremento desta consciência internacional, vários governos, foram encorajados a atuar pelos próprios cidadãos e tomaram ações políticas contra o regime violento da Líbia (ADAY et al., 2012).

Desta forma, as publicações que se fizeram nas RS permitiram chegar onde os meios de comunicação tradicionais não chegariam (ADAY et al., 2012). Num cenário em que não existe espaço para as reportagens convencionais, um cidadão com um telemóvel e acesso às RS pode fazer a diferença entre ninguém saber o que se passa ou o mundo inteiro saber (ADAY et al., 2012).

4.5.2. No Egipto – "Facebook Revolution"

Existem iniciativas que se amplificam nas RS, é o caso demonstrado por Sedra (2013) acerca da Shayfeencom. Esta é uma iniciativa que vigia e luta contra a corrupção vivida no Egipto usando para tal, a popularidade que alcançou nas RS. O objetivo que move esta iniciativa desde 2005 consiste em "apoiar as reformas políticas e implementar a democracia no país" educando e dando poder às pessoas com o aumento do *Awareness* no que concerne à democracia, assim como às reformas eleitorais e judiciais. No fundo, trata-se de um movimento politico que usa as RS para coordenar e organizar as atividades na luta contra a corrupção. Começou por ser criado com o intuito de preservar a legitimidade e integridade das eleições e

referendos que ocorreram em 2005 no Egipto, através da participação de mais de 5 000 voluntários que se juntaram ao grupo nas RS. Lutava-se fortemente contra a desigualdade e corrupção e a favor da destituição do poder presidencial de Hosni Mubarak, o então presidente do Egipto (Sedra, 2013).

Outro caso popular é o de Khaled Saeed. Segundo Sedra (2013), era um jovem cidadão egípcio de Alexandria que morreu a 6 de junho de 2010 depois de ter sido preso pela polícia e torturado até à morte. As fotografias da sua cara completamente desfigurada foram disseminadas pelas RS, nomeadamente num grupo de Facebook criado para o efeito, "We are all Khaled Said". Essas imagens atrozes, que se tornaram num símbolo de revolta contribuíram para o descontentamento que culminou nas revoluções de 2011. Ainda segundo Sedra (2013), mais de 70 000 egípcios juntaram-se à causa através do Facebook e puderam assistir aos protestos. Para além disso, os egípcios encontraram ainda motivação nas revoluções que aconteciam na Tunísia e eram transmitidas nas RS (Sedra, 2013).

Em 2011, as tensões sociais sustentavam-se na brutalidade policial, violações de direitos humanos, estado de emergência, limitações na Liberdade de expressão e pensamento, corrupção persistente, problemas económicos relacionados com a elevada taxa de desemprego e dos preços de bens alimentares face aos baixos salários (Sedra, 2013). As pessoas protestavam a favor do término do regime de Mubarak e melhoria da qualidade de vida das pessoas e respeito pelos seus direitos. Os confrontos entre a polícia e os protestantes resultaram num número aproximado de 800 pessoas mortas e 6 000 pessoas feridas (Sedra, 2013).

Após a revolução no Egipto que ocorreu em 2011, o movimento social Shayfeencom ganhou força com a adesão de mais adeptos (Sedra, 2013). Durante o período das eleições, o movimento mobilizou milhares de voluntários pelo país numa questão de semanas. O grupo treinava o seu exército de voluntários para as eleições, dando-lhes *Awareness* e sensibilização através de vídeos no YouTube e seminários *online* (Sedra, 2013).

Face ao exposto, as autoridades egípcias ao se aperceberem do poder das RS e dos telemóveis que erguiam cada vez mais cidadãos jornalistas, decidiram bloquear as RS e a Internet em todo o Egipto, para que as pessoas não comunicassem. No entanto, sofreram com o reverso da moeda dessa decisão pois ao impedir a comunicação através das RS, involuntariamente mobilizaram um grande número de pessoas para as ruas que queriam demonstrar a sua revolta (Sedra, 2013).

4.5.3. No Irão

Duas horas depois das eleições presidenciais terem terminado, foi anunciado pelo governo do Irão que o presidente eleito com 62,63% de votação era Ahmadinejad (BOWER et al., 2009). No dia seguinte, o Irão explodiu com protestos contra o segundo reinado deste presidente. As RS, foram usadas massivamente como ferramentas de divulgação da luta popular e o Twitter foi a arma preferida dos protestantes, levando a sua palavra ao mundo inteiro (TWT, 2009). Aqui, surgiram grupos de cidadãos jornalistas cuja função era documentar, textual e visualmente, os acontecimentos no Irão e depois, fazê-los chegar ao mundo através das RS. No entanto, a revolução fracassou com as medidas drásticas do governo iraniano, nomeadamente, impedir o acesso às telecomunicações e Internet (parcialmente) (TWT, 2009).

Apesar disso, um vídeo publicado no *website* Current.com foi divulgado pelos noticiários americanos CNN, ABC, NBC e CBS. Nesta filmagem, captada por cidadãos jornalistas, podemos ver uma mulher a morrer, nos braços de alguém, cujo rosto se inunda em sangue por ter sido baleada no peito durante os protestos (BOWER et al., 2009). O nome da vítima era Neda Agha-Soltan e a sua morte foi transformada num símbolo do movimento revolucionário pela liberdade (BOWER et al., 2009). São vários os vídeos no YouTube que homenageiam e retratam a sua morte, uns inspirando a revolução através da música num vídeo intitulado “Song for Neda”, outros documentando a história de quem foi, quem queria ser, os ideais pelos quais lutava (YouTube, [2015b]) e como aconteceu esta “trágica morte na repressão violenta das pós-eleições do Irão a 20 de Junho de 2009” (Azadi, 2010).

O governo do Irão não estava preparado para a revolução cibernauta que se avizinhava e os esforços foram no sentido de censurar e impedir a comunicação com o exterior do país impedindo as telecomunicações e a Internet (parcialmente) (TWT, 2009). É que o Irão conta com uma grande massa de *bloggers* e *hackers* que se esforçaram para manter os canais de internet abertos. Alguns *websites* resistiram à repressão do governo (TWT, 2009) e o vídeo de Neda tornou-se viral na Internet, atraindo milhares de pessoas em todo o mundo para esta causa (Palmer, 2009).

É impressionante o impacto que as RS têm no mundo civil e militar, senão vejamos: o reconhecido ditador e presidente do Irão, Ahmadinejad, volta a ser eleito presidente a 12 de junho de 2009; a eleição resulta imediatamente em protestos e

confrontos de milhares de cidadãos contra a polícia; dado que as eleições não foram anuladas, as marchas de protesto continuaram com dezenas de milhares de protestantes nas ruas e os jornalistas estrangeiros impedidos de dar cobertura aos acontecimentos que resultariam em 7 mortes no dia 15; a 20 de junho a televisão do estado anuncia 450 detenções e 10 pessoas mortas, onde se incluía Neda Agha-Soltan (Reuters, 2010); nesse mesmo dia, o presidente dos EUA, Barack Obama incitou o governo iraniano a cessar todas as ações violentas e injustas contra o próprio povo, lamentando-as e alertando para o facto de o mundo estar atento a todos os acontecimentos, afirmando: *"(Iran must) stop all violent and unjust actions against its own people. The Iranian government must understand that the world is watching. We mourn each and every innocent life that is lost"* (Palmer, 2009).

4.6. Obtenção de Situational Awareness para as OPMIL

Num país densamente povoado e com acesso às tecnologias de informação, Kase (et al., 2014) refere que existem diferentes atitudes e alianças na população local, que podem ser hostis, neutrais ou amigas. Ainda segundo Kase (et al., 2014), a maior parte dessa população é responsável por criar um elevado fluxo de informação ao usar as RS para comunicar, organizar e calendarizar eventos públicos (KASE et. al., 2014). Alguma dessa informação pode ser crítica e permitir a otimização da execução das missões militares que a FA desempenha nesses países, tais como as INFOPS, missões de manutenção da paz e ajuda humanitária, entre outras.

Segundo Kase (et al., 2014), as RS podem ser uma poderosa ferramenta ao dispor dos comandantes, ajudando a compreender e a moldar as áreas de responsabilidade. Afirma igualmente que se os comandantes souberem utilizar as RS, estas podem ajudar a influenciar as comunidades e melhorar a qualidade e pontualidade da partilha de informações relevantes (KASE et al., 2014), potenciando o SA.

Se os decisores se esforçarem para manter, potenciar e empregar uma presença nas RS, conseguirão obter informações cruciais acerca de ameaças emergentes e ainda compreender o terreno (Mayfield, 2011). Zeng (et al., 2010) refere que as RS podem ser uma fonte de dados e informação para aumentar o SA e assim compreender o quadro situacional. Ao nível tático e operacional, o aumento do SA pode permitir que os comandantes tomem decisões mais informadas no momento de

despender bens e recursos (ZENG et al., 2010), tal como veremos na Operação Manatim.

Segundo Goolsby (2010), no nível estratégico, as RS criam oportunidades para o estudo e compreensão da cultura e comportamentos locais que de outra forma seria difícil de interpretar. As comunidades locais são uma gigantesca fonte de observadores que superam em larga escala os quantitativos de militares observadores. No fundo, a representação das comunidades locais nas RS pode substituir o trabalho que os militares teriam em observar o ambiente na busca de SA. Ainda segundo Goolsby (2010), mais importante ainda é que estas comunidades podem possuir conhecimento linguístico, cultural e contextual, fatores que apoiam a elaboração do quadro situacional por parte dos decisores (Goolsby, 2010). Desta forma as RS podem ajudar à comunicação intercultural e traduzir linguagens.

Kase (et al., 2014) refere ainda outra caraterística importante da envolvência operacional nas RS, que consiste na capacidade de reconhecer de forma natural quais os dados e informações que em determinada comunidade se consideram importantes. Segundo o mesmo, esta envolvência permite que os comandantes compreendam o que tem interesse e relevo em determinada comunidade, bem como avaliar os efeitos de determinadas ações. Ou seja, estas capacidades poderão tornar mais realistas e menos incertas a avaliação, seleção e criação das ações a tomar (KASE et al., 2014).

Caso Estudo da Operação Manatim

O contexto em que a operação ocorreu pode ser visto no subcapítulo 6.1.

Para o assunto em causa, Mineiro (2015)[12] refere que o primeiro passo foi descobrir quais as RS que eram utilizadas nas zonas de influência (são as zonas que têm a ver com a respetiva operação), que neste caso eram política e militar. Assim, foram referenciadas e acompanhadas as publicações de diversos atores: um *blogger*, que estava na Guiné-Bissau (GB) e escrevia praticamente todos os dias; várias pessoas que faziam *retweet* de informação; e na parte política, referenciaram jornalistas, líderes de opinião e entidades oficiais. (Mineiro, 2015).

Através da informação veiculada pelo Twitter foi possível antecipar cerca de um dia e meio o pedido oficial de Cabo Verde a Portugal, para efetuar a extração de 2000 cabo-verdianos na Guiné-Bissau, refere Mineiro (2015). “Ora quando nós vimos essa informação, veiculada no Twitter, rapidamente se tentou confirmar se isso

[12] O Major Paulo Mineiro é Chefe da Área de Informação Pública da FA, foi o porta-voz da Força de Reação Imediata (FRI) e foi o *Public Affairs Officer* (PAO) da Operação Manatim.

correspondia à realidade. A vantagem que se obteve foi ao nível logístico porque, mesmo sem confirmação da notícia, possibilitou-nos o planeamento antecipado. Isto permitiu averiguar que material logístico seria necessário para fazer corresponder a essa necessidade e se isso seria ou não possível de executar". Mais, a análise da informação a circular nas RS permitiu descobrir as tendências políticas que se viviam na região e com que países da região Portugal poderia contar para a extração dos portugueses na GB (Mineiro, 2015).

Mineiro (2015), acrescenta que as RS potenciaram, sem dúvida, o SA da missão militar e que a exploração das RS permitiu antecipar, ganhar tempo e fazer planeamentos que se vieram a confirmar justificáveis por se ter avaliado bem a importância da informação nelas veiculada, bem como a transmitida pelas pessoas no terreno (Mineiro, 2015).

Os EUA reconhecem as potencialidades das RS, nomeadamente no que toca à obtenção de SA. Senão vejamos: minutos depois do Malaysia Airlines Flight 17 ter sido abatido a 17 de Julho de 2014 na Ucrânia, matando todas as 298 pessoas a bordo, um analista da Defense Intelligence Agency (DIA)[13] obteve uma pista através da observação das RS. Este analista falava Russo e encontrou um *post* feito por um separatista pró-russo na Ucrânia, através de um *website* das RS da Rússia chamado VK. Nesse *post*, o separatista afirmava ter abatido um avião de carga militar Ucraniano (Barnes, 2014).

Neste sentido, o Tenente-General Michael Flynn, chefe da DIA, refere que "A primeira indicação de quem o abateu, com que arma o fez, quando e como foi abatido proveio das RS (…) literalmente em minutos" (Barnes, 2014). Gonçalves (2015) também afirma que no Afeganistão pôde constatar a velocidade a que as informações são injetadas nas RS, sendo numa questão de segundos ou minutos depois do início dos acontecimentos (Gonçalves, 2015).

"As RS potenciam muito o SA em OPMIL e quem não tiver acesso às RS está desatualizado", refere Gonçalves (2015). Segundo o mesmo, a celeridade no acesso às informações que são publicadas em tempo quase real, logo após os acontecimentos, é um dos aspetos que fazem das RS uma ferramenta importante nas

[13] A *Defense Intelligence Agency* é uma agência dos EUA que monitoriza os movimentos militares estrangeiros. Esta agência confia e usa cada vez mais as RS, onde encontram fontes abertas de informação que podem usar contra os maus atores.

OPMIL. “No Afeganistão as pessoas sabem a importância das RS e se houver uma explosão no local “A”, nos próximos 30 segundos já se encontra informação nas RS e em menos de 3 minutos sabe-se o que se está a passar nesse local, através dos *posts*” (Gonçalves, 2015). Esta não é, no entanto, uma posição consensual como veremos na seguinte análise (Anexo B).

►Análise dos inquéritos (ver Anexo B): De acordo com o inquérito efetuado aos militares da FA que participaram em OPMIL, 56% dos militares afirmam que a informação obtida através das RS é útil (Figura B-2, Anexo B) e 38,9% dos inquiridos usaram as RS em missão por as considerarem uma fonte de informação (Figura B-1, Anexo B). Para além disso, 31,1% acreditam que as RS permitem o ganho de SA durante as OPMIL (Tabela B-4, Anexo B).

No entanto, Gonçalves (2015), entende que a segurança dos militares em operações pode depender bastante do SA que se adquire a partir das RS, e, por isso, estas podem ser vistas como uma ferramenta de segurança pessoal, na medida em que, se os militares tiverem que optar por um de dois caminhos, vão primeiro às RS e tomam a sua decisão consoante os *posts* que observam, ou seja, se existir ameaça de perigo num dos caminhos, opta-se pelo outro[14] (Gonçalves, 2015).

Mas isto só é possível quando existe uma consciência coletiva acerca das potencialidades das RS, nomeadamente ao nível da segurança que o SA incrementado pelas mesmas pode dar, tal como refere Gonçalves (2015). Dado que todos os cidadãos têm necessidade de segurança, na generalidade todos publicam acerca das ameaças e eventos perigosos (Gonçalves, 2015).

No entanto, nem todas as informações são fidedignas, é necessário gerir a informação para saber identificar se uma ameaça pode ou não constituir um fator de perigo. Segundo Gonçalves (2015), as RS ajudam na gestão da informação na medida em que permitem avaliar a credibilidade dos relatos das RS. “O cruzamento dos *posts* das RS, permitia esclarecer determinados eventos, como por exemplo, distinguir se um rebentamento comentado nas RS se tratava de uma bomba ou da explosão de um pneu”. As RS permitem saber se uma dada informação merece investigação e permitem diferenciar uma ameaça de uma situação real (Gonçalves, 2015).

Metaforicamente, podemos pensar nas RS como um mundo onde as pessoas podem ter um rosto, podem não ter qualquer rosto ou podem iludir que têm um rosto.

[14] Gonçalves (2015) comenta que este SA e análise era efetuado pelos militares das Nações Unidas, no entanto a NATO tinha outros procedimentos (Gonçalves, 2015).

Qualquer pessoa pode publicar nas RS, o que potencia alguns perigos para as operações, nomeadamente ao nível da aquisição de SA. Gonçalves (2015) afirma que uma das problemáticas incide na importância que se atribui ao conteúdo dos *posts* das RS, que tanto pode ter sido publicado por uma criança numa brincadeira, como pode ser publicado por alguém que sabe de facto o que diz. Não obstante, ambas as publicações devem ser encaradas com a mesma seriedade, mesmo sendo uma falsa e outra verdadeira. Nunca sabemos ao certo quem está por detrás da publicação e qual a sua intenção com a mesma. Conclui ainda que as RS têm bastante ruído, mas qualquer ameaça que tenha sido detetada deverá ser levada a sério (Gonçalves, 2015).

As RS como o Facebook e o Twitter permitem-nos avaliar os perfis de quem faz determinadas publicações bem como ter acesso a informações que essas pessoas publicaram há anos atrás permitindo estudar as diferenças de comportamentos que essa pessoa assumiu ao longo dos anos (PSimões, 2015) e ainda escrutinar e filtrar essas fontes de informação, por fiabilidade e interesse (Mineiro, 2015).

Antigamente, tínhamos que ter muito mais pessoal no terreno para recolha de INTEL, ao passo que hoje em dia, é possível fazê-lo sem sair do local de trabalho, à frente de um computador, refere PSimões (2015). No fundo, é como se tivéssemos pessoal no terreno para recolha de INTEL há anos. Trata-se de replicar aquilo que acontece no terreno e transpor para o mundo digital, porque as pessoas e a forma de funcionar não mudou mas mudou o meio e a quantidade de informação que é muito maior (PSimões, 2015). Mineiro (2015) e PSimões (2015) concordam que, para se recolher boa INTEL, os "analistas" da informação deverão ter a capacidade de cruzar a informação do pessoal que está no terreno com a informação digital.

Segundo o Tenente-General Flynn e outros oficiais dos EUA, desde 2013, os EUA têm investido largamente em meios de recolha e análise das RS, nomeadamente ao nível do Facebook, Twitter e RS estrangeiras como forma de obtenção de INTEL (Barnes, 2014). Em 2011, Waterman (2011) já referia que o comando central dos EUA utilizava um *software* cuja função era encontrar os *websites* de RS usados pelos terroristas (Waterman, 2011).

Este investimento por parte dos EUA pode ser explicado e entendido à luz da sociologia. Pois, tal como refere ENISA (2007), o ser-humano tem um desejo natural de se relacionar com outros, nomeadamente através da Internet, o que, combinado com os múltiplos efeitos das tecnologias das RS, pode tornar os *users* menos

discriminatórios no que toca a aceitar pedidos de amizades. Normalmente os *users* não têm consciência da quantidade de pessoas que acedem às informações que têm nos perfis e a sensação de intimidade que é criada por se sentirem envolvidos entre amigos digitais pode conduzir a revelações que normalmente não são apropriadas no contexto da informação pública (ENISA, 2007), onde se inserem as fugas de informação classificada para um meio publico e globalizado, as RS.

O Tenente-General Flynn continua, afirmando que as RS poderão revolucionar a OSINT, que se foca em encontrar elementos chave em fontes de informação públicas. Os oficiais da DIA referem ainda que os computadores do governo Americano podem ter a capacidade de reunir dados e informação de múltiplas fontes das RS e fazer o rastreio de quantidades exorbitantes de informação pública (Barnes, 2014).

Diana (2011) refere que devido a uma quebra de segurança, o WikiLeaks conseguiu saber que os EUA estavam, em 2011, a procurar obter um programa de computador, "*Persona Management Software*" que iria permitir o comando online de unidades de identidades falsas nas RS. Este programa deveria ter a capacidade de gerir 10 perfis por *user*, onde cada perfil teria uma história, experiência de vida, outros detalhes de apoio e uma ciberpresença consistente em termos técnicos, culturais e geográficos (Diana, 2011). Dias depois, a 01 de Março, Waterman (2011), refere que o comando militar dos EUA localizado em Tampa, Florida que gere os conflitos no Iraque e Afeganistão comprou um programa de computador que permite que os militares criem identidades falsas nas RS (Waterman, 2011). Tudo indica que as Forças Armadas dos EUA têm integrado cada vez mais as RS nas suas operações (Diana, 2011).

Cronologias à parte, o objetivo destas identidades falsas seria dar aos militares a possibilidade de se infiltrarem em determinados grupos e em certos casos praticar desinformação dentro de organizações extremistas como é o caso da al-Qaeda e os Taliban com o intuito de negar as operações (Waterman, 2011). Este programa aumenta o SA dos militares através da apresentação em tempo real de informações locais pertinentes para manter a identidade falsa, tais como, informações acerca da hora local, meteorologia, e noticias. Essas informações são relativas à morada em que essa identidade falsa supostamente habita, permitindo que o militar esteja contextualizado e possa atuar em conformidade (Waterman, 2011).

Diana (2011) menciona que com este programa os militares podem assumir diferentes identidades falsas *online*, com diferentes objetivos operacionais, sem saírem do local de trabalho e sem terem medo de serem descobertos pelos adversários. Segundo a mesma, estas identidades deverão ter a capacidade de aparecer em qualquer parte do mundo e interagir a partir das plataformas das RS e serviços convencionais da Internet. A cada identidade é dado um endereço IP correspondente a diferentes regiões do globo, o que permite iludir o inimigo quanto à localização do agente que está por detrás das identidades falsas (Diana, 2011).

Outra característica deste programa é a capacidade de fazer cruzamento de dados de todas as RS disponíveis, onde se incluem o Facebook, Twitter, MySpace, entre outros, com o intuito de recolher dados pessoais e usá-los para conseguir acesso a outros *users* dentro desses círculos sociais (Diana, 2011).

Existem várias técnicas que se podem usar para tornar as identidades falsas mais reais, nomeadamente ao nível da informação. Tendo o agente conhecimento de quais as escolas ou colégios frequentados pelos alvos, ou onde vivem, atuando em conformidade como se tivesse ligações reais a esses ambientes, mais facilmente os alvos irão partilhar informações com o agente infiltrado nas RS. De acordo com Diana (2011), para se ganhar acesso a grupos privados nas RS, o agente pode inscrever-se no *website* oficial da escola que o alvo frequenta e procurar por um estudante "E" conhecido do alvo que não tenha perfil nas RS. Cria depois um perfil nas RS como se fosse o "E". Dessa forma o agente irá fazer-se passar por alguém que não é, podendo obter informações dadas pelo alvo (Diana, 2011).

Neste contexto, continua a fonte, o agente deverá de certa forma influenciar o alvo a aceitar o pedido de amizade voluntariamente. Nesse sentido, antes de enviar um pedido de amizade para o alvo, o agente deverá entrar no círculo de amigos do alvo. Para tal, pode criar amizade com alguém que tenha por exemplo 300 ou 500 amizades nas RS e que tenha amizade com o alvo. Adiciona depois mais amizades dentro desse círculo aumentando cada vez mais o número de amizades em comum com o alvo. Assim, poderá ser mais facilmente aceite por parecer ser alguém de confiança (Diana, 2011).

Existem várias ferramentas públicas que podem potenciar o SA. São aplicações que estão ligadas ao Twitter e que para um normal utilizador das RS podem ser divertidas mas que, pelo que já vimos, em contexto operacional podem ter uma utilidade muito diferente e ser uma potencialidade para as OPMIL, nomeadamente

para a aquisição de SA. Segundo EC (2015)[15], quando esteve em operações internacionais, no âmbito da NATO, a plataforma de RS que mais utilizou foi o Twitter e refere que "esta é a melhor ferramenta para se utilizar em contexto operacional pois é a que melhor se adapta à necessidade particular de ler o ambiente sociopolítico da área de operação onde a força está a operar. Permite, entre outros, obter perceção, leitura de ideias, opiniões e sentimentos das populações locais sobre a intervenção militar em causa". Permite também obter informações pontuais para planeamento de algumas ações militares (obtenção de informações de caráter ambiental – informações de trânsito, manifestações, ações policiais a decorrer) (EC, 2015).

É importante obter-se este tipo de SA, que a fonte refere como SA ambiental, porque, por exemplo, no caso das manifestações contra a guerra e forças militares, poderão surgir graves problemas se os manifestantes se depararem com os motivos de protesto, que neste caso são os militares (caso que já aconteceu, segundo a fonte). Estas informações são cruciais porque percorrer 4 km nos veículos militares tanto pode demorar 10 minutos como 1 hora, ou até mesmo resultar em fatalidades se não se obtiver SA (EC, 2015).

Algumas das ferramentas públicas que habitam no *Twitterverse*, quando operadas em conjunto com o Google Maps, por exemplo, permitem ao utilizador várias possibilidades de leitura das RS. Vejamos algumas dessas ferramentas.

Trendsmap: é uma ferramenta que permite visualizar as tendências de discussão mais abordadas no Twitter. Exemplos de tendências podem ser por exemplo: uma catástrofe natural, uma revolução, uma personalidade em destaque, etc (McClain, 2010). No fundo, trata-se de saber o que os *twitterers* estão a falar no momento e onde estão. Permite ainda explorar mais a fundo os tópicos de discussão através de um clique no mesmo. Ao fazê-lo, surgem dois gráficos com o histórico de discussão, local e global, bem como alguns detalhes que explicam porque esse tópico é assunto de discussão. Podem ainda ser visualizados vídeos e notícias que são seguidos pelos *tweets* mais recentes acerca desse tópico que é atualizado em tempo real (McClain, 2010).

[15] EC é a sigla para Entrevistado Confidencial e refere-se a uma entrevista feita no âmbito desta dissertação, a um militar que por força do cargo que exerce na FA não pode ser identificado. Possui experiência em OPMIL internacionais e reconhece a importância das RS.

Figura 3 - Trendsmap (McClain, 2010)

GeoChirp: Este programa permite descobrir o que as pessoas estão, num determinado momento, a publicar no Twitter, numa determinada região dentro de um raio de distância selecionado pelo *user*. Os últimos *tweets* dessa região são apresentados em baixo do mapa. Esta ferramenta permite filtrar os resultados por palavras-chave, número de *tweets* a apresentar e o raio de distância de procura (entre 2 a 80 km, aproximadamente) (McClain, 2010).

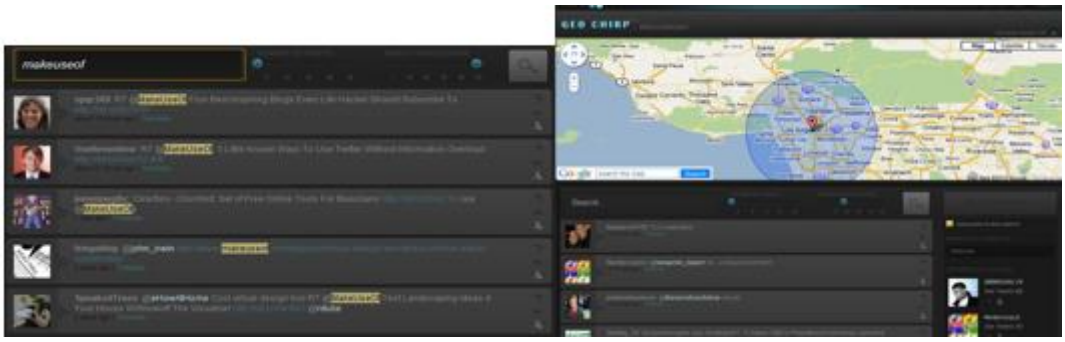


Figura 4 - GeoChirp (McClain, 2010)

Twittervision: permite ver *tweets* por todo o mundo através do Google *maps*. Depois da entrada neste *website*, não é necessário fazer mais nada para que se vejam os *tweets* a aparecerem no mapa-mundo com atualização em tempo real (McClain, 2010). Ao surgir um *tweet*, aparece numa pequena janela a informação do texto do *tweet* bem como quem enviou e o local de onde foi enviado esse *tweet*. Depois, segue para um novo *tweet* da mesma forma. Dentro deste *website* pode selecionar-se o modo 3D que permite visualizar o mapa tridimensional (McClain, 2010). O Twittervision memoriza todos os *users* com uma fotografia e localização de origem do

tweet e permite ver em tempo real as notícias de ultima hora e as conversas no Twitter (Pierce, 2009).

Figura 5 - Twittervision (McClain, 2010)

EC (2015) comenta que no Afeganistão, ocorrem ataques constantemente e que num cenário deste género os militares se encontram muitas vezes aquartelados. Se tiverem que sair da base o primeiro que fazem é aceder às RS para conhecerem as condições de segurança na rua (informações de trânsito, manifestações, ações policiais, entre outras situações que possam bloquear o movimento dos militares e ser uma ameaça para a segurança dos mesmos). Vários comentários nas RS fornecem este tipo de informações (EC, 2015), por exemplo:

Tabela 2 - Exemplos de comentários nas RS que fornecem SA.

User	Post (tweet ou comentário)	Hora	Local
A	"Acabei de ficar preso na neve"	11:34	Síria
B	"Parado no trânsito há 1 hora na estrada X"	12:34	Síria
C	"Hoje não chego a casa para almoçar"	13:04	Síria
D	"Acho que ouvi uma bomba"	16:31	Afeganistão
E	"Ouvi um estrondo e os carros estão parados"	16:32	Afeganistão
F	"Rebentou um pneu à minha frente na rua Y"	16:35	Afeganistão
G	"Tirem-me daqui, malditas ruas intransitáveis"	16:50	Afeganistão
H	"... Estava melhor de bicicleta"	17:01	Afeganistão
J	"Não acredito, trânsito na estrada X mais uma vez"	20:02	Síria
K	"Outra vez operações policiais na estrada"	20:17	Síria

Análise: Cruzando os *posts* de A e B podemos perceber que devido à neve na estrada, o trânsito está muito condicionado, podem haver acidentes e carros encravados na neve. Segundo B o trânsito pode estar muito lento ou até mesmo parado na estrada X. Não sabemos se C está no trânsito mas é uma possibilidade. O melhor a fazer é não seguir pela estrada X.

Cruzando os *posts* de D, E e F percebemos que o estrondo ouvido perto das 16:30 no Afeganistão foi intenso, gerou algum pânico, mas em princípio terá sido apenas o rebentamento de um pneu. Analisando os *posts* de G e H pode-se concluir que, provavelmente, o rebentamento de pneu provocou congestionamento na rua Y. Mais uma vez, o melhor a fazer é não seguir pelas ruas perto de Y sob pena se ficar encurralado no trânsito.

Por último, os *posts* J e K indicam que existe trânsito na estrada X novamente e que poderá dever-se às operações policiais. Teria que se explorar e cruzar mais *posts* para se conseguir informações mais concretas.

4.7. Conclusão Intermédia

Tal como se refere no subcapítulo 4.1, cada vez mais pessoas recorrem às RS como fonte de receção e transmissão de informação o que permite a obtenção de SA em tempo quase real. Vimos ainda que a análise das RS permite a previsão de futuros acontecimentos e que as mesmas podem ser usadas para as OPMIL, como exemplificado no caso estudo “Fort Hood Shootings” e pelos relatos de Gonçalves (2015). Foi também demonstrado com diversos exemplos que as RS podem potenciar o SA em diversas causas: apoio à população (subcapítulo 4.2, 4.3 e 4.4) e como uma ferramenta que permite organizar protestos e disseminar as causas por todo o mundo (subcapítulo 4.5).

Por último, no subcapítulo 4.6, foram abordadas as RS como uma ferramenta de ganho de SA. Neste subcapítulo foram citados diversos autores que referem as vantagens, em contexto operacional, do ganho de SA pelas RS, tais como: acesso a informação pública acerca de eventos importantes (KASE et. al., 2014) e ameaças emergentes (Mayfield, 2011) através de várias ferramentas das RS como refere McClain (2010); compreender o terreno (Mayfield, 2011), cultura, linguagem, comportamentos locais (Goolsby, 2010), ambiente político (Mineiro, 2015), leitura de ideias, opiniões e sentimentos da população (EC, 2015); distinguir que informações se consideram importantes no local (KASE et. al., 2014); efetuar um melhor planeamento logístico (Mineiro, 2015); encontrar informações classificadas acerca do adversário (Barnes, 2014); obter informação pública acerca de eventos perigosos que ocorram no terreno das operações e garantir a segurança dos militares, segundo Gonçalves (2015) e EC (2015); conhecer o historial comportamental de determinados

alvos (PSimões, 2015) e criar uma base de dados com informações de múltiplas fontes das RS (Barnes, 2014); praticar ações de espionagem (Diana, 2011).

Tal como referido no subcapítulo 4.6, os inquéritos (ver Anexo B) demonstram que 56% dos militares inquiridos encontram utilidade na informação disseminada nas RS (Figura B-2, Anexo B) e 31,1% concordam que as RS potenciam o SA para as OPMIL (Tabela B-4, Anexo B).

Desta forma, as entrevistas e os inquéritos, aliados à pesquisa bibliográfica, permitiram validar a seguinte hipótese, **"O uso das Redes Sociais nas missões, permite capacitar os militares com um melhor *Situational Awareness*".** No entanto, por motivos de confidencialidade, não foi estudado o *modus operandi* para a aquisição de SA por parte da FA.

Página intencionalmente deixada em branco

5. As Redes Sociais para a Motivação dos Militares

Este capítulo surge como uma análise, no sentido de averiguar se as RS permitem incrementar a motivação dos militares que se encontram em OPMIL no estrangeiro, a importância e relevo que isso assume para as operações e se atualmente é um fator tido em conta na FA.

5.1. Análise à Motivação

No âmbito das OPMIL, as RS podem representar um risco para a segurança mas por outro lado, se forem usadas apropriadamente, exercem uma função importante para a moral e bem-estar dos militares e das suas famílias (Jensen et al., 2014). Para alguns militares em missões no estrangeiro o acesso às RS é uma prioridade pois permitem manter a proximidade com os familiares e/ou amigos (F/A) e também estes sentem que as RS permitem encurtar a distância. O valor da integração das RS nas Forças Armadas, assenta nos benefícios que elas trazem aos militares em missões, e às vantagens estratégicas que se podem explorar (Jensen et al., 2014).

Os militares podem ser destacados para missões longas e nesse sentido, as RS são excelentes para a moral e motivação dos militares tornando-se extremamente importantes no contexto das operações no estrangeiro (Gonçalves, 2015).

Em missão, o *stress* e afastamento das famílias é notório e nesse sentido as RS permitem aproximar os militares das suas famílias, resultando em motivação acrescida (EC, 2015). MSimões (2015)[16] concorda com a importância das RS para os militares destacados e salienta que essa motivação, beneficia as operações, na medida em que os militares são mais empenhados nas suas funções. Acrescenta ainda que as "RS permitem dar e ter notícias de um enorme espectro de familiares comodamente e com privacidade" (MSimões, 2015).

Gonçalves (2015) reconhece a importância das RS e prova disso é que quando foi nomeado como responsável pela motivação dos militares destacados na Lituânia, a sua primeira preocupação foi disponibilizar uma sala com computadores com internet livre (sem restrições de segurança) onde os militares pudessem passar o tempo, sempre que não estivessem a trabalhar. Desta forma, "não só eles andavam satisfeitos porque falavam com as famílias e aliviavam algum *stress*, como também conseguia saber onde estavam, porque certos ambientes (como os bares por

[16] O Major Miguel Simões é Chefe do Gabinete das Operações Aéreas e participou numa missão no Afeganistão pela ISAF, onde verificou a importância das RS em operações para a motivação dos militares.

exemplo) podem ser desviantes das nossas funções principais enquanto militares". Acrescenta ainda que, se não existirem adequadas condições de *Welfare*, os militares irão tendencialmente procurar formas menos próprias de se distraírem (Gonçalves, 2015).

Neste sentido, também Costa (2015)[17] e Mineiro (2015) revelam as suas experiências com a introdução das RS em OPMIL. Costa (2015) que comandou um destacamento militar na Islândia recentemente, afirma reconhecer os perigos associados ao uso das RS pelos militares, que as usam de forma particular e muitas vezes insegura porque procuram manter o ânimo, moral e motivação (Costa, 2015). Assim, continua Costa (2015), nas operações na Islândia, com o apoio de um oficial das RP, ofereceu aos militares a possibilidade de publicarem nas RS informações acerca do decorrer das operações, de forma controlada e segura (como será visto no subcapítulo 7.4.1), motivando os mesmos e contribuindo para a tranquilidade dos familiares, que dessa forma sabiam do paradeiro dos militares em operações (Costa, 2015). Vejamos o que foi aferido com a análise no Anexo B.

►<u>Análise dos inquéritos (Anexo B):</u> Os inquéritos permitiram definir que a esmagadora maioria dos militares já teve conta nas RS, totalizando 95,6% (Subcapítulo B-1, Anexo B), pelo que se conclui que as RS estão muito disseminadas pelos militares operacionais.

►Segundo os inquéritos (Subcapítulo B-2, Anexo B), 86% dos militares afirmaram que durante a missão sentiram maior necessidade de aceder às RS e segundo a Tabela B-3 (Anexo B) 56,9% usaram as RS todos os dias. A maior parte usou as RS para falar com a família e amigos, ou seja 69,4% (Figura B-1, Anexo B), e 48,6% contactaram com os F/A pelas RS para os tranquilizar (Subcapítulo B-4, Anexo B).

►Segundo a Tabela B-5 (Anexo B), os militares inquiridos revelam que o acesso às RS durante as OPMIL no estrangeiro, são um fator de motivação. Mais concretamente, 69% dos militares que as usaram durante as operações, afirmam que são motivadoras, dos quais 54% classificam-nas como "Muito motivadoras" e ainda, 68% classificam o uso das RS como sendo importante, dos quais 50% classificam a importância como "Muito importante" (Tabela B-5, Anexo B).

[17] O Coronel Fernando Costa é atualmente o Comandante do Corpo de Alunos da Academia da Força Aérea Portuguesa e foi Comandante de destacamento de F-16 na Islândia na missão Iceland Air Policing.

►Segundo a Tabela B-16 (Anexo B) as publicações que a FA faz nas RS são benéficas para a moral e motivação dos militares. Prova disso, é que 65,8% dos militares sentem orgulho na FA ao verem essas publicações[18] (Tabela B-16, Anexo B). Mais, essas publicações são um fator motivador para 47,4% dos militares (Tabela B-16, Anexo B).

5.2. Conclusão Intermédia

Neste capítulo, vimos que a motivação dos militares, é extremamente importante para o sucesso das operações (Gonçalves, 2015) e que nesse sentido, como refere Jensen (et al., 2014) as RS podem fortalecer a moral e bem-estar dos militares e dos familiares que através do seu uso se sentem mais próximos (Jensen et al., 2014). E com este acréscimo de motivação, os militares são mais empenhados nas suas funções (MSimões, 2015). Também vimos que Gonçalves (2015) e Costa (2015) valorizam bastante as RS e reconhecem que devem ser disponibilizadas aos militares em operações, o que se verificou com as respostas ao inquérito (Anexo B).

Segundo a Tabela B-5 (Anexo B), 69% dos inquiridos encaram as RS como um fator de motivação. Onde 69,4% as usaram para contactar com os F/A (Figura B-1, Anexo B), e 48,6% para os tranquilizar (Subcapítulo B-4, Anexo B).

Também vimos que as publicações das RS da FA (RSFA) são um motivo de orgulho para 65,8% de militares e são motivadoras para 47,4% (Tabela B-16, Anexo B). Para além disso, Costa (2015) refere que as RS são importantes para as operações da FA pois para além de motivarem e moralizar os militares, também permite que os militares tranquilizem os seus familiares.

Desta forma, a análise bibliográfica, as entrevistas e os inquéritos permitiram concluir que as RS permitem motivar os militares em operações de duas formas: no uso direto pelos militares e pela divulgação das missões nas RSFA. Assim, validam-se as duas hipóteses: **"O uso das Redes Sociais pelos militares é um fator de motivação durante as Operações Militares"** e **"O uso efetivo das Redes Sociais da Força Aérea Portuguesa para divulgar as missões motiva e moraliza os militares destacados e contribui para a tranquilidade das suas famílias".**

[18] Pressupõem-se que o sentimento de orgulho referido fortalece o bem-estar e confiança dos militares para com a FA, o que por sua vez se pode traduzir em vontade e coragem para servir, que aqui designamos como moral dos militares.

Página intencionalmente deixada em branco

6. Influência das Redes Sociais na Opinião Pública

Este capítulo estuda diversos casos relacionados com a FA e que permitem perceber a importância da presença da mesma nas RS. Para além disso, também pretende aferir se o uso institucional das RS, bem como o uso particular pelos seus militares, podem influenciar a OP acerca da imagem da FA e das suas operações.

"Se nós não contarmos a nossa história, alguém a contará por nós" e hoje em dia muitas "histórias" são contadas ou ampliadas através das RS. Se não tivermos uma presença vincada nas RS bem como relações fortes com os órgãos de comunicação social, as nossas "histórias" poderão ser mal contadas (Mineiro, 2015).

No século em que estamos, a comunicação é fundamental, as pessoas querem ser informadas, sentem que devem ser informadas e que os serviços têm obrigação de as informar, refere Mineiro (2015). As pessoas não admitem não ser informadas e não admitem não poder comentar as notícias, acrescenta. Neste sentido, "para que a FA receba o apoio das pessoas terá que estar neste fluxo e esforçar-se para ser um órgão de informação atualizado que publica a sua missão, o porquê das missões e quais as dificuldades sentidas nas missões. Devemos manter as pessoas informadas para que percebam a nossa existência" (Mineiro,2015).

Ao nível da OP, as RS tanto podem representar uma vantagem como uma desvantagem para a FA e nesse sentido, é importante reconhecer as desvantagens e minimizá-las.

6.1. Operação Manatim

Na sequência do Golpe de Estado da Guiné-Bissau, em 2012, foi ativada a Força de Reação Imediata (FRI) no sentido de resgatar os cidadãos Portugueses daquele País se houvesse necessidade. Esta missão ficou conhecida por Operação Manatim (Mineiro, 2015).

A FRI traduz a capacidade de Portugal perante os seus cidadãos a viverem ou trabalharem no estrangeiro que, por razões conjunturais emergentes nos países hospedeiros, tenham necessidade de receber apoio ou ser resgatados para um local seguro (Mineiro, 2015).

Comunicação Pública: A comunicação/informação pública acerca do que acontece numa organização e consequentemente também em missão é fundamental. Esta visa dar a conhecer às pessoas o que está a acontecer, as razões e ainda

esclarecer quais são os meios envolvidos e o que as pessoas poderão esperar dessa missão (Mineiro, 2015).

Esta operação teve uma forte componente em dois sentidos, por um lado informar as pessoas e por outro lado impedir que alguma informação difundida, independentemente do canal, pudesse prejudicar a missão (Mineiro, 2015).

Sempre que a Informação Pública não funciona ou quando não existem canais abertos entre a comunicação social e os responsáveis das FAA, poderá dar origem a informação nefasta para o sucesso das operações. Um exemplo disso foi a falta de canais abertos durante esta operação que levou à publicação de uma notícia pela Renascença que veio a "inflamar" as relações entre a Guiné-Bissau e Portugal (Mineiro, 2015).

Apesar de os meios da FRI terem sido divulgados, a verdade é que a inexistência de contactos regulares com a imprensa permitiu que alguém os informasse sobre a partida de uma fragata. Esta informação foi tida como um reforço dos meios que Portugal tinha alocado, o que não correspondia à verdade (Mineiro, 2015).

Mineiro (2015) refere que a relação que a FA procura criar com a comunicação social é de transparência e cumplicidade profissional. Esta relação permite que, da parte dos jornalistas, exista abertura para o contraditório. Se esta forma de atuar estivesse vertida na estrutura do Comando da FRI talvez a notícia da partida do 3º navio - "Forças Armadas reforçam meios para eventual resgate de portugueses na Guiné"- tivesse sido escrita sem empolamentos. Assim, o que resultou para a OP e, fundamentalmente para o Estado da Guiné-Bissau foi o "reforço de meios por parte de Portugal" (Mineiro, 2015).

6.2. Caso Resort 4 Estrelas

No dia 05 de Maio de 2012, foi noticiado no *website* do Jornal de Notícias (JN) e no dia seguinte publicado no jornal impresso que "parte do contingente militar destacado para a eventual missão de resgate de portugueses na Guiné-Bissau" estava "alojado há três semanas, num resort turístico de quatro estrelas em Cabo Verde". Estes 36 militares, que faziam parte da FRI, devido às condições em que estavam alojados "deixou perplexos turistas" e segundo a mesma fonte, as "Forças Armadas garantem que a situação é normal, quando não existem instalações militares adequadas para alojar as tropas". Um dos turistas comenta ao JN que os militares passam muito do seu tempo na praia, na piscina ou a passear e salienta ainda que,

ao passo que os turistas têm que pagar pela viagem, “estes militares estão a receber o salário pago pelo Estado e ainda têm todas as despesas pagas" (MONTEIRO; BARBOSA, 2012)

A notícia foi explicada ao JN pelo Estado-Maior-General das Forças Armadas (EMGFA) dizendo que a missão exigia uma intensa atividade operacional, da qual as pessoas não se aperceberiam (MONTEIRO; BARBOSA, 2012). O *Public Affairs Officer* (PAO) da operação em causa, Operação Manatim, interveio imediatamente nas RS para “explicar que numa operação existiam fatores fundamentais para assegurar que a missão fosse cumprida, nomeadamente a segurança física e alimentar dos militares” (Mineiro, 2015).

No âmbito desta operação, o PAO, usou todas as ferramentas ao dispor da FA para fazer monitorização, controle e divulgação da missão. As ferramentas usadas foram unicamente as da FA, já que o EMGFA não as tem (Mineiro, 2015). O que assume uma acrescida importância, já que “As RS foram um órgão difusor desta notícia e esse é um fator que temos que ter sempre em conta” (Mineiro, 2015).

A notícia em causa obteve 21435 visualizações só no endereço da notícia do JN e foi partilhada por 92 pessoas no Facebook, não tendo sido apuradas quantas vezes a notícia foi re-partilhada nas RS. Salienta-se também que esta notícia recebeu 187 comentários no endereço próprio da notícia, dos quais se destacam numerosos comentários depreciativos às Forças Armadas e FA em específico (MONTEIRO; BARBOSA, 2012).

6.3. Caso TugaLeaks

O TugaLeaks é um *website* de publicação de notícias online “onde várias pessoas podem escrever e comentar, e foi criado numa era onde a informação estava na Internet e não em papel”. Este *website* dá muito valor aos comentários às notícias feitos pelas pessoas que publicam pois, permitem “complementar a (…) notícia e acrescentar um valor humano e singular do ponto de vista de um cidadão comum à notícia redigida” e é apreciado “o poder de cada cidadão em contribuir ativamente para uma notícia” (TugaLeaks, [2014]).

No dia 08 de Fevereiro de 2013, o TugaLeaks publica uma “Denúncia” intitulada “Coronel da Força Aérea faz jantar de aniversário da mãe na Base Aérea de Beja”. Segundo a mesma, os militares que serviram o jantar demonstraram indignação com a situação, os convidados não eram militares e “tiveram ainda direito a um motorista

e um autocarro, ambos da Força Aérea" e deixa no ar a questão "quem é que irá pagar toda a festa de anos da mãe do Coronel" (Cruz, 2013).

Até à data, a notícia teve 2966 partilhas nas RS e recebeu 27 comentários só no *website* oficial do TugaLeaks (Cruz, 2013), não foi apurado a totalidade de comentários à notícia que se fizeram nas RS, no entanto, o grupo de Facebook "Anonymous Portugal" e "Indignados Lisboa" partilharam a notícia no Facebook no próprio dia e 4 dias depois, respetivamente. A notícia partilhada pelo "Anonymous Portugal" foi partilhada por 117 pessoas (Anonymous, 2013) e a notícia partilhada pelo grupo "Indignados Lisboa" foi partilhada por 28 pessoas (Indignados, 2013). Ambas as partilhas dos dois grupos receberam comentários bastante depreciativos concernentes à FA.

6.4. Importância da FA nas RS

A presença nas RS de uma instituição como a FA trás enormes vantagens, de acordo com o Chefe da área de Informação Pública da FA. "É que se não estivermos presentes nas RS, não sabemos o que dizem de nós, não podemos monitorizar, nem podemos intervir". Devido ao alcance proporcionado pelas RS, estas permitem à FA atingir uma grande quantidade de público, o que permite divulgar e promover a imagem da instituição, mostrar às pessoas o que fazemos e como fazemos, bem como intervir face às notícias e comentários, se for caso disso. Assim, o uso das RS permite atingir os grandes objetivos da informação pública da FA que são: informar, divulgar e instruir as pessoas. "Informar no sentido de dizer o que fizemos, divulgar no sentido de afirmarmos o que fazemos e instruir no sentido de ensinar as pessoas o que fazemos, porque fazemos e como fazemos" (Mineiro, 2015).

Como afirma Mineiro (2015) a representação institucional da FA nas RS cria laços e melhora a relação das pessoas com a instituição, fazendo com que as pessoas queiram intervir nas nossas RS e ainda com que as pessoas se sintam mais esclarecidas e motivadas para aceitar as notícias respeitantes à FA. Por exemplo, se as pessoas compreenderem as missões da FA bem como os motivos associados aos gastos orçamentais, serão mais compreensivas quando surgirem notícias como as referidas; ou por outro lado, permite que as pessoas tenham uma noção crítica realista, favorável à FA, quando se cruzarem com notícias e comentários pejorativos disseminados nas RS (Mineiro, 2015), vejam-se os exemplos em baixo, que

demonstram diferentes tipos de comentários feitos acerca da notícia expressa anteriormente em “Caso Resort 4 estrelas”:

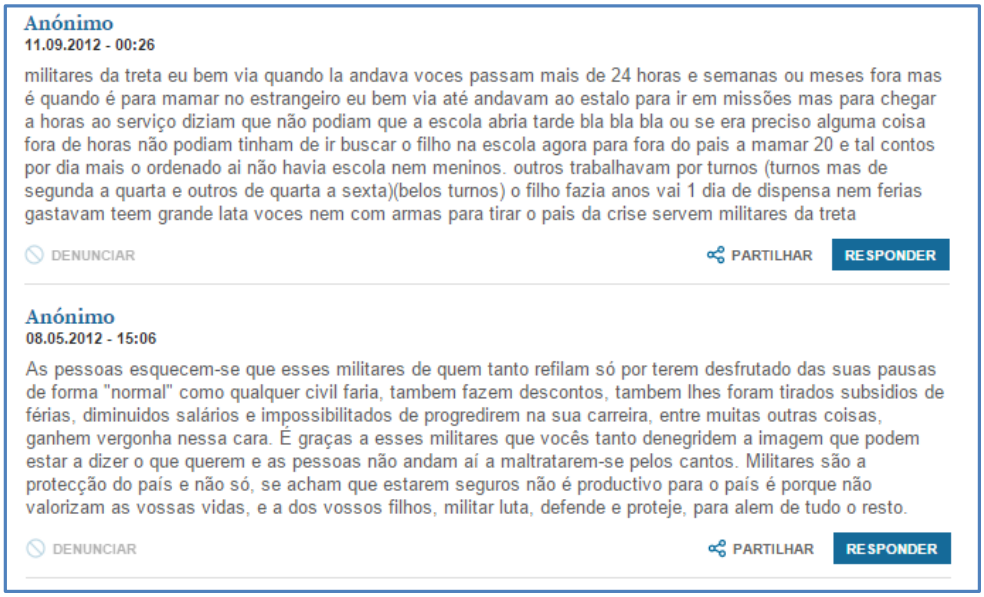


Figura 6 - Comentários no JN (MONTEIRO; BARBOSA, 2012). Em cima: comentário pejorativo contra os militares; em baixo: alguém que defende a missão dos militares

Figura 7 - Comentários no JN (MONTEIRO; BARBOSA, 2012). Em cima: comentário de um “provável militar” que se revolta contra outros comentários; Em baixo: comentário de um “suposto ex-combatente” que entra em conflito com o comentário de cima.

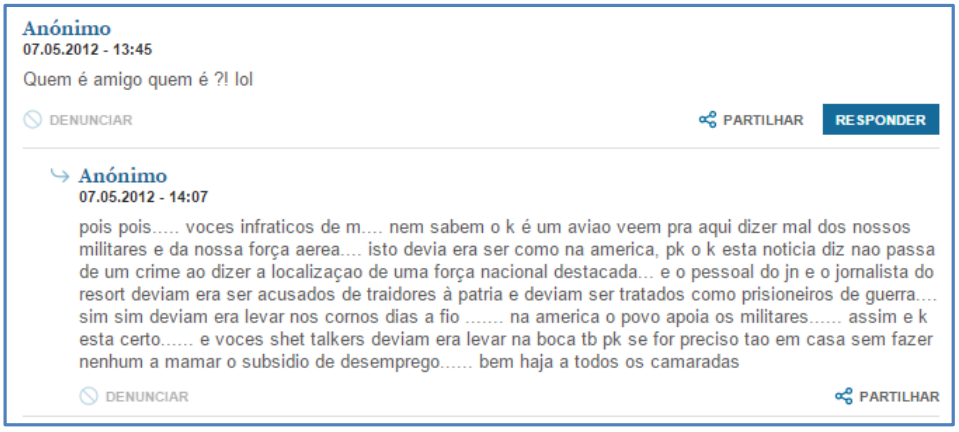


Figura 8 - Comentário no JN (MONTEIRO; BARBOSA, 2012) de um "provável militar" revoltado contra os comentários da Opinião Pública.

Por outro lado, e continuando a seguir Mineiro (2015) a presença da FA nas RS permite não só que as pessoas percebam melhor a nossa missão e a realidade da FA, mas também permite monitorizar o que se publica nas RS, no sentido de encontrar e sugerir correções a publicações feitas acerca da FA ou pelos próprios militares do Ramo e que possam estar a degradar a imagem da instituição (ver as Figuras 6,7 e 8) ou que prejudiquem a segurança da missão. Se não tivermos representação nas RS, não temos este *Awareness* (Mineiro, 2015).

Segundo Mineiro (2015), também no contexto internacional é importante e vantajoso para as operações da FA o uso das RS, é que, dado o alcance que poderemos ter com essas publicações, poderemos influenciar a OP internacional. Aliás, esta ideia materializa-se nos exercícios que a FA organiza. Aqui, existe a preocupação de divulgar a missão em português e inglês, o que contribui para uma influenciar a OP (Mineiro, 2015).

No caso particular de cada militar, Mineiro (2015) refere que, se existir a consciência para as questões de segurança nas RS, ou para a preservação da imagem da instituição ou ainda a consciência para as potencialidades da RS, então todos os militares podem contribuir com as suas publicações para influenciar positivamente a OP. Por exemplo, de acordo com Mineiro (2015), num cenário em que a FA está envolvida numa missão de ajuda humanitária no estrangeiro, as publicações individuais dos militares constituintes da missão nas suas RS, e onde sejam colocadas fotos, vídeos, texto que mostre essa ajuda é algo que pode ajudar a promover a imagem da FA e das FAA (Mineiro, 2015). Desta forma, a OP pode ser influenciada positivamente através das publicações dos militares e das RSFA.

Face ao expendido e segundo Nunes (2012), se confrontando as pessoas com certas notícias ou informações acerca da FA, é possível influenciar as suas opiniões, então, a OP pode ser influenciada positivamente através das publicações nas RSFA que, por sua vez, ao serem partilhadas pelos militares da FA nas suas RS pessoais, alcançam uma audiência maior (Nunes, 2012).

►Análise dos inquéritos (Anexo B): No sentido do disposto anteriormente, 45,6% dos militares inquiridos reconhecem que as RS permitem influenciar a OP em nosso favor (Sétimo parágrafo do Subcapítulo B-8, Anexo B).

►Segundo a Tabela B-16 (Anexo B), 88,4% dos inquiridos que já tiveram conta nas RS conhecem as RSFA, onde se destaca o Facebook que é a RSFA mais conhecida, que conta com 98,7% de militares. É de realçar, ainda na mesma tabela, que 79% estão atentos às publicações da FA (Tabela B-16, Anexo B). Também se acrescenta que, segundo a Figura B-6 (Anexo B), 50% dos militares comentam as publicações da FA muitas vezes, esporadicamente ou raramente o que demonstra interesse pelas publicações da FA.

►A Tabela B-17 (Anexo B) revela que a maioria dos militares, que tem conta nas RS e conhece as RSFA, já partilhou as publicações da FA nas RS, representando 64,5% (Tabela B-17, Anexo B). Segundo a mesma tabela, as intenções de cada militar ao fazê-lo variam, já que a maioria dos militares partilha as publicações das RSFA "para promover a imagem da FA" (56,6%) e "para promover a missão da FA" (53,9%) (Tabela B-17, Anexo B). Neste sentido, se os militares divulgam as publicações que promovem a imagem da FA e das operações, estarão a influenciar positivamente a OP, o que resulta numa vantagem no contexto deste capítulo.

►E também, segundo a Tabela B-18 (Anexo B), 78% dos militares que sentem orgulho ao verem as publicações das RSFA, partilham essas publicações (Tabela B-18, Anexo B). O que significa que essa percentagem de militares sente vontade de partilhar esse sentimento com a OP, o que, segundo Mineiro (2015), ajuda a potenciar a imagem da FA e das suas operações.

6.5. Conclusão Intermédia

A opinião das pessoas acerca das Forças Armadas é variável. É uma "guerra" de opiniões e críticas quotidianas que habitam e são potenciadas pelas RS, vejam-se as Figuras 6,7 e 8.

O Major Mineiro da FA destaca esta realidade e alega que a FA deve preocupar-se em formar e sensibilizar os seus militares para o trato com as RS, nomeadamente ao nível dos esclarecimentos de outros comentários, informando a OP acerca do que fazemos, como fazemos e porque fazemos, sabendo contar as "histórias" da FA, promovendo a sua imagem sem pôr em causa a segurança das operações e acima de tudo saber quem contactar em caso de dúvidas nestas matérias (Mineiro, 2015).

Tal como referido nas conclusões no Subcapítulo 5.2, as publicações das RSFA moralizam os militares por gerarem um sentimento de orgulho (Tabela B-16, Anexo B) e aliado a isso, 78% dos militares que sentem orgulho ao verem as publicações das RSFA, partilham essas publicações (referido no Subcapítulo 6.4 e Tabela B-18, Anexo B), o que ajuda amplificar a imagem da FA e das operações.

Para além disso, a análise dos inquéritos expressa no subcapítulo 6.4 permite concluir que a maior parte dos militares que partilham as publicações das RSFA fazem-no para potenciar a sua imagem (Tabela B-17, Anexo B).

Podemos então concluir que **"O uso das Redes Sociais, de forma individual e institucional, para potenciar a imagem da Força Aérea Portuguesa, influencia positivamente a Opinião Pública acerca das Operações Militares".** Assim, valida-se a hipótese.

7. (In)segurança nas Redes Sociais

Neste capítulo iremos analisar as potencialidades e os perigos inerentes à utilização das RS e que podem amplificar ou comprometer as OPMIL da FA. Assim, neste capítulo serão demonstrados os perigos que as RS comportam para as OPMIL, quais os comportamentos que os militares deverão adotar nas RS, como se comportam de facto os militares nas RS e por último será feita a comparação da FA com outras forças militares.

"O adversário está presente nas RS, *blogs* e fóruns, atento para encontrar todas as informações sensíveis acerca dos objetivos militares. Assim, é imperativo que todos os militares e as respetivas famílias compreendam a importância de praticar bons comportamentos que não comprometam a segurança das OPMIL" - Sergeant Major of the Army Kenneth O. Preston[19] (OTCPA, 2011)

Segundo Valente (2015)[20], as RS são sem dúvida uma ferramenta de apoio às OPMIL, trazendo potencialidades, mas também contemplando perigos. Tal significa que o uso deste veículo de informação social, pode potenciar as operações da FA ou, e seguindo Valente (2015), se não se controlar este veículo de informação, o mesmo poderá virar-se contra nós. Controlando o nosso veículo e estando atento ao adversário, reduzimos os riscos de quebras de segurança e potenciamos o nosso SA (Valente, 2015).

7.1. Perigos das Redes Sociais

Como vimos afirmando as RS podem ser um forte apoio na obtenção de SA contra o adversário mas ao mesmo tempo, tal como refere Valente (2015) poderemos ser nós a fonte de SA do mesmo e nesse sentido, a FA tem que se proteger, dando conhecimento e sensibilizando os seus militares (Valente, 2015).

O ser humano é uma barreira frágil no que toca à segurança cibernética e tanto os *hackers* como os manipuladores sociais sabem disso. As suas ações aparentam ser inofensivas e legitimas e com elas tentam enganar as pessoas por forma a ultrapassarem as barreiras de segurança (BDS, 2010), o que segundo Valente (2015), pode resultar em graves consequências para o militar, para a família ou para as operações da FA. No mesmo sentido, MSimões (2015) constata que é muito difícil

[19] Sergeant Major of the Army é o posto mais alto dos sargentos no U.S. Army

[20] O Major António Valente é Chefe da Repartição de Tecnologias da Informação (DCSI). Como Chefe da Secção de Ciberdefesa, é responsável por monitorizar as condições de segurança da FA, fazer auditorias de segurança e ajuda na elaboração de normas de segurança.

(senão impossível) controlar o que os militares publicam nas RS, sendo extremamente fácil que através de um comentário ou uma fotografia, sejam divulgados elementos que podem comprometer a segurança das operações (MSimões, 2015). Com a proliferação dos *Smartphones*, com capacidade de geolocalização, fotografar, filmar e publicar diretamente nas RS, esta realidade não está longe da FA. Vejamos.

►Análise dos inquéritos (Anexo B): segundo a Tabela B-8 (Anexo B), os *Smartphones* são sistemas banais de se encontrarem nos militares em operações. Mais concretamente, 90% dos militares inquiridos já teve e 73,3% tinha-o durante a missão (Tabela B-8, Anexo B).

Adiante, segundo a NSA [2015][21], as RS promovem o comportamento social e encorajam os *users* a partilharem informação e a confiarem naqueles a que estão conectados dentro das RS. No entanto, assim que uma informação é publicada nas RS, deixa de ser privada e mesmo que o *website* tenha boas definições de privacidade, existem muitas aplicações de RS instaladas inconscientemente e que permitem aos hackers o acesso às informações do equipamento (NSA, [2009]).

Até mesmo publicações que, à partida podem parecer triviais, podem ser perigosas, podendo resultar em fatalidades (OTCPA, 2011). Os inimigos procuram todas as informações possíveis em *blogs*, fóruns, *chats* e *websites* que contenham informações pessoais como o Facebook, Twitter, entre outros, para montarem um *puzzle* informativo que os possibilite atacar um alvo (OTCPA, 2011).

Valente (2015) refere que um adversário ou uma divisão da FA que possua uma equipa de especialistas na área de análise da informação em RS e que esteja atento aos *posts* consegue fazer um mapa de um destacamento com base nessas publicações (sejam fotografias, vídeos ou textos publicados). Tal é possível devido às técnicas de engenharia social. Porque "facilmente se adiciona uma amizade nas RS, podendo-se tratar de um adversário, que depois de estar dentro da nossa RS, pode publicar fotografias fazendo parecer que também é um militar da FA e facilmente é adicionado por outros amigos nossos". A certo ponto, "esse agente terá adicionado tantas amizades de militares portugueses que lhe permitirá fazer um mapa dos destacamentos a decorrer e com essa informação poderá comprometer as OPMIL da FA e não só" (Valente, 2015).

[21] NSA refere-se à National Security Agency, a Agência de Segurança Nacional dos EUA.

No quadro das ameaças à segurança das OPMIL, ENISA (2007) enquadra as seguintes no âmbito das RS:

- Agregação de dados: os perfis das RS podem ser descarregados para uma base de dados (onde podem constar informações como: nome, idade, morada, local de trabalho, familiares, amigos, animais de estimação, gostos, locais de preferência, etc.) (ENISA, 2007).

►Análise dos inquéritos (Anexo B): A Figura B-4 (Anexo B) evidencia esta ameaça. 73% dos militares inquiridos, não se preocuparam em remover das RS tudo o que os pudesse identificar como militares, antes de ingressarem na missão, (Figura B-4, Anexo B)

- Agregação de dados secundários: para além da informação constante nos perfis, é possível recolher outros dados de cariz pessoal nas RS, através dos *posts* e fotografias, por exemplo (ENISA, 2007).

Valente (2015), afirma que através das RS podemos descobrir as pegadas dos nossos alvos na forma de *posts*, *tweets*, dados pessoais e outras informações publicadas pelo público-alvo. Se depois pegarmos em todos esses dados e informações recolhidas, fizermos a filtragem e cruzamento podemos gerar conhecimento. Dados geram informação e informação gera o conhecimento (Valente, 2015). Nesse sentido, Marques (2015)[22] refere que um adversário que procure informações nas RS, ao analisar uma fotografia de um militar irá retirar dela tudo o que seja informação classificada, como por exemplo: armamento, aeronaves e a posição geográfica desses elementos (Marques, 2015).

►Análise dos inquéritos (Anexo B): A Tabela B-7 (Anexo B), demonstra que este perigo é uma realidade na FA já que 29,2% dos militares que usaram as RS durante missão fizeram publicações que mencionavam o local, com quem estavam no momento e/ou identificaram os camaradas (Tabela B-7, Anexo B).

- Reconhecimento facial: as fotografias são muito populares nas RS e podem servir para se identificar alguém e procurar mais informações acerca dessa pessoa noutras RS (ENISA, 2007).

- *Content-based Image Retrieval* (CBIR): é uma tecnologia em ascensão que permite relacionar caraterísticas de uma imagem com uma base de dados e assim saber o local em que a fotografia foi tirada (por exemplo, através de uma pintura de

[22] O Major José Marques é atualmente Adjunto para os Sistemas de Informação (EMFA-DIVCSI).

quarto com caraterísticas particulares, é possível identificar onde esse quarto se encontra, se este estiver presente nessas bases de dados gigantes (ENISA, 2007).

- *Click-jacking*: Consiste em disponibilizar hiperligações que aparentam ser inofensivas mas que, quando clicadas, podem significar ações diferentes das pretendidas pela pessoa e que são executadas inconscientemente (FBI, [2015]). Na verdade, ao clicar numa hiperligação deste tipo podemos estar a fazer *download* de *malware* ou a enviar o nosso IP para um *website* de destino. Ao nível das RS, algumas táticas de *click-jacking* foram usadas onde as hiperligações maliciosas se encontravam camufladas nos botões de "*Like*" e "*Share*". (FBI, [2015])

- *Doxing*: publicar informações de identificação pessoal de terceiros incluindo o nome completo, a data de nascimento, a morada e imagens, retirados das RS. Essas informações podem ser acerca do próprio, de familiares ou amigos. (FBI, [2015])

- Aliciação: Conversa estratégica com o intuito de extrair informações das pessoas sem que as mesmas sintam que estão a ser interrogadas. (FBI, [2015])

- *Pharming*: Redireccionamento dos *users* de *websites* legítimos para *websites* fraudulentos com o propósito de extrair dados confidenciais ou infetar o equipamento. (FBI, [2015])

Exemplo de caso: um *social engineer* que através de conversas nas RS, consegue que o seu alvo aceda ao *website* da FA, que aparentemente corresponde ao *website* real da FA, mas que na verdade é uma cópia (cópia feita pelo *hacker*). Quando a vitima tiver acedido ao *website* falso, estará a abrir a porta ao adversário para obter informações como *passwords*, conversas acerca de operações, entre outras informações importantes (FBI, [2015]).

Phishing – envio de correio eletrónico que aparenta ter sido enviado por uma pessoa ou organização legitima, mas que pelo contrário, contém um *link* ou um ficheiro com *malware*. Se este ataque for direcionado para um alvo específico (organização ou pessoa), trata-se de *spear phishing*. O *phishing* pode ainda ser realizado através do envio de links maliciosos nas RS. (FBI, [2015])

Esta técnica pode ainda ser usada com o intuito de ganhar acesso integral a uma conta nas RS, permitindo ao atacante saber tudo o que o alvo tem nas RS e inclusive fazer publicação como se fosse o responsável por essas contas (Valente, 2015).

Fraude cibernética: o adversário pode aproveitar eventos populares e notícias como um isco para que os militares abram correio eletrónico ou visitem *websites* infetados (FBI, [2015]).

Personificação – acontece quando o atacante finge ser um amigo de um alvo nas RS, influenciando-o a fornecer informação privada ou a fazer *download* de aplicações ou conteúdos maliciosos (NSA, [2009]).

Conteúdo malicioso (*malware*) – as RS permitem que os *users* partilhem vários tipos de multimédia, desde imagens, a clips de vídeo e documentos (NSA, [2009]). Estes conteúdos podem ser instaladas sem o conhecimento do *user* e executam ações com diversos fins, desde furto de *passwords* até à apropriação da capacidade de computação (RFA390-6, 2011).

Fuga de informação involuntária – As fugas de informações acerca das OPMIL podem ocorrer inconscientemente, quando um militar faz publicações que não deveria sem se aperceber da informação que está a expor (Gonçalves, 2015). Ou pode ainda ocorrer quando os familiares, pouco conscientes dos perigos das RS, fazem publicações que podem comprometer as OPMIL (Mineiro, 2015).

►Análise dos inquéritos (Anexo B): Na Figura B-5 (Anexo B), constata-se que 47% dos militares afirmam que os familiares e/ou amigos (F/A) chegaram a fazer publicações nas RS que mencionavam a missão em que os militares estavam envolvidos (Figura B-5, Anexo B). Com o inquérito realizado, foram aferidos ainda que tipo de informações foram dadas aos F/A acerca da missão, onde se destaca que 70% dos militares, informaram sobre o local e a data da missão aos familiares e/ou amigos (Tabela B-10, Anexo B). Mais, segundo a Tabela B-11 (Anexo B) 13,3% dos militares inquiridos assumiram que não consciencializaram os F/A acerca dos perigos das RS, dos quais 3,3% de militares acreditam que não têm que ter cuidados nas RS (Tabela B-11, Anexo B).

Geotagging – Com novas tecnologias surgem novos riscos. Tem-se notado o aumento de popularidade de aplicações que permitem geolocalização de publicações nas RS, no entanto, a exposição da geolocalização das publicações pode, em certas situações, ser devastador para as OPMIL (OTCPA, 2011).

O Geotagging é uma tecnologia que faz a identificação geográfica automática de fotografias, vídeos, *websites* e mensagens de texto através de aplicações de localização. Permite que as pessoas encontrem imagens e informações comuns à localização do telemóvel ou computador (AFPAA, 2013). Os militares devem ter em especial atenção a não permissão desta caraterística nos telemóveis bem como a não utilização de aplicações de localização durante as operações. O Geotagging representa sérios riscos de segurança pessoal e operacional (AFPAA, 2013).

Steve Warren refere que hoje em dia, em quase todos os *Smartphones* existe GPS integrado e em cada fotografia tirada com esse telemóvel, estarão identificadas as coordenadas geográficas onde essa fotografia foi tirada (Rodewig , 2012).

Com as tecnologias atualmente existentes e as aplicações de telemóvel facilmente acessíveis, existe sempre o perigo do militar estar a ser seguido e involuntariamente dar informações sobre a localização onde esse telemóvel está, bem como ao fazer *posts* nas RS estar a informar publicamente onde se está devido à geolocalização, tal é corroborado por Marques (2015) que acrescenta que isso representa uma ameaça para os militares da FA pois pode indicar onde estão a decorrer OPMIL e os trajetos que foram feitos (Marques, 2015). Neste sentido, a problemática do Geotagging foi aprofundada pelos inquéritos (Anexo B).

►Análise dos inquéritos (Anexo B): A Tabela B-8 (Anexo B) revela que 26,7% dos militares inquiridos não sabem o que é o Geotagging (Tabela B-8, Anexo B). Para além disso, também se demonstra na mesma que 16,7% dos militares inquiridos tinham o *Smartphones* durante a missão e ignoram o que é o Geotagging (Tabela B-8, Anexo B). Pior ainda, é que segundo a Tabela B-9 (Anexo B), de um grupo de militares que não sabem o que é o Geotagging e usaram as RS durante a missão, constata-se que 58,8% tinham consigo o *Smartphones* abrindo a possibilidade das operações serem geolocalizadas pelo adversário (Tabela B-9, Anexo B).

7.2. Casos Estudo

1- Em 2007, o Geotagging conduziu a uma situação catastrófica. Segundo Steve Warren, após ter chegado a uma base no Iraque uma nova frota de helicópteros AH-64 Apaches, alguns militares tiraram fotografias e publicaram-nas na Internet, sem terem tido o cuidado de retirar a opção de Geotagging dos seus telemóveis. Através dessas fotografias, o inimigo foi capaz de saber a localização exata dos helicópteros e destruiu 4 dos helicópteros com um ataque de morteiro (Rodewig , 2012).

2- Em Maio de 2009 o Facebook foi usado por indivíduos fraudulentos que contataram com os familiares do pessoal militar destacado dos EUA. Fizeram-se passar por soldados e informaram os avós dos alvos de que estavam a regressar da missão no Iraque pedindo que isso se mantivesse em segredo para que pudessem surpreender os pais (BDS, 2010). Mais tarde, pediram aos “avós” o envio de grandes quantidades de dinheiro para pagar os custos das reparações do carro (BDS, 2010).

3- Depois da morte de Osama Bin Laden em 2011, foi publicado um vídeo no Facebook que garantia mostrar a captura do mesmo. Esse vídeo era falso e quando os *users* clicavam no vídeo, era-lhes imposta a necessidade de copiar um código de *JavaScript* para a barra do *browser* (FBI, [2015]). Ao fazerem-no, estavam também a partilhar automaticamente esse vídeo para a rede dos amigos no Facebook, bem como permitiam aos *hackers* acesso completo às contas das vítimas. (FBI, [2015])

4- Em Julho de 2014 Alexander Sotkin, um jovem militar Russo, publicou *selfies* no Instagram que o localizavam em território Ucraniano. Para alguns, significou uma excelente fonte de INTEL cujo significado era a presença declarada dos militares Russos no Este da Ucrânia, para outros significou apenas um erro por deixar essas fotografias com o Geotagging ativado (Jensen, et al., 2014).

7.3. Comportamento dos Militares nas Redes Sociais

A principal preocupação ao usar as RS é a segurança das operações. As OPSEC (*Operations Security*) são cada vez mais importantes, uma vez que as RS são um meio de transmissão de informação que está a crescer muito rapidamente (OTCPA, 2011).

Acerca da Segurança das Operações, o DoD (2011) refere que todo o pessoal (onde se incluem as famílias e amigos do pessoal de serviço) tem a responsabilidade de se assegurar que nenhuma informação publicada nas RS possa constituir perigo para os militares ou que possa ser usada pelos adversários como uma oportunidade de causar dano aos militares (DOD, 2011). Entre o tipo de informações possível encontram-se as informações técnicas, horários e datas de movimentos militares, localização de unidades militares, detalhes sobre armamento ou discussão sobre locais a frequentar pelos militares (DOD, 2011).

Na ótica dos EUA, quando um militar usa as RS deve-se reger constantemente pelas normas de conduta. Ou seja, fazer comentários ou qualquer tipo de publicações que violem os regulamentos e as regras básicas de conduta militar, são procedimentos proibidos (OTCPA, 2011). As RS dão a possibilidade aos militares de se expressarem, no entanto, mesmo fora de serviço, estão sujeitos a regulamentos próprios e por isso, denegrir a imagem dos militares ou publicar informação sensível é punível. Ainda segundo a mesmo fonte, é importante que todos os militares saibam que nas RS também estão a representar as Forças Armadas (OTCPA, 2011).

Marques (2015) afirma que as RS devem ser encaradas pelos militares da FA como algo que pode trazer consequências reais, como tal, os seus comportamentos nas RS deverão ser sempre cuidados tal como são no seu dia-a-dia. “Somos militares 24 horas por dia e estamos sujeitos ao Regulamento de Disciplina Militar (RDM), o que implica que o nosso comportamento esteja sempre sujeito às suas normas”. Refere ainda que, sempre que tivermos um comportamento impróprio nas RS podemos ser punidos tal como se o fizéssemos num café com amigos. É por isso imperativo que os militares tenham sempre a noção dos deveres militares que juraram cumprir e quais os comportamentos que devem ter (Marques, 2015).

Na generalidade, os militares da FA têm a plena consciência de que têm o dever de respeitar os regulamentos aos quais estão sujeitos, mas por outro lado, não têm a adequada noção do perigo que a comunicação através das RS pode representar para as operações. Ainda segundo Marques (2015) existe a necessidade, na FA, de criar políticas e sensibilizar os militares para a realidade das RS (Marques, 2015).

No caso particular dos EUA, este tipo de sensibilização e criação de políticas é abundante e está acessível a qualquer pessoa que visite as páginas oficiais de diversos órgãos de defesa, dos quais se destacam: DoD, U.S. Army, U.S. Air Force, U.S. Navy e U.S Marine Corps.

Nas publicações feitas pelos órgãos supra referidos, são mencionados diversos documentos pelos quais os militares se deverão reger bem como os comportamentos que deverão adotar nas RS.

Dos vários perigos das RS, um que se destaca é o Geotagging e nesse sentido, segundo o OTCPA (2011), os militares nunca deverão identificar geograficamente as publicações nem usar aplicações nas RS que possibilitem a geolocalização seja em operações, treino ou de serviço em locais cuja identificação espacial em formato de coordenadas, possa danificar as OPMIL. Nesse sentido, enquanto em operações, os militares devem desativar a função GPS dos seus *Smartphones*. Caso contrário, as OPMIL poderão ser comprometidas (OTCPA, 2011).

Outros comportamentos a adotar pelos militares nas RS consistem em evitar mencionar o posto, localização da base, datas dos destacamentos, nomes, especificações e capacidades de equipamento (OTCPA, 2011).

Um dos grandes desafios das RS para as OPMIL é que se consiga separar a esfera pessoal da esfera profissional, refere EC (2015). Ou seja, vejamos o exemplo: os militares em operações são várias vezes alvos de sedução por parte de outros

users das RS. Na verdade, muitos desses são espiões que constroem perfis falsos e seduzem militares através das fotografias de perfil e pelas conversas. Depois dos militares se deixarem seduzir, o espião tem oportunidade de recolher muitas informações secretas, nomeadamente (informações acerca de armamento, data e local de futuras operações, etc.) (EC, 2015).

7.3.1. Consciência de Segurança dos Militares da FA

Mineiro (2015) refere que ao nível da FA, ainda não existe consciência de segurança por parte dos militares em missões, como tal o mesmo autor garante que se fizermos uma pesquisa aos perfis dos militares em operações internacionais, iremos encontrar quebras de segurança nas suas publicações. Ainda segundo o mesmo, as questões de segurança nas RS não devem ser encaradas como algo do senso comum, antes pelo contrário, devem ser dadas instruções claras e precisas como forma de diminuir ou anular publicações prejudiciais. Mineiro (2015) chegou a identificar e intervir em quebras de segurança por parte de alguns militares em missões internacionais. Estas falhas estavam relacionadas com determinadas publicações onde era possível identificar quem era o user, que o mesmo era militar da FA e onde se encontrava a prestar serviço no momento (Mineiro, 2015).

No sentido do disposto, vejamos a análise do inquérito (Anexo B).

►Análise dos inquéritos (Anexo B): Tal como referido no subcapítulo 7.1, 29,2% dos inquiridos identificaram as suas publicações com o local, e/ou com quem estavam durante o tempo da missão (Tabela B-7, Anexo B).

► Outro dos perigos tem a ver com a exposição pública da profissão dos militares, já que apenas 23% dos inquiridos preocuparam-se em descaraterizar[23] as RS antes de ingressarem nas missões, tal como demonstra a Figura B-4 (Anexo B). No entanto, a Tabela B-4 (Anexo B) revela também que a grande maioria dos militares, isto é, 87,8% dos militares inquiridos, acredita que as RS podem conduzir a quebras de segurança (Tabela B-4, Anexo B).

►Segundo a Tabela B-6 (Anexo B), 95,6% dos militares que usaram as RS em missão contataram com os familiares e/ou amigos pelas RS e desses, segundo a Figura B-3 (Anexo B) 88,9% contactaram através das mensagens privadas nas RS (através do *chat*), o que segundo Mineiro (2015) pode ser uma forma segura de conversar com os familiares. Como tal, Mineiro (2015) refere que para além da

[23] Por descaraterizar entende-se retirar das RS tudo o que possa identificar o indivíduo como militar.

descaraterização das RS, os militares devem ter a consciência dos perigos que podem afetar as operações e agir em conformidade, nomeadamente, *briefar* as famílias e combinar códigos para poderem falar em segurança nos *chats* das RS (Mineiro, 2015).

Nesse sentido, demonstra-se um exemplo *chat*, na Figura 9:

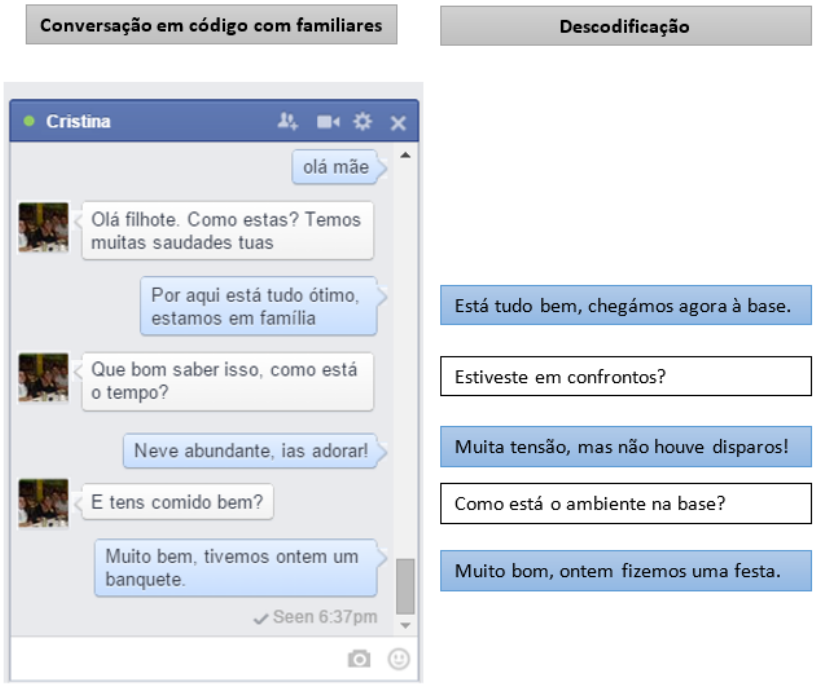


Figura 9 - Conversa em código entre um militar e a sua mãe, através do chat do Facebook.

7.4. Realidade da FA quanto aos Perigos das RS

Marques (2015) e Mineiro (2015) referem que não existem políticas nem doutrinas na FA que uniformizem e regulem a utilização das RS. Mineiro (2015) acrescenta que não são feitas suficientes ações de sensibilização aos militares acerca desta temática e deveria haver uma maior preocupação hierárquica[24] acerca desta realidade (Mineiro, 2015).

De acordo com Mineiro (2015), esta realidade parece resultar da perceção de que devemos ter uma presença nas RS, não se identificando, no entanto, toda a amplitude do uso das RS, nomeadamente ao nível das capacidades disponíveis e dos perigos que podem comprometer as operações (Mineiro, 2015).

7.4.1. Experiência

Segundo Costa (2015), as RS podem comprometer uma operação. Enquanto comandante de destacamento na Islândia, uma das grandes preocupações consistiu

[24] Por preocupação hierárquica entende-se como a preocupação das hierarquias competentes para criação das Ordens de Operações e outros documentos que devam refletir a adequada integração das RS nas OPMIL.

em controlar a informação que era publicada nas RS pelos militares destacados, dada a quantidade de meios que permitem veicular informação classificada para essas plataformas e a dificuldade que existe em controlar. Para o efeito, com a cooperação de um oficial das RP, foi dada liberdade aos militares para que pudessem publicar nas RS, ao mesmo tempo que essa informação era monitorizada e filtrada, satisfazendo assim os elementos do destacamento por verem algum do seu trabalho e experiências a serem publicadas, ao mesmo tempo que se garantia o controlo "parcial" da situação. Parcial, porque o controle das publicações nas RS nunca é absoluto (Costa, 2015).

Costa (2015) refere ainda que desde a preparação do destacamento, nos briefings, foi altamente ampliado que durante a operação seria difundida nas RS todo o tipo de publicações que os militares quisessem desde que não comprometessem a segurança das operações. Nesse sentido, as publicações eram primeiro monitorizadas e avaliadas em termos de segurança para depois serem publicadas num *blog* no *website* do EMFA[25], criado para o efeito, onde desde o início do destacamento se publicou informação acerca da operação, fotografias e entrevistas onde os militares retratavam o seu dia-a-dia.

Muitas das publicações nesse *blog* eram depois republicadas nas RSFA e eventualmente nas RS pessoais de cada militar. Costa (2015) constata ainda que o facto de alguém se encarregar de publicar o trabalho dos militares no destacamento, faz com que os próprios não tenham tanta necessidade de o fazer no perfil pessoal e muitas vezes comprometendo a segurança das operações (Costa, 2015).

Esta prática foi assumida pelo comandante do destacamento referido, por opção e experiência própria, já que o mesmo participa nas RS e conhece os perigos e vantagens das RS em OPMIL (Costa, 2015).

Costa (2015) aponta que na FA ainda não existe formação nem sensibilização dos comandantes no âmbito das RS apesar de ser uma formação importante e que, neste momento, a formação de cada militar deriva apenas da experiência de uso pessoal das RS (Costa, 2015).

7.4.2. Consciencialização

No âmbito da FA é necessária a sensibilização dos militares e a criação de políticas e guias práticos de utilização das RS e das tecnologias (tal como existe nos EUA). Ou seja, não basta criar políticas pois estas só serão eficazes se forem

[25] EMFA é o Estado-Maior da Força Aérea Portuguesa.

cumpridas, refere Marques (2015). As políticas regulam como deve ser o comportamento do militar, nomeadamente na esfera das RS. Por isso, abaixo das políticas terão que haver outras literaturas e ações que expliquem o que é que o militar deve fazer para cumprir as políticas e isso torna-se possível através dos seguintes exemplos: *links* no *website* da FA e nas RSFA que remeta para questões frequentes (*FAQ's*), exemplos práticos, guias, ensino nas instituição académicas militares, casos estudo, distribuição de panfletos, palestras, apresentação de filmes, entre outros. Continuando a seguir Marques (2015), todos estes mecanismos permitem efetivar na prática a política. No fundo, trata-se de consciencializar os militares acerca da problemática em questão, sendo esta ação ainda mais importante do que a própria política que surge como enquadradora (Marques, 2015).

Esta preocupação existe no RFA 390-6 que revela que a falta de cultura de segurança "traduz-se essencialmente num problema organizacional motivado pela incompreensão e, consequentemente, pelo incumprimento dos regulamentos e procedimentos de segurança aprovados". Se os recursos humanos "não possuírem a formação e o treino adequados não poderão prevenir, detetar e reagir aos incidentes de segurança, tornando-se assim mais vulneráveis a ataques de "engenharia social"" (RFA390-6, 2011).

Em 2015, Gonçalves (2015) ainda alerta para uma ingenuidade muito grande por parte das pessoas no que toca a matérias relacionadas com as quebras de segurança ao nível das RS e que na maior parte das vezes são inconscientes. Tal seria facilmente resolvível com explicações, instruções e briefings. Salienta ainda que enquanto esteve em operações no Afeganistão não recebeu nem soube de ninguém que tivesse recebido qualquer briefing acerca da utilização das RS (Gonçalves, 2015). Por outro lado, EC (2015) revela que atualmente são feitas ações de sensibilização e formação na utilização das RS no âmbito pessoal sem comprometer a segurança da operação (pessoas e bens) para os militares que vão para missões EC (2015), algo que MSimões (2015) constata como uma verdade, referindo que na preparação para a missão que desempenhou no Afeganistão, foi *briefado* acerca das quebras de segurança nas RS (MSimões, 2015).

►<u>Análise dos inquéritos (Anexo B):</u> No entanto, tal como referido em anexo (Tabela B-13, Anexo B) nem todos os militares são devidamente *briefados*. A Tabela B-13 (Anexo B) revela que 17,8% dos militares não foram *briefados* antes de ingressarem na missão mais longa (Tabela B-13, Anexo B) e a Tabela B-12 (Anexo

B) indica que 10% dos inquiridos nunca foram *briefados* acerca das RS (Tabela B-12, Anexo B). Ainda na Tabela B-12 (Anexo B) contabilizam-se 33,3% de militares que podem ter sido ameaças à segurança, na medida em que não foram devidamente *briefados* acerca das RS antes de todas as missões.

►Segundo a Tabela B-14 (Anexo B) 67,8% dos inquiridos afirmam que deviam ser feitos mais *briefings* acerca das RS e ainda na mesma tabela, 63,3% afirmam que poucos militares dão a devida importância aos *briefings*.

Caso Estudo: Na sequência do disposto anteriormente, Mineiro (2015) relata que *briefou* apenas um grupo de militares que foi em missão para o Mali e que 2 militares não puderam assistir a esse briefing. Mais tarde, ambos os militares vieram a cometer quebras de segurança ao nível das RS: num dos casos, a mãe do militar identificou nas RS o local em que as operações estavam a decorrer; no outro caso, o próprio militar publicou que tinha acabado de cumprir uma missão, revelando a força que estava no terreno (Mineiro, 2015). É ainda de salientar, que os restantes grupos não receberam briefing acerca das RS (Mineiro, 2015).

A FA não se encontra na estaca zero no que concerne às ações de consciencialização. No início do presente ano letivo 2014/2015 foi ministrada uma palestra aos alunos da AFA acerca dos perigos das RS, o que permite, principalmente aos novos alunos, tomarem a consciência dos perigos das RS no âmbito militar, refere Costa (2015). O mesmo entende que este tipo de palestras deverá ser ministrado todos os anos na AFA (Costa, 2015). Mineiro (2015), que foi o palestrante acerca dos perigos das RS em 2014 na AFA, refere que também foi ministrada uma ação de sensibilização a um pequeno grupo na OTA em janeiro de 2015 e que, também ao nível das esquadras de voo da FA já foram feitas algumas mas sempre a convite das próprias esquadras. Devido ao facto de existirem poucos militares com conhecimento da temática das RS, torna-se complicado que, por vontade própria, se disponibilize a palestrar mais vezes para os militares da FA (Mineiro, 2015).

Mais uma vez, releva-se a importância da Consciencialização. O RFA 390-6 destaca que “a área de formação deve merecer especial atenção, com a inclusão do estudo destas matérias em todas as estruturas curriculares e em todos os graus de formação administrados na Força Aérea, muito em especial aqueles relacionados com as TIC. Prosseguir esta política na formação, além de proporcionar o conhecimento sobre a ciberdefesa, introduz a consciência sobre esta realidade e o cuidado que ela

merece promovendo, simultaneamente, a tão desejada "cultura de segurança"" (RFA30-6, 2011).

7.4.3. Literatura da FA acerca das RS

Marques (2015), afirma que a FA, nomeadamente o EMFA, ainda não criou doutrina nem políticas que regulamentem a utilização da Internet, mais concretamente a utilização das RS pelos militares. A criação deste tipo de documentos que regulamentem especificamente a utilização das RS é importante (Marques, 2015) e segundo Mineiro (2015), existe a necessidade que seja criada literatura portuguesa a que qualquer militar possa recorrer para se enquadrar no âmbito desta temática. Neste sentido, Valente (2015) refere que esse tipo de políticas estão ainda a ser feitas. Mineiro (2015) afirma igualmente que os militares devem ser ensinados a usar e se comportar corretamente nas RS pois "não basta dizer-se que um computador é uma arma, tem que se ensinar os militares a usar a arma e não basta dizer-se que se não contarmos a nossa história alguém a conta por nós, tem que se ajudar os militares a contar a história, sem comprometerem as OPMIL" (Mineiro, 2015).

7.4.3.1. ORDOPS

Mineiro (2015) constata que até à data não existiu ainda nenhuma ORDOPS[26] publicada onde tenham sido contempladas informações referentes à segurança nas RS, embora represente um tópico importante. No mínimo, deveria constar a necessidade de *briefar* os militares quanto à temática em causa: comportamentos a ter nas RS durante as OPMIL (Mineiro, 2015).

Neste sentido, foram revistas pelo autor um total de 22 ORDOPS Não Classificadas, das quais 10 remetem ao ano de 2013 e as outras 12 ao ano de 201, retirando-se algumas conclusões:

- É dado enfase à necessidade de acessos à internet como meio de bem-estar dos militares (*Welfare*) aquando em operações no estrangeiro, nas seguintes: NEP/OPS-028; ORDOPS 008/13; ORDOPS CA 012/13; ORDOPS 013/13; ORDOPS 014/13; ORDOPS 021/13; ORDOPS CA 003/14; ORDOPS CA 005/14; ORDOPS CA 006/14. No entanto, em nenhuma são destacadas as RS, em específico, como uma ferramenta de motivação para os militares, nem referidos os cuidados a ter.

[26] Ordens de Operações. É um documento promulgado pelo Comando Aéreo.

- Em diversas ORDOPS, é atribuída importância aos meios de comunicação social[27], já que é referido que não se pode participar em atividades ou comunicar com os meios de comunicação social sem a autorização específica de entidade nacional, nas seguintes: ORDOPS 008/13; ORDOPS CA 010/13; ORDOPS 016/13; ORDOPS CA 017/13; ORDOPS CA 020/13; ORDOPS CA 008/14.
- É referido que o comandante de destacamento não está autorizado a Produzir ou libertar para os Órgãos de Comunicação Social (OCS) informação respeitante a acidentes/incidentes que envolvam pessoal e meios nacionais., nas seguintes: ORDOPS 008/13; ORDOPS CA 010/13; 013/13; ORDOPS CA 017/13; ORDOPS CA 020/13; ORDOPS CA 006/14; ORDOPS CA 008/14.
- Mais próximo do universo das RS, na ORDOPS 006/14 são referidos os cuidados com os média e os objetivos das RP da FA, visando alcançar alguns objetivos no que concerne à OP acerca de temas como a missão da FA e dos meios que dispõe. São também disponibilizados contactos para esclarecimento de dúvidas quanto ao trato com os média. É de salientar que em nenhum ponto é referido o uso das RS para potenciar a imagem da FA, nem acerca dos cuidados a ter pelos militares, o que assume especial importância já que se refere a disponibilização da internet como um meio de *Welfare*.
- Na ORDOPS 010/14 são referidas as RS, mas apenas no âmbito da divulgação da informação pública acerca do evento, o 62º Aniversário da FA.

7.4.3.2. Diretivas

Nas diretivas publicadas pelo CA, não existe nenhuma informação acerca das RS, em particular no que concerne ao 60º aniversário da FA, em 2012, não existe escrita a possibilidade de publicitação do evento nas RS, uma vez que um dos objetivos é "divulgar a temática aeronáutica, as atividades, a capacidade técnica e a competência profissional do pessoal da Força Aérea junto da população, em geral e, da juventude em particular". Nesse sentido, é definido que o GABCEMFA publicita junto dos órgãos de comunicação social e do público em geral todos os eventos relacionados com as Comemorações (DIROP, 2012).

[27] Segundo o Priberam [2013a], comunicação social define-se como o conjunto dos órgãos de difusão de notícias (imprensa, rádio, televisão).

Na Diretiva 06/09, publicada pelo EMFA (2009), é assumida a necessidade de "normalizar um conjunto de princípios e procedimentos de segurança (…) relacionados com a utilização de equipamentos de TIC". Refere ainda que a evolução das TIC bem como a utilização das mesmas, têm uma reconhecida dificuldade de serem acompanhadas pela doutrina da NATO ou de Portugal. Refere ainda que a doutrina existente está dispersa por várias publicações e desatualizada face aos novos equipamentos que vão surgindo (EMFA, 2009). No entanto, a presente diretiva é destinada apenas às áreas de segurança de Classe 1, onde ocorre o "armazenamento, processamento e transmissão de informação classificada com o grau de classificação de segurança de CONFIDENCIAL ou superior".

A diretiva apresentada não se aplica à realidade do presente ano, no que toca à facilidade de perpetuação de quebras de segurança, no âmbito das RS em OPMIL, por parte dos militares que gerem informações com o grau de classificação de segurança de Confidencial ou superior. Ainda assim, é referido na mesma que "Toda a estrutura da Força Aérea deverá estar comprometida com os objetivos da segurança, donde a manutenção das condições de segurança da exploração dos SIC é uma responsabilidade partilhada por todos e assente no respeito pela doutrina de segurança em vigor." (EMFA, 2009).

7.4.3.3. NEPS[28]

Foram revistas pelo autor 114 NEPs Não Classificadas e não foram encontradas quaisquer informações referentes às RS. Nomeadamente, nas NEPs de segurança geral e interna Não Classificadas, não consta qualquer informação acerca de quebras de segurança derivadas do uso indevido das RS.

7.4.3.4. Apresentações

De acordo com a pesquisa do investigador, não existem apresentações no *website* da FA ou na rede interna da FA que sensibilizem para os perigos das RS, preservação da imagem institucional, quebras de segurança, ferramentas das RS, entre outras temáticas que envolvam as RS.

7.4.3.5. RFA 390-6

O RFA 390-6 é uma publicação destinada a "estabelecer a Política de Ciberdefesa na Força Aérea". Neste documento, que remonta a 2011, as RS são um

[28] Notas de Execução Permanente. É um documento promulgado pelo Comando Aéreo.

assunto abordado onde são frisados alguns perigos inerentes ao uso incorreto das mesmas e onde é realçado que são “o campo de excelência para a aplicação de técnicas de engenharia social e a propagação de *malware*” (RFA390-6, 2011).

O acesso ao documento não está facilitado, já que para o obter, o investigador teve que se dirigir ao Sub-Registo no EMFA não o tendo encontrado nem no *website* da FA, nem na Rede Interna nem em qualquer outro local.

7.4.4. As Redes Sociais noutras Forças Militares

No sentido de se aprender e dar a conhecer a realidade da FA quanto à utilização segura das RS, serve o presente subcapítulo para enquadrar a realidade da instituição com a realidade de outras Forças Militares.

7.4.4.1. Reino Unido

As Forças Armadas do Reino Unido (FARU) já aceitaram a realidade das RS e desenvolveram uma estratégia que encoraja o seu uso. No entanto, é exigido que os militares sejam responsáveis e que tenham completa consciência daquilo que podem publicar de forma a não comprometer a segurança pessoal e operacional (Jensen, et al., 2014). A experiência das FARU indica que os militares têm cada vez mais vontade de interagir nas RS e por isso, as medidas de segurança são importantes (Jensen, et al., 2014).

O ministério da defesa do Reino Unido criou uma campanha *online*, em 2013, que se chama “*to think before you share online*” e encoraja os seus militares a usarem as RS sem se identificarem como sendo militares (MOD, 2013). Nessa campanha são identificados os efeitos danosos que advêm da má utilização das RS, podendo afetar negativamente a moral dos militares bem como o apoio da OP. São focadas diversas áreas de preocupação através de texto e da apresentação de vários vídeos de sensibilização, tais como: a proteção dos militares e das suas famílias; a proteção da instituição militar; e a proteção da reputação militar (MOD, 2013).

7.4.4.2. Estados Unidos da América

Nos EUA, ao nível dos departamentos de defesa nacional, existem diversas publicações que promovem a consciencialização dos militares quanto ao aproveitamento das potencialidades das RS e quanto às questões de segurança. Neste sentido, serão mencionados os seguintes: DoD, U.S.Army, U.S.Air Force, U.S. Navy e U.S Marine Corps.

7.4.4.3. DoD

O DoD tem uma conta oficial no *website* www.slideshare.com onde, numa das 54 apresentações que disponibiliza ao público, se destaca para a temática em causa, um briefing de consciencialização acerca da segurança nas RS. Neste briefing são dadas várias sugestões que visam proteger a instituição e outras que visam a proteção individual. São disponibilizados contactos oficiais para dúvidas e direcionamento para outros briefings importantes ao nível da internet (BDS, 2010).

O DoD dispõe ainda de uma página no *website* oficial, acerca das políticas de uso das capacidades da internet, onde se incluem as RS, e redireccionamento para outras forças dos EUA igualmente conscientes acerca das RS: USArmy, USNavy, USAirForce, USMarine Corps (DOD, [2015b]).

7.4.4.4. U.S. Air Force

Dispõe ao público informações acerca de segurança nas RS através do "2013 Social Media Guide" (USAF, [2015]). E acerca da segurança em operações no contexto das RS publicou em 2011 o documento "Air Force Instruction 10-701" (DOTAF, 2011).

7.4.4.5. U.S.Army

O U.S. Army publica no seu *website* oficial o documento "USArmy Social Media Handbook" (OTCPA, 2011).

7.4.4.6. U.S. Navy

Têm várias páginas publicadas, que qualquer pessoa pode visitar, acerca das RS, nomeadamente:

- Boas práticas nas RS, onde se ensinam a usar as RS com as diversas aplicações que existem alertando simultaneamente para os seus perigos (DON, [2015]);

- Políticas do Department of the Navy (DON) que abordam a utilização das RS (DON, 2014);

- "Social media handbook" do DON (DON, 2012);

- *Blog* de sensibilização no Tumblr (USNMBLOG, [2015]) bem como, a disponibilização de uma apresentação acerca das RS e segurança das operações disponível para *download* (OOI, 2014).

7.4.4.7. U.S. Marine Corps

No *website* oficial são dadas a conhecer outras páginas que os militares, ou qualquer pessoa, podem visitar acerca de:

- Comportamentos que os militares devem ter nas RS (USMC, [2015a]);
- Linhas orientadoras acerca de como os marines podem comentar ou publicar informação não oficial acerca dos Marine Corps nas RS (USMC, [2015b]).

7.4.5. Recomendações

O investigador entende que todo o subcapítulo 7.4.4 pode ser assumido como uma recomendação para a FA no sentido da integração assídua e integral das ações de consciencialização acerca do uso das RS pelos militares da FA. Essas ações podem ter lugar em salas de conferência, na rede interna da FA, no *website* oficial da FA e nas RSFA.

No sentido da criação de políticas, ENISA (2007), faz algumas recomendações, onde se incluem: ações de sensibilização através de campanhas educativas e informação acessível acerca dos perigos das RS; revisão dos regulamentos onde se deverão incluir os diferentes cenários em que as RS podem potenciar perigos; desencorajar a proibição das RS, referindo que estas deverão ser usadas de forma controlada e livremente mas com campanhas que visem educar as pessoas a saberem usar as RS (ENISA, 2007).

7.5. Conclusão Intermédia

As RS são uma mais-valia até certo ponto, tal como refere Valente (2015) na introdução do capítulo 7. Segundo MSimões (2015) no subcapítulo 7.1 e Costa (2015) no subcapítulo 7.4.1, é muito difícil controlar o que os militares publicam nas RS e que, segundo Valente (2015), podem prejudicar as operações tal como podem potenciar. Existem diversos perigos associados ao uso das RS que podem prejudicar as operações, tal como refere ENISA (2007) no subcapítulo 7.1. Para além disso, os militares da FA revelam que estes perigos são reais, face às respostas que deram ao inquérito (ver os Subcapítulos B-5 e B-6 do Anexo B).

Vejamos, no subcapítulo 7.1, vimos que existe uma quantidade significativa de militares (26,7%) que não reconhecem um dos perigos mais acentuados para as OPMIL, o Geotagging (Tabela B-8, Anexo B), resultando num grupo de militares que usaram as RS e o Smartphone em missão não sabendo o que é o Geotagging, constituindo assim 13,9% dos militares que usaram as RS em operações (Tabela B-

9, Anexo B). Ainda no subcapítulo 7.1, vimos que a maior parte dos militares (70%) informou os F/A acerca do local e data da missão (Tabela B-10, Anexo B) e quase metade dos militares (47%) que usaram as RS durante as operações afirmam que os F/A fizeram publicações acerca da missão (Figura B-5, Anexo B). Ainda neste subcapítulo, foi referido que 13,3% dos militares não *briefaram* os F/A (Tabela B-11, Anexo B), o que pode potenciar as quebras de segurança através dos F/A.

No subcapítulo 7.3.1, vimos que a maior parte dos militares que tinham conta nas RS durante as operações não descaraterizaram o perfil (Figura B-4, Anexo B) e uma quantidade significativa de militares (cerca de 30%), durante as operações, fizeram publicações que mencionavam dados confidenciais (Tabela B-7, Anexo B).

No subcapítulo 7.4.2, vimos que nem todos os militares são devidamente *briefados* antes de ingressarem nas missões (Tabela B-12 e Tabela B-13, Anexo B) o que pode potenciar as quebras de segurança, tal como se vê nas relações da Tabela B-15 (Anexo B).

Assim, estamos em condições de validar a seguinte hipótese **"O uso de Redes Sociais durante as missões representa um risco de quebras de segurança, pondo em perigo as Operações Militares"**.

Adiante, Marques (2015) refere no quinto parágrafo do subcapítulo 7.3 que existe a necessidade, na FA, de ser dada a devida sensibilização aos militares acerca das RS. Também Mineiro (2015) refere no subcapítulo 7.3.1 que "ainda não existe consciência de segurança por parte dos militares em missões" e garante facilmente encontramos quebras de segurança perpetuadas pelos militares que estão neste momento em operações (Mineiro, 2015). No subcapítulo 7.4, Mineiro (2015) refere que não são feitas suficientes ações de sensibilização aos militares acerca desta temática e deveria haver uma maior preocupação hierárquica acerca do assunto em causa (Mineiro, 2015). E também segundo a análise do inquérito (ver Anexo B), no subcapítulo 7.4.2, a Tabela B-14 (Anexo B) demonstra que 67,8% militares concordam que deviam ser feitos mais *briefings* acerca das RS e, ainda no mesmo, 63,3% militares concordam que poucos militares dão a devida importância aos *briefings* (Tabela B-14, Anexo B). Face ao exposto e ao referido até agora neste subcapítulo 7.5, estamos em condições de concluir que deveria existir maior preocupação quanto à utilização segura das RS e em consciencializar os militares, pelo que se declara refutada a seguinte hipótese: **"A Força Aérea Portuguesa tem a preocupação**

devida em consciencializar os militares que ingressam nas Operações Militares, acerca do uso das Redes Sociais".

No subcapítulo 7.4.2 refere-se que o RFA 390-6 realça a importância da formação e "inclusão do estudo destas matérias [cibersegurança] em todas as estruturas curriculares e em todos os graus de formação administrados na Força Aérea". No entanto, Marques (2015) e Mineiro (2015), no subcapítulo 7.4.3 não reconhecem a existência de qualquer documento da FA que enquadre os militares para as questões de segurança nas RS. Neste sentido, no subcapítulo 7.4.3.1, Mineiro (2015) acrescenta que nunca tomou conhecimento da existência de uma ORDOP onde se referisse a necessidade de consciencializar os militares para a temática da segurança nas RS. De facto, nesse subcapítulo é mencionada essa inexistência aquando da análise das ORDOPS de 2013 e 2014, bem como de outros documentos ou apresentações mencionados nos subcapítulos 7.4.3.2, 7.4.3.3 e 7.4.3.4.

A publicação do RFA 390-6 é novamente abordada no subcapítulo 7.4.3.5, onde se refere que o conteúdo da mesma assenta sobre os perigos da Internet e das RS. No entanto, este documento não está facilmente acessível a qualquer militar da FA tal como se refere no subcapítulo 7.4.3.5 nem é do conhecimento de todos os militares (Subcapítulo 7.4).

Assim, estamos em condições de validar a seguinte hipótese **"Não está divulgada na Força Aérea Portuguesa informação sobre os perigos do uso das Redes Sociais".**

Página intencionalmente deixada em branco

8. Conclusão e Recomendações

Neste capítulo é feita uma conclusão do estudo realizado. Essa conclusão resulta de uma análise e interligação de todas as conclusões intermédias a que o investigador chegou ao longo do trabalho. Será obtida resposta para as questões derivadas e por último à pergunta central de toda a dissertação, a questão de partida. Por fim são também propostas algumas recomendações para trabalhos futuros.

8.1. Conclusão

Esta dissertação pretende dar a conhecer ao leitor a atualidade da FA face às novas plataformas que gerem hoje a maior parte dos contactos entre as pessoas, as RS. É um trabalho de investigação que aprofunda o universo das RS, centrando o interesse nas capacidades e potencialidades das mesmas no contexto das OPMIL da FA. O investigador propôs-se a elaborar um inquérito destinado aos militares da FA que já participaram em missões internacionais tendo obtido uma amostra de 90 militares. Foram ainda efetuadas 8 entrevistas com diferentes objetivos, destinadas a militares conhecedores das matérias em questão. Para além dessas entrevistas, vários militares foram abordados para a temática e puderam partilhar os seus conhecimentos, esclarecendo o autor acerca de diversas áreas: como são usadas as RS em missão e com que objetivos, que falhas de segurança são notadas durante as missões ao nível das RS, como vivem os militares numa operação militar no estrangeiro e que fontes de motivação encontram, que literatura existe na FA acerca das RS e que outras bibliografias são aconselhadas para o estudo em causa (onde se destaca o Sub-Registo da FA, sediado no Estado-Maior da FA).

O trabalho foi estruturado por diversos capítulos e subcapítulos onde se destacam: Introdução, Revisão da Literatura, Análise e Conclusões.

Na introdução o investigador pretende enquadrar o leitor para o restante estudo e dá a conhecer o fio condutor pela qual a dissertação se guia apresentando as questões nas quais se sustenta e os pressupostos assumidos, na forma de hipóteses de trabalho, que pretendem ver-se validados ou refutados, podendo assim responder no presente capítulo às questões derivadas.

Na Revisão da Literatura, o autor compõe os tecidos que enformam a investigação e que permitem ao leitor perceber o contexto em que a temática se insere.

A análise incide sobre os capítulos três, quatro, cinco, seis e sete. No capítulo 3 são dadas a conhecer as RS abordadas nos capítulos 4 e 6. No capítulo 4 são demonstradas as potencialidades das RS, nomeadamente para a obtenção de SA em várias causas: apoio à população, causas humanitárias, controlo epidémico, causas políticas e sociais, culminando nas OPMIL. É estudada a importância do SA, de que forma se pode ganhar esse SA e que ferramentas se podem utilizar. São também dados a conhecer alguns relatos de militares da FA que experimentaram as capacidades das RS para o ganho de SA.

No capítulo 5 são estudadas as RS como uma ferramenta de motivação para os militares que se encontram em missões no estrangeiro, onde se cruzam as entrevistas com os inquéritos realizados. No capítulo 6 pretende-se concluir se as RSFA permitem influenciar a OP, favorecendo a imagem da FA e das operações, onde mais uma vez são tratadas as entrevistas e inquéritos. No último capítulo da análise, o capítulo 7, pretende-se demonstrar o lado negativo das RS para as operações, passando estas a serem encaradas como uma "faca de dois gumes", no sentido de que, se a FA não souber gerir as novas tendências dos militares, nomeadamente a utilização das RS em OPMIL, poderão surgir resultados negativos.

Na sequência desta análise, foram alcançadas várias conclusões.

<u>As RS como fonte de aquisição de SA:</u>

- A aquisição de SA através das RS é feita em vários campos e traz vantagens significativas (capítulo 4);
- Esse SA pode permitir uma melhor gestão de esforços por parte dos comandantes (subcapítulo 4.6);
- As RS permitem a recolha de INTEL no contexto das OPMIL subcapítulo 4.6);
- O SA proveniente das RS é uma garantia de segurança pessoal e operacional para os militares em operações no estrangeiro (subcapítulo 4.6).

<u>As RS como objeto de motivação e moral (principalmente capítulo 5):</u>

- Existe preocupação hierárquica[29] com a motivação dos militares (capítulo 5 e subcapítulo 7.4.3.1);

[29] Tal como referido anteriormente (subcapítulo 7.4), por preocupação hierárquica entende-se como a preocupação das hierarquias competentes para criação das Ordens de Operações e outros documentos que devam refletir a adequada integração das RS nas OPMIL.

- As RS, em específico, não são uma preocupação hierárquica para a motivação dos militares (subcapítulo 7.4.3.1);
- As RS permitem “encurtar” distâncias entre os militares e os familiares;
- A maior parte dos militares da FA que participaram em OPMIL, usaram as RS para falar com os familiares e quase 50% usou as RS todos os dias;
- A maior parte dos militares inquiridos (69%) concordam que as RS são uma fonte de motivação;
- Todos os entrevistados que participaram em OPMIL concordam que as RS são motivadoras.

<u>As RS como uma ferramenta de influência da OP:</u>

- Se não existir uma relação de “cumplicidade profissional” entre a FA e a comunicação social, poderão surgir notícias que prejudiquem as operações e a imagem da FA (subcapítulo 6.1);
- A utilização das RS pela FA é importante para “informar, divulgar e instruir” o público (subcapítulo 6.4);
- Se a FA não tiver uma presença nas RS não consegue monitorizar e responder às notícias veiculadas nas RS (subcapítulo 6.4);
- A presença da FA nas RS fortalece a relação com as pessoas (subcapítulo 6.4);
- As RS permitem “influenciar” a OP nacional e internacional (subcapítulo 6.4);
- Os militares sentem orgulho nas publicações das RSFA e partilham as mesmas nas suas páginas pessoais, o que promove a imagem da FA à OP (subcapítulo 6.4);
- Para além de influenciar a OP positivamente, as publicações da FA aumentam a moral dos militares, o que os leva a partilhar essas publicações, e que, por sua vez ajuda a potenciar a imagem da FA (subcapítulo 6.4).

<u>Quebras de Segurança nas RS:</u>

- Devido à proliferação das tecnologias de comunicação, nomeadamente os *Smartphones*, as RS são um perigo inevitável para as OPMIL, na medida em que, não existem vantagens em proibir somente os acessos às RS pelos computadores disponibilizados para as operações (subcapítulo 7.1);
- Existe uma forte necessidade dos militares da FA serem instruídos para o uso correto das RS, caso contrário, poderão ocorrer quebras de segurança em futuras

OPMIL da FA (subcapítulo 7.1), com resultados negativos para os militares, familiares e operações (subcapítulo 7.2);

- Existe necessidade de criar doutrinas e políticas que regulamentem a utilização das RS pelos militares da FA (subcapítulo 7.3);
- A consciência atual por parte dos militares da FA acerca da utilização segura das RS, pode fazer perigar as operações por não estarem tão bem consciencializados quanto deveriam (subcapítulos 7.3.1 e 7.4.2);
- Não existe na FA literatura acerca das RS que seja facilmente acessível e onde os militares se possam socorrer em caso de dúvidas ou simplesmente aprender como usar correta e eficazmente as mesmas (subcapítulo 7.4.3);
- Os EUA têm imensa sensibilização pública e facilmente acessível a qualquer pessoa, onde abordam questões como: quebras de segurança em operações, uso das RS para liderança, uso das RS pelos familiares, uso das RS pelos militares, perigos das RS, ferramentas úteis das RS, entre outros temas relacionados (subcapítulo 7.4.4).

Com base nas conclusões intermédias referidas em cima, vejamos agora os pressupostos definidos inicialmente (subcapítulo 1.3):

Hipótese 1 – "O uso das Redes Sociais nas missões, permite capacitar os militares com um melhor *Situational Awareness"*;

Hipótese 2.1 – "O uso das Redes Sociais pelos militares é um fator de motivação durante as Operações Militares";

Hipótese 2.2 – "O uso efetivo das Redes Sociais da Força Aérea Portuguesa para divulgar as missões motiva e moraliza os militares destacados e contribui para a tranquilidade das suas famílias";

Hipótese 3 – "O uso das Redes Sociais, de forma individual e institucional, para potenciar a imagem da Força Aérea Portuguesa, influencia positivamente a Opinião Pública acerca das Operações Militares";

Hipótese 4.1 – "O uso de Redes Sociais durante as missões representa um risco de quebras de segurança, pondo em perigo as Operações Militares";

Hipótese 4.2 – "A Força Aérea Portuguesa tem a preocupação devida em consciencializar os militares que ingressam nas Operações Militares, acerca do uso das Redes Sociais";

Hipótese 4.3 – “Não está divulgada na Força Aérea Portuguesa informação sobre os perigos do uso das Redes Sociais”.

À luz das conclusões intermédias obtidas e tendo em conta os pressupostos colocados, é possível responder às questões derivadas definidas inicialmente:

–Q1. “O uso de Redes Sociais em Operações Militares permite capacitar os militares com um melhor *Situational Awareness*?".

As RS com todas as ferramentas que contemplam (capítulo 3 e capítulo 4.6), aliadas à vontade que as pessoas têm de interagir com as mesmas (subcapítulo 4.1), torna-as uma fonte de informação e de SA para duas partes: para as operações, em forma de INTEL acerca do cenário das operações, do ambiente e do adversário (Subcapítulo 4.6); e para a segurança pessoal dos militares envolvidos, pois conseguem recolher informações atuais, diariamente, acerca das condições de segurança que se vivem nos locais vizinhos (Subcapítulo 4.6). Assim, as entrevistas aliadas à pesquisa bibliográfica, permitem concluir que a resposta é afirmativa.

–Q2. “As Redes Sociais são plataformas potenciadoras da motivação dos militares envolvidos em Operações Militares?".

A participação nas RS por parte dos militares que participam em OPMIL internacionais, é um forte contributo para as OPMIL porque os militares encontram motivação no uso das RS, nomeadamente para contactarem com os familiares e amigos. Esse contacto, bem como as publicações da FA permitem tranquilizar os familiares. Estas conclusões foram obtidas com base nas entrevistas e na análise dos inquéritos espelhados no subcapítulo 5.1. Assim, a resposta à Q2 é afirmativa.

–Q3. "A utilização das Redes Sociais no contexto das Operações Militares tem influência na Opinião Pública?".

As RS usadas pela FA ou particularmente pelos militares da FA, permitem potenciar a imagem institucional e das operações, divulgar, informar e instruir o público e dessa forma influenciar positivamente a OP, quer seja em Portugal, quer seja em OPMIL no estrangeiro (subcapítulo 6.4). Aliás, a falta de utilização e presença nas RS pode prejudicar a OP (subcapítulos 6.1, 6.2 e 6.3). A resposta dá-se então como afirmativa.

–Q4. “O uso de Redes Sociais incrementa o risco das quebras de segurança no âmbito da atividade militar?".

No subcapítulo 7.1 e 7.2 foi demonstrada a existência de perigos associados às RS para as OPMIL da FA, provando-se através da análise dos inquéritos, que os militares da FA e os respetivos familiares e amigos, representam um risco para as quebras de segurança (subcapítulo 7.1 e 7.4.1). Outros elementos relacionados com as RS que também incrementam o risco das quebras de segurança no âmbito da atividade militar são: a falta de briefings, demonstrado pelas entrevistas e inquéritos (subcapítulo 7.4.2); a falta de consciência dos militares em relação aos cuidados a ter com as RS (subcapítulos 7.1 e 7.3.1); a falta de literatura suficiente (subcapítulo 7.4.3) e a falta de ações de sensibilização suficientes acerca das RS (subcapítulo 7.4.2) o que pode traduzir na falta de consciência dos militares. Assim, a análise dos inquéritos, das entrevistas e documentos bibliográficos, permitiu aferir que existe risco de quebras de segurança essencialmente em duas partes: dos militares que ingressam nas missões e dos familiares e amigos. O que pode fazer perigar várias partes: os próprios militares; os familiares e amigos; e as OPMIL. A resposta à pergunta é afirmativa, o uso das RS incrementa o risco de quebras de segurança no âmbito da atividade militar, tal como contemplado nos subcapítulos mencionados.

Surge assim a resposta à questão de partida a partir de toda a argumentação apresentada nesta dissertação, e em particular no articulado apresentado neste capítulo que resume essa mesma argumentação:

“As Operações Militares da Força Aérea Portuguesa são potenciadas pelo uso das Redes Sociais?”

Todo o trabalho desenvolvido permitiu responder às questões derivadas que se definiram inicialmente. Essas respostas permitem agora concluir a questão principal do trabalho.

Face à Q1, vimos que as RS são uma fonte de informação e de SA para as operações e para os militares no uso particular. Concluiu-se que “O uso de Redes Sociais em Operações Militares permite capacitar os militares com um melhor *Situational Awareness*”.

Na Q2, constatámos que é vantajoso para as operações, disponibilizar aos militares as RS como uma fonte de motivação. Neste sentido, “As Redes Sociais são plataformas potenciadoras da motivação dos militares envolvidos em Operações Militares”.

Na questão seguinte, a Q3, foi concluído que deve haver uma presença da instituição e dos militares nas RS e existem duas formas de influenciar a OP: através dos militares no uso particular e através RS usadas pelas FA; e que, se as RS forem usadas por ambos com o intuito de potenciar a imagem da FA e das operações, então nesse caso "A utilização das Redes Sociais no contexto das Operações Militares tem influência na Opinião Pública" de forma positiva.

Por último, na questão Q4, foram apresentados alguns perigos inerentes ao uso das RS, que podem prejudicar as operações e provou-se que esses perigos existem e podem ocorrer nas operações da FA, comprometendo as mesmas. Também se revelou que existe falta de consciência dos militares em relação aos perigos e que, relacionado ou não com isso, constatou-se que não existe literatura facilmente acessível acerca dos cuidados a ter nas RS. Desta forma, conclui-se que "O uso de Redes Sociais incrementa o risco das quebras de segurança no âmbito da atividade militar" da FA.

Face às conclusões obtidas, podemos agora responder à questão de partida. As RS potenciam as OPMIL, se forem exploradas as suas capacidades e se a FA tiver em conta que existe o perigo iminente de quebras de segurança por parte dos militares, quer as RS estejam autorizadas durante a operação ou não. Assim, se existir a adequada consciencialização de todos os militares, a FA pode retirar muito proveito das mesmas para as OPMIL.

Conclui-se que "**As Operações Militares da Força Aérea Portuguesa são potenciadas pelo uso das Redes Sociais".**

8.2. Considerações Finais

Esta dissertação de mestrado foi desenvolvida para sensibilizar e consciencializar o leitor para as capacidades e potencialidades das RS em diversos âmbitos, mas dando especial destaque ao âmbito das OPMIL, que no fundo é o âmago desta dissertação. Não só sensibilizar e consciencializar o leitor mas também "quem de direito" na FA para que sejam tomadas medidas que permitam aproveitar as capacidades das RS em prol da instituição militar e dos seus militares bem como minimizar o risco de quebras de segurança.

Assim, e face às conclusões retiradas, recomenda-se o seguinte:

- As RS contêm muito ruído de informação, mas ainda assim, uma pequena equipa com expertise nestes ambientes de informação consegue adquirir informações

fidedignas que potenciam o SA para as operações. Neste sentido, as OPMIL são potenciadas pelo uso das RS pelo que deve ser ponderado o seu uso oficial em missões militares;

- As RS permitem motivar os militares em contexto operacional que, por estarem longe dos familiares, sentem maior necessidade de se envolverem nas RS. Este incremento de motivação torna-os mais empenhados no cumprimento das funções. Neste sentido, as OPMIL são potenciadas pelo uso das RS. Face ao expendido as RS devem ser utilizadas nas operações;

- A consciencialização devida de todos os militares da FA para os comportamentos a adotar nas RS, pode melhorar a OP acerca da FA. Mais, a utilização das capacidades de disseminação de informação das RS para impulsionar a imagem e missão da FA, pode influenciar positivamente a OP nacional e internacional (no local onde as OPMIL da FA têm lugar). O apoio da OP aumenta a moral dos militares e influencia positivamente o decorrer das operações. Neste sentido, as OPMIL são potenciadas pelo uso das RS pelo que as mesmas devem ser utilizadas no decurso das missões;

- Mas, as RS não trazem apenas potencialidades para as OPMIL. Incrementam um sério risco de quebras de segurança, que por vezes nem os próprios "infratores" reconhecem quando podem estar a perigar as operações. Neste sentido, as OPMIL podem ser comprometidas pelo uso das RS. Assim, devem ser criados mecanismos de auxílio à publicação por parte dos militares.

8.3. Recomendações e Contribuições Futuras

Apesar do trabalho desenvolvido mencionar algumas recomendações à FA, "no sentido da integração assídua e integral das ações de consciencialização acerca do uso das RS pelos militares da FA" (subcapítulo 7.4.5), o investigador entende que esta é uma questão que merece especial atenção e que pode ser vertida numa dissertação de mestrado onde se explorem:

- O grau de perigo que os militares da FA podem representar para as operações (testando as ações dos militares face a determinado tipo de situações nas RS que podem comprometer as operações sem que os mesmos se apercebam);
- A qualidade dos briefings ministrados noutros países e na FA acerca das RS;
- Quais os tópicos mais importantes a serem abordados num briefing deste tipo e fazer um modelo para um briefing sobre as RS com base nas aprendizagens.

9. Referências Bibliográficas

ADAY, Sean - Social Media, Diplomacy, and the Responsibility to Protect. [Em linha]. Take Five, 2012. [Consult. 18 Jan. 2015]. Disponível em WWW: <URL: http://takefiveblog.org/2012/10/17/social-media-diplomacy-and-the-responsibility-to-protect/>.

ADAY, Sean [et al] – Blogs and Bullets II: New Media and Conflict after the Arab Spring. [Em linha]. U.S. Institute of Peace, 2012. [Consult. 18 Jan. 2015]. Disponível em WWW: <URL: http://www.usip.org/publications/blogs-and-bullets-ii-new-media-and-conflict-after-the-arab-spring>.

AIR FORCE PUBLIC AFFAIRS AGENCY (AFPAA) – Air Force Social Media Guide. 4.ª ed. Texas: U.S. Air Force, 2013.

ALBERTS, David [et al.] - Understanding Information Warfare. Estados Unidos da América: CCRP Publication Series, 2001.

ALI, Sadaf R.; FAHMY, Shahira - Gatekeeping and citizen journalism: The use of social media during the recente uprisings in Iran, Egypt, and Libya. In Media, War & Conflict. Vol. 6, (2013), p. 55-69.

AMERICAN RED CROSS (ARC) - Press Release: Web Users Increasingly Rely on Social Media to Seek Help in a Disaster. [Em linha]. 2010. [Consult. 08 Dez. 2014]. Disponível em WWW: <URL: http://newsroom.redcross.org/2010/08/09/press-release-web-users-increasingly-rely-on-social-media-to-seek-help-in-a-disaster/>.

AMMUNITION - Darcy DiNucci. [Em linha]. California: ammunition, [2007]. [Consult. 10 Jan. 2015]. Disponível em WWW: <URL: http://www.ammunitiongroup.com/about/darcy-dinucci/>.

ANONYMOUS PORTUGAL – Quem Vai Pagar A Festa Da Mãe Do Coronel?!. [Lista em linha]. Facebook, 2013. [Consult. 31 Jan. 2015]. Disponível em WWW:<URL: https://www.facebook.com/AnonymousPORTUGAL/posts/525228340833458>.

AZADI, Neda – HBO The True Story of Neda Agha-Soltan ايران سلطان آقا ندا زندگي English (1) [A história de Neda Agha-Soltan]. [Em linha]. YouTube, 2010. [Consult. 18

Jan. 2015]. Disponível em WWW: <URL: https://www.youtube.com/watch?v=mYN53BOeijY>.

BAILLIE, Amber - Communication is about relationships, says Lt. Gen. Johnson at media forum. [Em linha]. Colorado: U.S. Air Force Academy, 2014. [Consult. 13 Nov. 2014]. Disponível em WWW: <URL: http://www.usafa.af.mil/news/story_print.asp?id=123404363>.

BARNES, Julian E.– U.S. Military Plugs Into Social Media for Intelligence Gathering: Defense Intelligence Agency Head Says Online Postings Played Crucial Role in Ukraine Jet Shootdown Investigation. [Em linha]. Washington: The Wall Street Journal, 2014. [Consult. 05 Jan. 2015]. Disponível em WWW:<URL: http://www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557>.

BBC NEWS - Muslim cartoon row timeline [Em linha]. BBC News, 2006, actual. 19 Fev. 2006. [Consult. 24 Out. 2014]. Disponível em WWW: <URL: http://news.bbc.co.uk/2/hi/middle_east/4688602.stm>.

BBC NEWS - Charlie Hebdo attack: Three days of terror [Em linha]. BBC News, 2015, actual. 14 Jan. 2015. [Consult. 15 Jan. 2015]. Disponível em WWW: <URL: http://www.bbc.com/news/world-europe-30708237>.

BEAL, Vangie - Twitter Dictionary: A Guide to Understanding Twitter Lingo [Em linha]. California: Webopedia, 2010, actual. 26 Ago. 2014. [Consult. 07 Jan. 2015]. Disponível em WWW: <URL: http://www.webopedia.com/quick_ref/Twitter_Dictionary_Guide.asp>.

BEAL, Vangie – Technology Hashtags: Webopedia's Twitter Guide to Technology Topics [Em linha]. California: Webopedia, 2013, actual. 09 Mai. 2013. [Consult. 07 Jan. 2015]. Disponível em WWW: <URL: http://www.webopedia.com/quick_ref/twitter-hashtags-for-technology-topics.html>.

BEIZER, Doug - Military uses social media to share info on Fort Hood shootings, 2009. [Em linha]. Virginia: GCN, 2009. [Consult. 12 Jan. 2015]. Disponível em WWW: <URL: http://gcn.com/articles/2009/11/06/fort-hood-social-media.aspx>.

BERNAYS, Edward L. – Propaganda. 1928

BOWER, Eve [et al] – Ahmadinejad hails election as protests grow. [Em linha]. Tehran: CNN, 2009. [Consult. 18 Jan. 2015]. Disponível em WWW:<URL: http://edition.cnn.com/2009/WORLD/meast/06/13/iran.election/>.

BOYD, Danah M.; ELLISON, Nicole B. - Social Network Sites: Definition, History, and Scholarship. [S.l.]: [s.n.], 2007.

BUREAU OF DIPLOMATIC SECURITY (BDS) – Social Networking Cyber Security Awareness Briefing. [Em linha]. USA: Department of Defense, 2010. [Consult. 10 Dez. 2014]. Disponível em WWW:<URL: http://www.slideshare.net/DepartmentofDefense/social-media-cyber-security-awareness-briefing/>.

BURN-MURDOCH, John [et al] - Twitter traffic during the riots [Em linha]. London: The Guardian, 2011. [Consult. 09 Set. 2014]. Disponível em WWW:<URL: http://www.theguardian.com/uk/interactive/2011/aug/24/riots-twitter-traffic-interactive>.

CARRERA, Filipe – Marketing Digital na versão 2.0. Lisboa: Edições Sílabo, 2009.

CASTELLS, Manuel O. - The Rise of the Network Society. In The Information Age: Economy, Society and Culture. Cambridge, 2000. vol. 1.

CASTELLS, Manuel O. - The Power of Identity. In The Information Age: Economy, Society and Culture. Cambridge, 2004. vol. 2.

CHEFE DO ESTADO-MAIOR – Diretiva N.º 06/09: Utilização de Equipamentos de Tecnologias da Informação e Comunicações em Áreas de Segurança de Classe 1. Lisboa: EMFA, 2009.

CHRISTENSSON, Per – IM [Instant Message ou Mensagens Instantâneas]. [Em linha]. TechTerms, actual. 01 Jul. 2007. [Consult. 02 Fev. 2015]. Disponível em WWW: <URL: http://techterms.com/definition/im>.

CHRISTENSSON, Per – ICT [Tecnologias de Informação e Comunicações (TIC)]. [Em linha]. TechTerms, actual. 04 Jan. 2010. [Consult. 02 Fev. 2015]. Disponível em WWW: <URL: http://techterms.com/definition/ict>.

CHRISTENSSON, Per – VoIP [Voice Over Internet Protocol]. [Em linha]. TechTerms, [2015]. [Consult. 02 Fev. 2015]. Disponível em WWW:<URL: http://techterms.com/definition/voip>.

CLAUSEWITZ, Carl Von - On War. [s.l.]: Project Gutenberg, 2006.

CNN LIBRARY - 2011 Japan Earthquake - Tsunami Fast Facts. [Em linha]. London: CNN, actual. 11 Jul. 2014. [Consult. 10 Out. 2014]. Disponível em WWW:<URL: http://edition.cnn.com/2013/07/17/world/asia/japan-earthquake---tsunami-fast-facts/>.

COMANDO AÉREO – Diretiva Operacional Nº03/CA/2012: Comemorações do 60º Aniversário da Força Aérea. Ministério da Defesa Nacional, Força Aérea, 2012.

COMANDO AÉREO – ORDOPS CA 008/13: FRONTEX – Participação do C-295M na Joint Operation "POSEIDON SEA" 2013. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 010/13: FRONTEX – Participação do C-295M na Joint Operation "HERMES" 2013. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 011/13: Visita de SExa. O PR às Ilhas Selvagens - Madeira. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 012/13: Exercício BRILLIANT ARROW 2013; Certificação F-16M NRF2014. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 013/13: FRONTEX – Participação do C-295M na Joint Operation "INDALO" 2013. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 014/13: Early Operational Assessment – EOA; OFP M6.5. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 016/13: FRONTEX – Participação do C-295M na Joint Operation "HERMES II" 2013. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 017/13: Participação do P-3C CUP+ No Exercício "STEADFAST JAZZ 2013". Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 018/13: Destacamento de F-16M na BA4: 05NOV-12NOV2013. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 020/13: FRONTEX – Participação do C-295M na "JO HERMES 2013 – EXT JAN2014". Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – ORDOPS CA 021/13: Tactical Leadership Programme: TLP2014. Ministério da Defesa Nacional, Força Aérea, 2013.

COMANDO AÉREO – NEP/OPS-028: Destacamentos da Força Aérea. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 001/14: Destacamento de F-16M BA4 10MAR-14MAR2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 003/14: Exercício FRISIAN FLAG 2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 005/14: Curso FIGHTER WEAPONS INSTRUCTOR TRAINING: FWIT14. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 006/14: Destacamento P-3C CUP+: São Tomé e Príncipe e Cabo Verde; âmbito do exercício e acordos de cooperação bilateral . Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 008/14: FRONTEX – Participação do C-295M na "JO AENEAS/HERMES 2014". Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 010/14: Exposição estática que comemora o 62ºAniversário da Força Aérea inserida nas comemorações do centenário da aviação militar. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 011/14: Destacamento de ALPHA JET na BA4: 30JUL-06AGO2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 014/14: Air Race Championship (ARC): centenário da aviação militar. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 015/14: Baltics Air Policing 2014: BAP14 (Reservado). Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 016/14: Destacamento do Alouette III em Penamacor: 05-07 Ago2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 019/14: Readiness Response Plan 019/14: Activation and movement plan for NRF2015: PRT AF 1xP-3C (01 January to 31 December 2015) (Reservado). Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 022/14: Baltics Immediate Assurance Measures 2014: BAP IAM 14; P-3C CUP+ (Reservado). Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 023/14: Destacamento do Alouette III em Penamacor: 04-07 Nov2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 023/14: Destacamento do Alouette III em Tavira: 24-27 Nov2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO AÉREO – ORDOPS CA 024/14: Destacamento do Alouette III em Penamacor: 04-07 Nov2014. Ministério da Defesa Nacional, Força Aérea, 2014.

COMANDO OPERACIONAL – NEP/OPS-005: Transporte de altas entidades (VIP's) em Aeronaves da FAP. Ministério da Defesa Nacional, Força Aérea, 1994.

CRUZ, Rui – Coronel da Força Aérea faz jantar de aniversário da mãe na Base Aérea de Beja. [Em linha]. TugaLeaks, 2013. [Consult. 31 Jan. 2015]. Disponível em WWW:<URL: http://www.tugaleaks.com/coronel-base-aerea-beja.html>.

DAWSON, Douglas; HILL, Steven; BANK, Ryan – Use Social Media for Crises. U.S. Naval Institute Proceedings. Vol. 139, Nº10 (2013), p. 77-81.

DEPARTMENT OF THE AIR FORCE (DOTAF) - Cornerstones of Information Warfare. Washington: Department of the Air Force, 1995

DEPARTMENT OF THE AIR FORCE (DOTAF) – Air Force Instruction 10-701: Operations Security (OPSEC). USA: Department of the Air Force, 2011. p. 40.

DEPARTMENT OF THE ARMY – FM 100-6: Information Operations. Washington, DC: Headquarters, Department of the Army, 1996.

DEPARTMENT OF THE NAVY (DON) – Navy Command Leadership: Social Media Handbook. [Em linha]. Washington, DC: Department of the Navy, 2012. [Consult. 19 Jan. 2015]. Disponível em WWW: <URL: http://www.navy.mil/CommandDirectory.asp>.

DEPARTMENT OF THE NAVY (DON) – Department of the Navy Public Affairs Policy and Regulations. [Em linha]. Washington, DC: Department of the Navy, 2014. [Consult. 19 Jan. 2015]. Disponível em WWW: <URL: http://www.navy.mil/CommandDirectory.asp>.

DEPARTMENT OF THE NAVY (DON) – Social Media Best Practices. [Em linha]. Washington, DC: Department of the Navy, [2015]. [Consult. 19 Jan. 2015]. Disponível em WWW: <URL: http://www.navy.mil/CommandDirectory.asp>.

DIANA, Alison – Air Force Seeks Fake Online Social Media Identities. [Em linha]. The InformationWeek, DarkReading, 2011. [Consult. 19 Jan. 2015]. Disponível em WWW: <URL: http://www.darkreading.com/risk-management/air-force-seeks-fake-online-social-media-identities/d/d-id/1096228?>.

DINIS, José António Henriques - A Guerra de Informação: Perspectivas de Segurança e Competitividade. [Em linha]. Revista Militar, 2004. [Consult. 07 Set. 2014]. Disponível em WWW: <URL: http://www.revistamilitar.pt/artigo.php?art_id=410>.

DINUCCI, Darcy – Fragmented Future. In Design & New Media. Print Magazine, Vol. 53, Nº4 (1999), p. 32-222.

DIVCSI – RFA 390-6: Política de ciberdefesa da Força Aérea. Ministério da Defesa Nacional, Força Aérea, 2011.

European Network and Information Security Agency (ENISA) - Security Issues and Recommendations for Online Social Networks. Grécia: Giles Hogben, ENISA, 2007.

European Network and Information Security Agency (ENISA) – Social Engineering: Exploiting the Weakest Links**.** ENISA, 2008.

FA - Missão. [Em linha]. FA - DCSI, [2015]. [Consult. 14 Jan. 2015]. Disponível em WWW: <URL: http://www.emfa.pt/www/pagina-001>.

FEDERAL BUREAU OF INVESTIGATION (FBI) – Internet Social Networking Risks. [Em linha]. USA: U.S. Department of Justice, [2015]. [Consult. 02 Fev. 2015]. Disponível em WWW: <URL: http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks>.

GHYS, Étienne, ed lit. – The butterfly effect. Seoul: [s.n.], 2012

GOOLSBY, Rebecca - Social media as crisis platform: The future of community maps/crisis maps. In ACM Transactions on Intelligent Systems and Technology. ISSN 2157-6904. Vol. 1, Nº7 (2010)

GRUNIG, J.E.; HUNT T. - Managing Public Relations**,** New York: Holt, Rinehart & Winston, 1984.

HA, Tu Thanh; SLATER, Joanna - What is Charlie Hebdo and why was it a target? [Em linha]. The Globe And Mail, 2015, actual. 08 Jan. 2015. [Consult. 10 Jan. 2015]. Disponível em WWW: <URL: http://www.theglobeandmail.com/news/world/magazine-attacked-in-paris-skirted-controversy-with-cartoons-of-prophet/article22330111/?cmpid=rss1&click=sf_globe>.

HAENI, Reto – Information Warfare an Introduction. Washington DC, 1997.

HUMAN RIGHTS WATCH - Libya: 10 Protesters Apparently Executed. [Em linha]. The Thomson Reuters Foundation, 2011. [Consult. 18 Jan. 2015]. Disponível em WWW: <URL: http://www.trust.org/item/?map=libya-10-protesters-apparently-executed >.

INTERNET LIVE STATS (ILS) - Internet Users [Em linha]. Internet Live Stats, [2015]. [Consult. 01 Jan. 2015]. Disponível em WWW:<URL: http://www.internetlivestats.com/internet-users/>.

JENSEN, Rikke B. [et al.] – Soldiers on social media. [Em linha]. Phys.org, 2014. [Consult. 05 Jan. 2015]. Disponível em WWW:<URL: http://phys.org/news/2014-08-soldiers-social-media.html>.

JESSOP, Brent – Full Spectrum Information Warfare: Inofrmation Operation Roadmap Part 1. USA: Department of Defense, 2007

JOWETT, Garth S.; O'DONNELL, Victoria - Propaganda and Persuasion. 2ª ed. California: Sage, 1992.

JP 1 – Doctrine for the Armed Forces of the United States. USA: Chairman of the Joint Chiefs of Staff (Joint Publication 1, 14 Maio 2007), 2007.

JP 1-02 - Dictionary of Military and Associated Terms**.** USA: Chairman of the Joint Chiefs of Staff (Joint Publication 1-02, 8 Novembro 2010), 2010

JP 2-0 – Joint Intellinge. USA: Chairman of the Joint Chiefs of Staff (Joint Publication 2-0, 22 June 2007), 2007.

JP 3-13 – Information Operations. USA: Chairman of the Joint Chiefs of Staff (Joint Publication 3-13, 27 Novembro 2012), 2012.

KASE, Sue E. [et al] – Exploiting Social Media for Army Operations: Syrian Civil War Use Case. Aberdeen Proving Ground: Army Research Laboratory, 2014, Vol. 9122 (ARL-RP-0489)

KELLEHER, Tom A. - Public Relations Online: Lasting Concepts for Changing Media. California: Sage Publications, 2007. ISBN 1-4129-1417-5.

KENNEDY, Helen; MOORE, Robert F. - Horror at Fort Hood: Gunman Nidal Malik Hasan kills 13, wounds 31 in rampage on Texas Army base. [Em linha]. Daily News, 2009, actual. 06 Nov. 2009. [Consult. 20 Jan. 2015]. Disponível em WWW:<URL: http://www.nydailynews.com/news/national/horror-fort-hood-gunman-nidal-malik-hasan-kills-13-wounds-31-rampage-texas-army-base-article-1.414217>.

KOPP, Carlo - NCW 101: an introduction to network centric warfare**.** 1ª ed. Austrália: Air Power Australia, 2008. ISBN 9780980550603.

LAMPREIA, J. Martins – Técnicas de comunicação: publicidade, propaganda e relações públicas. 7.ª ed.. Mem Martins: Publicações Europa-América, Lda.,1996.

LAUDON, Kenneth C.; LAUDON, Jane P. – Sistemas de informação: com Internet. 4ª ed. Rio de Janeiro: LTC Editora, 1999. p.389.

LINDSAY, Bruce R. – Social Media and Disasters: Current Uses, Future Options, and Policy Considerations. Washington, DC: Congressional Research Service, 2011. (CRS Report R41987).

LISBOA, Indignados – O parasitismo de uma casta dita superior, a casta militar acima da "sociedade civil". [Lista em linha]. Facebook, 2013. [Consult. 31 Jan. 2015]. Disponível em WWW:<URL: https://www.facebook.com/IndignadosLisboa/posts/212940555510948>.

LORENZ, Edward N., ed lit. – Predictability; Does the flap of a butterfly's wings in brazil set off a tornado in Texas? Massachusetts: Institute of Technology Cambridge, 1972

MAYFIELD, Thomas D. - A Commander's Strategy for Social Media**.** USA: U.S. Army, 2011.

MCCLAIN, John– 3 Cool Twitter & Google Maps Mashups You Should Check Out. [Em linha]. makeuseof, 2010. [Consult. 16 Jan. 2015]. Disponível em WWW:<URL: http://www.makeuseof.com/tag/3-cool-twitter-google-maps-mashups-check/>.

MINISTRY OF DEFENCE (MOD) – Defence and armed forces – guidance: Think before you share online. [Em linha]. U.K: Ministry of Defence, 2013. [Consult. 02 Fev. 2015]. Disponível em WWW:<URL: https://www.gov.uk/think-before-you-share>.

MONTEIRO, Mília; BARBOSA, Rafael – Militares cumprem missão em resort de Cabo Verde. [Em linha]. Jornal de Notícias, 2012. [Consult. 23 Jan. 2015]. Disponível em WWW:<URL: http://www.jn.pt/PaginaInicial/Politica/Interior.aspx?content_id=2470634&page=-1>.

NATIONAL SECURITY AGENCY (NSA) - Social Networking Sites. [Em linha]. Systems and Network Analysis Center, [2009]. [Consult. 15 Out. 2014]. Disponível em WWW: <URL: https://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf>.

NATO – Enclosure “B”: Basic Principles and Minimum Standards of Security. NATO, 2010.

NATO – What is NATO?. [Em linha]. [2015]. [Consult. 23 Jan. 2015]. Disponível em WWW: <URL: http://www.nato.int/nato-welcome/index.html>.

NORTH ATLANTIC MILITARY COMMITTEE - MC 422/1: NATO Military Policy on Information Operations. 2002.

NORTH ATLANTIC MILITARY COMMITTEE - MC 422/4: NATO Military Policy on Information Operations. 2012.

NUNES, Pedro Filipe Taveira Seixas - A imagem da Força Aérea Portuguesa no contexto de Operações Baseadas em Efeitos; É possível beneficiar, a nível organizacional, com o uso da imagem da Força Aérea Portuguesa transmitida pela comunicação social? Sintra: Academia da Força Aérea. 2012. Dissertação de mestrado.

O’REILLY, Tim - What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. [Em linha]. O’Reilly Media, 2005. [Consult. 10 Jan. 2015]. Disponível em WWW:<URL: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>.

OBAMA, Barack - Remarks by the President in Address to the Nation on Syria. [Em linha]. The White House: Office of the Press Secretary, 2013. [Consult. 15 Dez. 2014]. Disponível em WWW:<URL: http://www.whitehouse.gov/the-press-office/2013/09/10/remarks-president-address-nation-syria>.

OFFICE OF INFORMATION (OOI) – Social Media Operations Security. USA: U.S. Navy, 2014.

OFFICE OF THE CHIEF OF PUBLIC AFFAIRS (OTCPA) – The United States Army Social Media Handbook. Washington, DC: Online and Social Media Division, 2011

OMAND, Sir David; BARTLETT, Jamie; MILLER, Carl - Introducing Social Media Intelligence: (SOCMINT). In Intelligence and National Security. Routledge. ISSN 0268-4527. Vol. 27, Nº6 (2012), p. 801-823.

PALEN, Leysia - Online Social Media in Crisis Events. In Educause Quarterly. ISSN 1528-5324. Vol. 31, Nº3 (2008), p. 76-78.

PALMER, Doug – Obama urges Iran stop 'violent and unjust actions'. [Em linha]. Washington: Reuters, 2009. [Consult. 19 Jan. 2015]. Disponível em WWW:<URL: http://www.reuters.com/article/2009/06/20/us-iran-election-obama-sb-idUSTRE55J1KS20090620>.

PASTOR-SATORRAS, Romualdo; VESPIGNANI, Alessandro - Evolution and Structure of the Internet: A Statistical Physics Approach**.** New York: Cambridge University Press, 2004. ISBN 0-521-82698-5.

PIERCE, David– 9 Awesome & Useful Google Maps Mashups. [Em linha]. makeuseof, 2009. [Consult. 16 Jan. 2015]. Disponível em WWW:<URL: http://www.makeuseof.com/tag/9-awesome-useful-google-maps-mashups/>.

PRIBERAM – Comunicação Social. [Em linha]. [2013a]. [Consult. 04 Jan. 2015]. Disponível em WWW: <URL: http://www.priberam.pt/dlpo/comunica%C3%A7%C3%A3o>.

PRIBERAM – *Media*. [Em linha]. [2013b]. [Consult. 04 Jan. 2015]. Disponível em WWW: <URL: http://www.priberam.pt/dlpo/m%C3%A9dia>.

QUIVY, Raymond; CAMPENHOUDT, Luc Van – Manual de investigação em ciências sociais. 2.ª ed.. Lisboa: Gradiva – Publicações, Lda., 1998. ISBN 972-662- 275-1

REUTERS – Timeline: Iran's Ahmadinejad since 2009 re-election. [Em linha]. Tehran: Reuters, 2010. [Consult. 18 Jan. 2015]. Disponível em WWW:<URL: http://www.reuters.com/article/2010/08/04/us-iran-president-events-idUSTRE67325A20100804>.

RICHELSON, Jeffrey T. – The U.S. Intelligence Community. 5ª ed. Colorado: Westview Press, 2008. p.318.

RODEWIG, Cheryl– Geotagging poses security risks. [Em linha]. Fort Benning: U.S. Army, 2012. [Consult. 05 Jan. 2015]. Disponível em WWW:<URL: http://www.army.mil/article/75165/Geotagging_poses_security_risks/>.

ROSMAN, Yossi [et al] – Lessons Learned From the Syrian Sarin Attack: Evaluation of a Clinical Syndrome Through Social Media. In Annals of Internal Medicine. American College of Physicians. vol. 160, Nº9 (2014).

RYAN, Damian; JONES, Calvin - Understanding Digital Marketing: Marketing strategies for engaging the digital generation**.** London: Kogan Page Limited, 2009. ISBN 978-0-7494-5389-3.

RYAN, Damian; JONES, Calvin - The best digital marketing campaigns in the world: mastering the art of customer engagement**.** London: Kogan Page Limited, 2011. ISBN 978-0-7494-6062-4.

SCHWARTAU, Winn - Information Warfare, Chaos on the electronic superhighway. Thunder's mounth press, 1994.

SEDRA, Kamal, ed lit. – "The Role of Social Media & Networking in Post-Conflict Settings: Lessons-learned From Egypt" Washington, DC: 2013.

SOCIALBAKERS – Twitter statistics directory [Em linha]. Socialbakers, [2015a]. [Consult. 15 Jan. 2015]. Disponível em WWW: <URL: http://www.socialbakers.com/statistics/twitter/>.

SOCIALBAKERS – Facebook statistics directory [Em linha]. Socialbakers, [2015b]. [Consult. 15 Jan. 2015]. Disponível em WWW: <URL: http://www.socialbakers.com/statistics/facebook/>.

SOLIS, Brian – Exploring the Twitterverse: Introducing The Twitterverse version 1.0 [Em linha]. 2011. [Consult. 03 Jan. 2015]. Disponível em WWW: <URL: http://www.briansolis.com/2011/01/exploring-the-twitterverse/>.

STATISTA - Global social networks ranked by number of users 2015 [Em linha]. New York: Statista, [2015a]. [Consult. 01 Jan. 2015]. Disponível em WWW: <URL: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.

STATISTA - Leading countries based on number of Facebook users as of May 2014 (in millions). [Em linha]. New York: Statista, [2015b]. [Consult. 01 Jan. 2015].

Disponível em WWW:<URL: http://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>.

STATISTA - Share of mobile social users in the United States who accessed Facebook via mobile from 2011 to 2017. [Em linha]. New York: Statista, [2015c]. [Consult. 01 Jan. 2015]. Disponível em WWW:<URL: http://www.statista.com/statistics/238635/share-of-us-population-who-accessed-facebook-via-mobile-phone/>.

SYMANTEC – ISTR: Internet Security Threat Report 2014. California: Symantec Corporation, 2014, vol. 19.

THE WASHINGTON TIMES (TWT) – Editorial: Iran's Twitter revolution. [Em linha]. The Washington Times, 2009. [Consult. 18 Jan. 2015]. Disponível em WWW:<URL: http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/>.

TOFFLER, Alvin - The Third Wave, New York: Bantam Books, 1980. ISBN 0-553-24698-4.

TOFFLER, Alvin – Powershift. New York: Bantam Books, 1990.

TOFFLER, Alvin; TOFFLER, Heidi - War and Anti-War. Boston: Little, Brown and Company, 1993.

TUGALEAKS – Estatuto editorial. [Em linha]. TugaLeaks, [2014]. [Consult. 31 Jan. 2015]. Disponível em WWW:<URL: http://www.tugaleaks.com/estatuto>.

TZU, Sun - A Arte da Guerra. Lisboa: Bertrand Editora, 2009. ISBN: 978-972-25-1988-5

U.S. AIR FORCE (USAF) – Social Media Guide. [Em linha]. USA: U.S. Air Force, [2015]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.af.mil/AFSites/SocialMediaSites.aspx>.

U.S. BUREAU OF LABOR STATISTICS (USBLS) – Reporters, Correspondents, and Broadcast News Analysts. [Em linha]. Washington, DC: U.S. Department of Labor, 2014. [Consult. 5 Jan. 2015]. Disponível em WWW: <URL:

http://www.bls.gov/ooh/media-and-communication/reporters-correspondents-and-broadcast-news-analysts.htm>.

U.S. CENSUS BUREAU (USCB) – …[população dos E.U.A em 2012]. [Em linha]. American Fact Finder, [2015]. [Consult. 5 Jan. 2015]. Disponível em WWW:<URL: http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk>.

U.S. DEPARTMENT OF DEFENSE (DOD) – … [Documento eletrónico de "User Agreement"]. [Em linha]. USA: U.S. Department of Defense, actual. 19 Jan. 2011. [Consult. 02 Fev. 2015]. Disponível em WWW:<URL: http://www.defense.gov/socialmedia/user-agreement.aspx>.

U.S. DEPARTMENT OF DEFENSE (DOD) – Social Media@DoD. [Em linha]. USA: U.S. Department of Defense, [2015a]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.defense.gov/home/features/2009/0709_socialmedia/>.

U.S. DEPARTMENT OF DEFENSE (DOD) – DoD Social Media Hub. [Em linha]. USA: U.S. Department of Defense, [2015b]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.defense.gov/socialmedia/>.

U.S. MARINE CORPS (USMC) – Social Media Standard Operating Procedures. [Em linha]. USA: U.S. Marine Corps, [2015a]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.marines.mil/News/SocialMedia/SOPs.aspx>.

U.S. MARINE CORPS (USMC) – Social Media Guidance for Unofficial Posts. [Em linha]. USA: U.S. Marine Corps, [2015b]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.marines.mil/News/SocialMedia/Guidance.aspx>.

U.S. NAVY MEDIA BLOG (USNMBLOG) – …[Blog no Tumblr da U.S.Navy]. [Em linha]. USA: U.S. Navy, [2015]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://usnavymedia.tumblr.com/>.

WALSH, Declan - Pakistan blocks Facebook in row over Muhammad drawings [Em linha]. Lahore: The Guardian, 2010, actual. 19 Mai. 2014. [Consult. 13 Nov. 2014]. Disponível em WWW:<URL:

http://www.theguardian.com/world/2010/may/19/facebook-blocked-pakistan-muhammad-drawings>.

WALTZ, Edward – Information warfare: principles and operations. Boston, London: Artech House, Inc., 1998. ISBN 0-89006-511-X

WARD, Mark – Cyber thieves target social sites. [Em linha]. BBC News, actual. 03 Jan. 2008. [Consult. 10 Dez. 2014]. Disponível em WWW:<URL: http://news.bbc.co.uk/2/hi/technology/7156541.stm>.

WATERMAN, Shaun – U.S. Central Command 'friending' the enemy in psychological war: software helps crack terror cells. [Em linha]. The Washington Times, 2011. [Consult. 19 Jan. 2015]. Disponível em WWW:<URL: http://www.washingtontimes.com/news/2011/mar/1/us-central-command-friending-the-enemy-in-psycholo/?page=all>.

WILLIAMS, Patricia A. H., ed lit. – "Information Warfare: Time for a redefinition" Perth: Security Research Centre, 2010.

WISEGEEK - What is Facebook? [Em linha]. Nevada: WiseGEEK, [2015a]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.wisegeek.org/what-is-facebook.htm>.

WISEGEEK - What is Twitter? [Em linha]. Nevada: WiseGEEK, [2015b]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://www.wisegeek.com/what-is-twitter.htm>.

YOUTUBE - Acerca do YouTube [Em linha]. Califórnia: YouTube, [2015a]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: https://www.youtube.com/yt/about/pt-PT/>.

YOUTUBE – Neda Agha Soltan [Em linha]. Califórnia: YouTube, [2015b]. [Consult. 18 Jan. 2015]. Disponível em WWW:<URL: https://www.youtube.com/results?q=neda+agha+soltan>.

ZALMAN, Amy - Jihadi [Em linha]. [2015]. [Consult. 17 Jan. 2015]. Disponível em WWW:<URL: http://terrorism.about.com/od/groupsleader1/a/TerroristGroups.htm>.

ZENG, Daniel [et al] – Social Media Analytics and Intelligence. In Guest Editors' Introduction. IEEE Intelligent Systems. (2010).

9.1. Entrevistas

- COSTA, 2015: Tópico da Entrevista com o COR Fernando Costa, realizada em 30 de Janeiro de 2015, na Academia da Força Aérea.

- EC, 2015: Tópico da Entrevista com um militar da FA cuja identificação não poderá ser publicada por força do cargo que exerce na FA, assim denomina-se por Entrevistado Confidencial (EC). Entrevista realizada em 23 de Janeiro de 2015, Comando Aéreo.

- GONÇALVES, 2015: Tópico da Entrevista com o TCOR Paulo Gonçalves, realizada em 08 de Janeiro de 2015, Estado-Maior da Força Aérea.

- MARQUES, 2015: Tópico da Entrevista com o MAJ José Marques, realizada em 13 de Janeiro de 2015, no Estado-Maior da Força Aérea.

- MINEIRO, 2015: Tópico da Entrevista com o MAJ Paulo Mineiro, realizada em 28 de Janeiro de 2015, Estado-Maior da Força Aérea, Relações Públicas.

- MSIMÕES, 2015: Tópico da Entrevista com o MAJ Miguel Simões, realizada em 14 de Janeiro de 2015, por correio eletrónico.

- PSIMÕES, 2015: Tópico da Entrevista com o MAJ Paulo Simões, realizada em 13 de Janeiro de 2015(a), Estado-Maior da Força Aérea.

- VALENTE, 2015: Tópico da Entrevista com o MAJ António Valente, realizada em 08 de Janeiro de 2015, no Estado-Maior da Força Aérea.

Página intencionalmente deixada em branco

Anexo A - Inquérito

Neste anexo, constam as perguntas feitas no inquérito e que serão analisadas no Anexo B. As perguntas estão divididas por grupos, que correspondem aos grupos do seguinte Anexo (Anexo B). Para o inquérito foram usadas 72 perguntas, a que apenas alguns militares tinham acesso consoante as respostas que davam. No entanto, só foram selecionadas para apresentação neste anexo, as perguntas cuja análise foi incluída neste trabalho.

Caraterização da amostra			
	Oficial		até 4 meses
1-Categoria?	Sargento	3-Qual foi a duração da missão mais longa em que esteve envolvido?	entre 4 a 8 meses
	Praça		entre 8 a 12 meses
	1		entre 1 a 2 anos
2-Em quantas missões internacionais participou?	2		mais de 2 anos
	3		
	mais de 3		

Figura A-1 - Perguntas de caraterização da amostra

Caraterização do uso das RS em missão				
4-Durante a missão em que esteve envolvido usou as Redes Sociais?	Sim		Atualizar o perfil com texto	
	Não		Publicar fotografias	
	Facebook	8-Em missão, usou as Redes Sociais para:*	Publicar vídeo	
	Twitter		Falar com a família	
5-Quais as Redes Sociais que usou em missão?*	Instagram		Falar com amigos	
	WhatsApp		Obter informação	
	Snapchat		Podem levar a quebras de segurança	
	Google +	9-Como encara as Redes Sociais no âmbito das operações militares?*	Aumentam o Conhecimento Situacional (Situational Awareness)	
	YouTube		Motivam os militares	
	LinkedIn		Podem servir para influenciar a opinião pública a nosso favor	
6-Com que frequência utilizou as Redes Sociais em missão?	1 a 2 dias por semana		Deviam haver mais briefings acerca das Redes Sociais em contexto operacional	
	3 a 5 dias por semana	10-Em missão, o uso das Redes Sociais é importante?	(nada importante)	(muito importante)
	Todos os dias		1 até 10	
7-Quando sentiu maior necessidade de aceder às Redes Sociais?*	Antes de ir para missão	11-Em missão, o uso das Redes Sociais é motivador?	(nada motivador)	(muito motivador)
	Durante a missão		1 até 10	
	Depois da missão			

Figura A-2 - Perguntas de caraterização do uso das RS em missão

Caraterização das Informações obtidas nas RS		
12-Em missão, a informação obtida nas Redes Sociais é útil?		
(nada útil)		(muito útil)
1	até	10

Figura A-3 - Pergunta de caraterização das Informações obtidas nas RS

Caraterização do contacto com os familiares			
13-Durante a missão contactou com familiares/amigos pelas Redes Sociais?	Todos os dias		Para tranquilizá-los
	Regularmente	15-Em missão usou as RS para falar com os F/A porquê?*	Para manter o contacto
	Nunca		Para atenuar a tristeza de estar em missão
14-De que forma contactou com eles pelas Redes Sociais?*	Mensagens privadas		Porque é um fator motivador
	Publicações de vídeo		Outras razões
	Publicações de imagem		Não se aplica
	Publicações de texto		
	Não contactei com eles pelas Redes Sociais		

Figura A-4 - Perguntas de caraterização do contacto com os familiares

Caraterização do perigo de quebras de segurança pelos militares			
16-Chegou a identificar as suas publicações durante o tempo que esteve em missão? *	Cheguei a identificar o local onde estava	19-Sabe o que é o Geotagging?	É um jogo das Redes Sociais que pode ser perigoso
	Cheguei a identificar com quem estava		É um movimento das Redes Sociais, para preservar a Terra contra as guerras
	Cheguei a identificar os camaradas que me acompanhavam na missão		É um processo que faz identificação geográfica automática
	Nunca identifiquei onde estava nem com quem estava	20-Preocupou-se em retirar a apresentação automática da localização suas publicações?	Não sei responder
17-Antes de ir para a missão, removeu das Redes Sociais tudo o que o pudesse identificar como militar?	Sim		Não era necessário
	Não		Não entendo o que isso é
18-Já teve um smartphone?	Sim e tinha-o comigo durante a missão		Sim, mas não retirei
	Sim, mas não o tinha na missão		Sim e retirei
	Não		

Figura A-5 - Perguntas de caraterização do perigo de quebras de segurança pelos militares

Caraterização do perigo associado aos F/A			
21-Informou os familiares ou amigos acerca da missão?	Não informei nem familiares nem amigos	23-Os seus familiares e/ou amigos destacavam nas RS o que você fazia em missão?	Sim e isso motivava-me
	Informei só os familiares		Sim, mas não me motivava
	Informei só os amigos		Acho que nunca aconteceu
	Informei familiares e amigos		Tenho a certeza que nunca aconteceu
22-O que lhes informou acerca da missão?	Informei-lhes sobre onde e quando seria a missão	24-Que cuidados teve em relação aos familiares e/ou amigos acerca das RS?*	Eles não têm que ter cuidados com as RS
	Informei apenas onde seria a missão		Não lhes falei sobre os cuidados a ter
	Informei apenas quando seria a missão		Disse-lhes para não revelarem informações da missão
	Ocultei que ia em missão		Demonstrei-lhes o perigo de certas publicações
	Não se aplica		

Figura A-6 - Perguntas de caraterização do perigo associado aos F/A

Caraterização da importância dos Briefings			
25-Até hoje, a quantos briefings assistiu acerca das Redes Sociais?	Nenhum	28-Qual(ais) das seguintes matérias foram abordadas nesses "briefings"?*	Quebras de segurança nas RS
	1		Cuidados de segurança nas RS
	2		Casos estudo acerca de quebras de segurança nas RS
	3		Gestão de matérias classificadas
	4		Não posso responder
	mais de 4	29-Ao nível da FAP, como classifica a importância que os militares atribuem aos briefings acerca das RS?	As Redes Sociais não são importantes para a FAP
26-Antes de ingressar na missão foi "briefado" acerca da utilização das Redes Sociais?	Sim		Sou o único a dar a devida importância
	Não		Poucos dão a devida importância
27-Considerou esse briefing importante?			Muitos dão a devida importância
(nada importante)	(muito importante)		Todos dão a devida importância
1 até 10			

Figura A-7 - Perguntas de caraterização da importância dos Briefings

Caraterização do interesse dos militares pelas Redes Sociais da FAP			
30-Conhece as Redes Sociais em que a FAP faz publicações?	Sim		Sempre
	Não	34-Costuma comentar essas publicações?	Muitas vezes
31- Quais as Redes Sociais FAP que conhece? *	Facebook		Esporadicamente
	Twitter		Raramente
	Google +		Nunca
	Instagram	35-Alguma vez partilhou as publicações da FAP nas Redes Sociais?	Sim
	YouTube		Não
32- Está atento às publicações da FAP nas Redes Sociais?	Sempre	36-Porque partilha as publicações da FAP? *	Para promover a missão da FAP
	Muitas vezes		Porque sinto orgulho
	Esporadicamente		Nunca partilhei
	Raramente		Outros motivos
	Nunca		Para promover a imagem da FAP
33-Que tipo de sentimentos lhe surge ao ver as publicações da FAP? *	Frustração		
	Orgulho na organização		
	Motivação		
	Outros sentimentos		

Figura A-8 - Perguntas de caraterização do interesse pelas RSFA

Página intencionalmente deixada em branco

Anexo B – Análise do Inquérito

Este anexo remete para a análise da utilização das RS por militares da FA que já participaram em missões internacionais. O inquérito foi criado através da plataforma Google Docs e enviado para 436 militares que participaram em missões internacionais nos anos 2012, 2013 e/ou 2014. No total, 10 inquéritos resultaram em envio falhado. Obteve-se um total de 90 inquéritos respondidos, onde se contabilizam 36 Oficiais (40%), 47 Sargentos (52%) e 7 (8%) Praças (Tabela B-2, Anexo B).

Para a análise dos inquéritos foi utilizada a plataforma SPSS Statistics 17.0 que permitiu fazer o cruzamento das respostas de diferentes perguntas, por exemplo: permitiu saber quantos dos militares que responderam "Sim" na pergunta 35 (Anexo A), também responderam "orgulho na organização" na pergunta 33 (Anexo A).

Indicações: Todas as tabelas e figuras deste anexo remetem para as perguntas que deram origem e essa referência surge na forma (Nº A), remetendo para o respetivo nº da pergunta do Anexo A. Pode estar no nome da tabela ou dentro.

Na coluna mais à direita de cada tabela, constam o número de militares (grupo) que puderam responder à questão, tal como explicado no Anexo A. Nesta análise serão apresentados os seguintes grupos (por esta ordem):

Tabela B-1 - Grupos de militares da análise dos inquéritos.

Grupos	Definição
90 Militares	Totalidade dos inquiridos
72 Militares	Militares que usaram as RS durante a missão
21 Militares	Militares que identificaram as OPMIL em publicações nas RS
86 Militares	Militares que já tiveram conta nas RS
17 Militares	Militares que usaram as RS em missão e não sabem o que é o Geotagging
74 Militares	Militares que foram *briefados* antes da missão mais longa participada
76 Militares	Militares que já tiveram conta nas RS e conhecem as RSFA
50 Militares	Militares que sentem orgulho ao verem as publicações da FA

(*): a presença do "asterisco vermelho" remete para todas as perguntas que possibilitaram aos inquiridos a escolha de mais do que uma opção.

B-1 Caraterização da amostra

Tabela B-2 - Caraterização da amostra de 90 militares

(1A) Categorias	Oficial	40%	**90 Militares**
	Sargento	52%	
	Praça	8%	
(2A) Missões efetuadas	1	41,1%	

	2	17,8%	
	3	6,7%	
	Mais de 3	34,4%	
(3A) Duração da missão mais longa (meses)	Até 4	53,3%	
	Entre 4 a 8	40,0%	
	Entre 12 a 24	3,3%	
	Mais de 24	3,3%	

- Na Tabela B-2 são identificadas as amostras de militares por posto, em quantas missões participaram e qual a duração da missão mais longa em que participaram;
- Acrescenta-se que 95,6% dos inquiridos já teve conta nas RS.

B-2 Caraterização do uso das RS em missão

Tabela B-3 - Utilização das RS pelos militares nas operações,

(4A) Uso das RS em missão	Sim	80%	**90 Militares**
	Não	20%	
(5A) RS utilizadas em missão*	Facebook	93%	**72 Militares**
	YouTube	30,6%	
	WhatsApp	25%	
	Twitter	5,6%	
(6A) Utilização das RS em missão (dias por semana)	7	56,9%	
	3 a 5	25%	
	1 a 2	18,1%	

- 80% dos militares usaram as RS em missão;
- A RS mais utilizada foi o Facebook, com 93%;
- 56,9% dos militares usaram as RS todos os dias durante a missão;
- Acrescenta-se que 86% dos militares, afirmaram que durante a missão sentiram maior necessidade de aceder às RS em comparação com o uso que deram antes ou depois da missão (ver Pergunta 7, Anexo A).

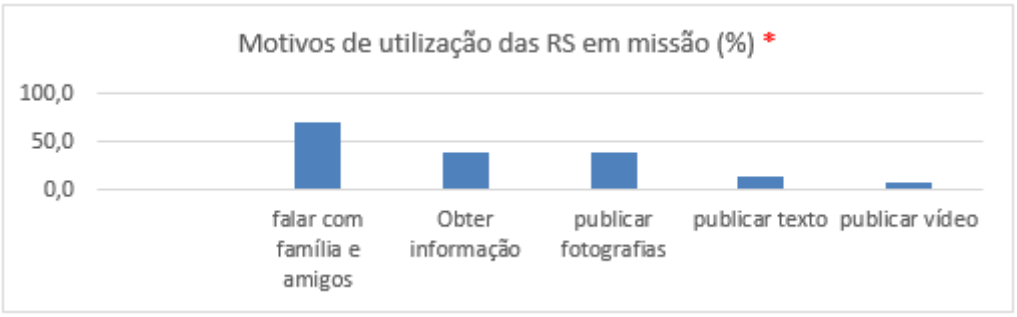


Figura B-1 – (8 A) Motivos de utilização das RS em missão (%)

- A maior parte, 69,4%, usou as RS principalmente para falar com a família e amigos e 38,9% usou as RS para obter informações e/ou publicar fotografias.

Tabela B-4 – (9 A) O que os militares pensam das RS nas operações

Opinião dos militares quanto às RS nas OPMIL		
Levam a quebras de segurança	87,8%	**90 Militares**
Aumentam o *Situational Awareness*	31,1%	
Podem servir para influenciar a OP a nosso favor	45,6%	

- 87,8% dos militares tem consciência que as RS podem levar a quebras de segurança;
- Apenas 31,1% acreditam que as RS permitem o ganho de SA durante as OPMIL, ou simplesmente não tiveram essa necessidade. Curiosamente, a maior parte desses militares nunca participou numa missão mais longa do que 4 meses, constituindo 76,2% dos 31,1% da Tabela B-4.

Tabela B-5 - Importância e motivação encontrada pelo uso das RS em missão

(10A) Importância	Muito importante/importante	68%	**72 Militares**
	Pouco/nada importante	32%	
(11A) Motivação	Muito motivador/motivador	69%	
	Pouco/nada motivador	31%	

- 68% referem que o uso das RS em missão é importante, dos quais, 50% classificam o seu uso como “Muito importante” ;
- 69% afirmam que o uso das RS em missão é motivador, dos quais, 54% classificam o seu uso como “Muito motivadoras”.

B-3 Caraterização das informações obtidas nas RS

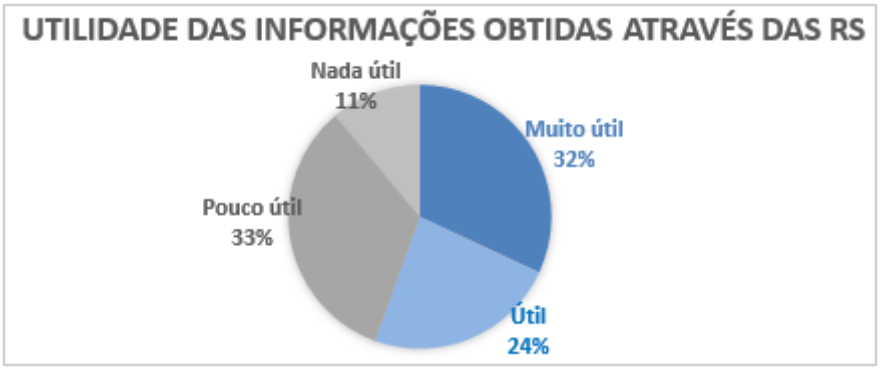


Figura B-2 – (12 A) Classificação de utilidade das informações obtidas através das RS.

- A maior parte dos militares que usaram as RS nas operações, encontra utilidade das informações obtidas nas RS, representando 56%.

B-4 Caraterização do contacto com os familiares

Tabela B-6 – (13 A) Frequência com que os militares contactaram com as famílias através das RS.

Todos os dias	29,2%	**72 Militares**
Regularmente	66,7%	
Nunca	4,1%	

- 95,6% dos militares que usaram as RS em missão contataram com os familiares através das RS de forma diária ou regular.

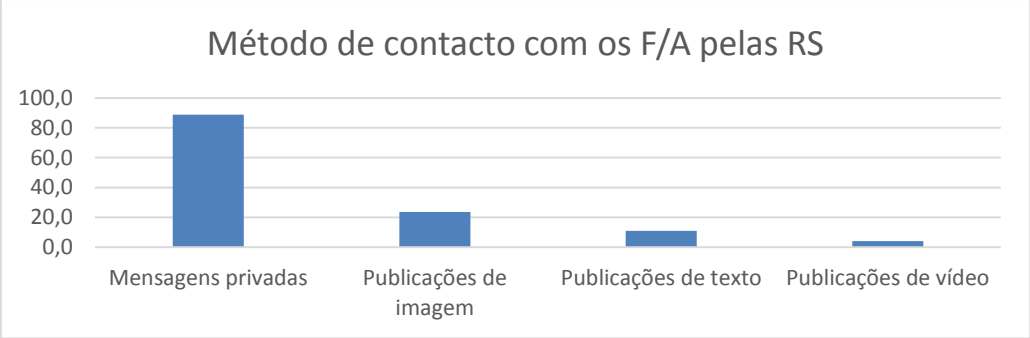


Figura B-3 – (14A) Método de contacto com os F/A pelas RS (múltipla escolha).

- 88,9% contataram os F/A através do chat nas RS (mensagens privadas);
- Acrescenta-se que 48,6% contactaram com os F/A pelas RS para os tranquilizar (ver Pergunta 15, Anexo A).

B-5 Caraterização do perigo de quebras de segurança pelos militares

Tabela B-7 – (16 A) Identificações acerca das operações feitas pelos militares.

Identificou?	Sim	29,2%	**72 Militares**
	Não	70,8%	
O que identificou? *	Local	71,4%	**21 Militares (29,2%)**
	Com quem estava	38,1%	
	Camaradas	28,6%	

- 29,2% identificaram as suas publicações nas RS;
- A maior parte dos inquiridos identificou o local onde estavam, representando 71,4% dos 21 militares que identificaram as publicações;
- Acrescenta-se que 14,3% dos 21 militares identificaram tudo (o local, com quem estavam e que camaradas os acompanhavam).

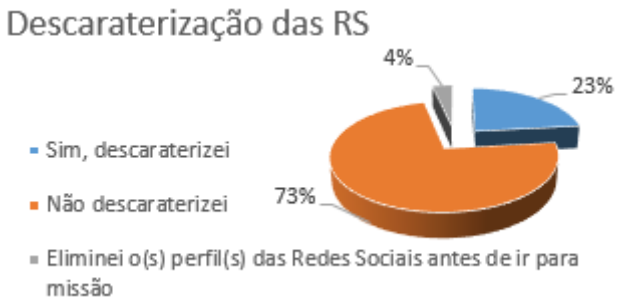


Figura B-4 - (17 A) Percentagem de militares que descaraterizaram as RS antes de ingressar na missão.

- Dos 86 militares que já tiveram conta nas RS, 73% afirmam que não descaraterizaram[30] as contas das RS;
- Apesar disso, 87,8% dos 90 militares reconhecem que as RS potenciam as quebras de segurança (Tabela B-4, Anexo B) (ver Pergunta 9, Anexo A).

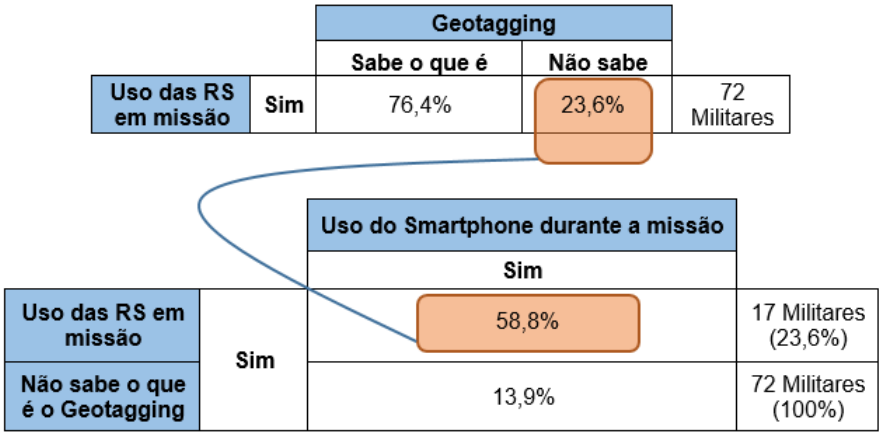
Tabela B-8 - Relação entre o uso do S*martphone* durante as operações e o conhecimento do que é o Geotagging

		***Smartphone* durante a missão**			
		Sim	Não		
(18 A) Já teve *Smartphone*	Sim	73,3%	16,7%	90%	**90 Militares**
	Não			10%	
(19,20A) Geotagging	Sabe o que é	56,7%	16,6%	73,3%	
	Não sabe	16,7%	10%	26,7%	

- 90% dos militares já teve *Smartphone* e 73,3% tinham o equipamento durante as operações;
- 16,7% dos militares podem constituir perigo para as operações na medida em que usaram o *Smartphone* durante as operações e não sabem o que é o Geotagging.

[30] Tal como já referido, por descaraterizar as RS entende-se, como uma medida de segurança, remover delas tudo o que possa identificar os indivíduos como militares.

Tabela B-9 - Relação tripla entre os militares que usaram as RS em missão, não sabem o que é o Geotagging e usaram o *Smartphone* em missão, constituindo um grupo de perigo representado a laranja.



- Ou seja, 23,6% dos militares que usaram as RS em missão, não sabem o que é o Geotagging;
- Mais grave ainda, é que 58,8% dos militares reuniam todas as condições de perigo para as operações, no que toca à problemática do Geotagging. Ou seja, estes militares usaram as RS durante a missão, não sabem o que é o Geotagging e também usaram o *Smartphone*, abrindo a possibilidade das operações serem geolocalizadas pelo adversário. Este grupo de militares constitui 13,9% do grupo que usou as RS em operações.

B-6 Caraterização do perigo associado aos F/A

Tabela B-10 – (21;22 A) Análise das informações dadas aos F/A.

		Informações dadas aos F/A acerca da missão					
		Onde e quando	Apenas onde	Apenas quando	Nenhuma		
A quem foram dadas informações	Só familiares	30%	6,7%	2,2%	3,3%	42,2%	**em 90 Militares**
	Familiares e amigos	40%	15,6%	0	0	55,6%	
		70%	22,3%	2,2%	3,3%		
		em 90 Militares					

- 2 respostas não foram consideradas;
- 70% dos militares informaram aos familiares ou aos familiares e amigos sobre onde e quando seria a missão (ver Perguntas 21 e 22, Anexo A).

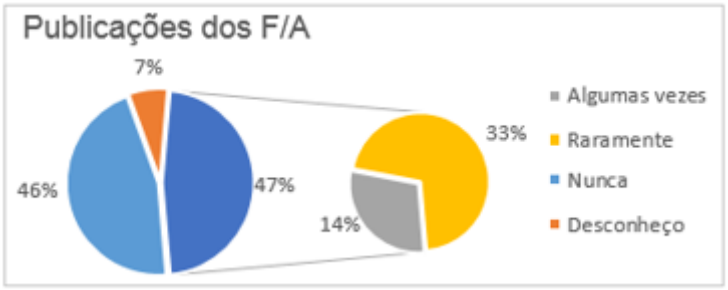


Figura B-5 – (23 A) Frequência das publicações dos F/A acerca da missão.

- Os militares que participaram nas RS durante a missão revelam que as famílias podem por vezes comprometer uma operação, dado que 47% dos 72 militares afirmam que as famílias fizeram publicações nas RS que mencionavam a missão em que os militares estavam envolvidos (ver Pergunta 23, Anexo A).

Tabela B-11 – (24 A) Sensibilização dos F/A pelos militares

"Que cuidados teve em relação aos F/A acerca das RS?" *		
"Eles não têm que ter cuidados"	3,3%	**90 Militares**
"Não lhes falei dos cuidados a ter"	10%	
"Disse-lhes para não revelarem informações sobre a missão nas RS"	48,9%	
"Demonstrei-lhes o perigo de fazer certas publicações nas RS"	54,4%	

- A maior parte dos militares teve o cuidado de falar com os F/A acerca das RS, alertando para os perigos das mesmas e para que os F/A não revelassem informações sobre a missão nas RS (54,4% e 48,9%, respetivamente);
- 13,3% dos militares revelam que não briefaram os F/A acerca dos cuidados a ter nas RS, dos quais 3,3% acreditam que os F/A não têm que ter cuidados nas RS, o que apesar de ser um valor baixo, não deixa de representar um perigo.

B-7 Caraterização da importância dos Briefings

Tabela B-12 – (2;25 A) Briefings recebidos vs. Nº de missões internacionais efetuadas (valores em %).

		Em quantas missões internacionais					
		1	**2**	**3**	**mais de 3**		
Até hoje, a quantos briefings assistiu acerca das RS?	**Nenhum**	3,3	0	1,1	5,6	10%	90 militares
	1	13,3	1,1	0	6,7	71,2%	
	2	14,4	8,9	4,4	4,4		
	3	6,7	4,4	0	6,7		
	4	0	1,1	0	0	18,8%	
	mais de 4	3,3	2,2	1,1	11,1		

- Antes de ingressarem nas missões, nem todos os militares são briefados acerca das RS. As respostas dos inquéritos evidenciam esta realidade, 90% dos militares já receberam pelo menos um briefing acerca da utilização das RS e 10% nunca receberam briefing acerca destas matérias;
- É de realçar que 5,6% dos militares nunca receberam briefing e participaram em 3 ou mais missões internacionais;
- Identificados com cor-de-laranja, encontram-se destacados 33,3% de militares que podem ter sido ameaças à segurança das operações, na medida em que não foram devidamente briefados acerca das RS antes de todas as missões e partindo do pressuposto de que basta um militar não ter recebido briefing acerca da segurança nas RS, antes da missão, para existir risco de que o mesmo comprometa a segurança das operações (ver o caso estudo exposto por Mineiro (2015), no Subcapítulo 7.4.2).

Tabela B-13 – (26;27 A) Classificação da importância dos briefings.

Recebeu Briefing acerca das RS	Sim	82,2%	**90 Militares**
	Não	17,8%	
Importância do Briefing	Muito importante/ Importante	82%	**74 Militares (82,2%)**
	Pouco importante	18%	

- 17,8% dos militares não receberam briefing acerca das RS antes de ingressarem na missão mais longa em que participaram;
- Acrescenta-se que segundo todos os inquiridos que foram *briefados* (82,2%), as quebras de segurança e os cuidados a ter nas RS, foram matérias abordadas (ver Pergunta 28, Anexo A). E realça-se que 74% dos *briefados*, consideraram o briefing como Muito Importante (Pergunta 27, Anexo A).

Tabela B-14 – (9;29 A) Classificação da importância dos briefings.

(9 A) Necessidade de mais briefings *	Sim	67,8%	**90 Militares**
	Não	32,2%	
(29 A) Atributo de importância	Muitos dão a devida importância	36,7%	
	Poucos dão a devida importância	63,3%	

- Face à realidade da nossa organização, nomeadamente no que toca à atribuição de importância hierárquica quanto à necessidade de existirem briefings assíduos antes dos militares ingressarem nas missões, constata-se que na opinião de quem esteve destacado não existem briefings suficientes acerca das RS. 67,8% militares destacaram a necessidade de mais briefings;

- E ainda, a maior parte dos militares (63,3%) acha que não se encaram os briefings acerca das RS com a devida importância.

Tabela B-15 – (19;24;26 A) Relação entre os militares briefados, conhecimento do Geotagging e preocupação em briefar os familiares e amigos.

		Militares que, antes de ingressar na missão:				
		Foram briefados	Não foram briefados			
Geotagging	**Sabe o que é**	61,1%	12,2%	73,3%	100%	**90 Militares**
	Não sabe	21,1%	5,6%	26,7%		
Briefou os F/A	**Sim**	71,1%	15,6%	86,7%	100%	
	Não	11,1%	2,2%	13,3%		

- 26,7% dos militares inquiridos não sabem o que é o Geotagging;
- 21,1% dos militares foram *briefados* e não sabem o que é o Geotagging, o que significa que 25,7% dos militares que foram *briefados* não sabem o que é essa caraterística das tecnologias atuais;
- Acrescenta-se ainda que 45,8% dos militares que não sabem o que é o Geotagging, já participaram em 3 ou mais missões e os restantes 54,2% participaram em 1 ou 2 missões (Pergunta 2 e 19, Anexo A);
- Segundo a Tabela B-15, também se constata que 11,1% dos militares foram *briefados* e não se preocuparam em dar a conhecer aos familiares e/ou amigos (F/A) os perigos das RS para as operações. O que significa que 13,5% dos militares que foram *briefados*, não se preocuparam em *briefar* os F/A;
- Assim, conclui-se o seguinte: os briefings não são tão eficientes como deveriam, ou os militares não os encaram com a devida seriedade; e deveriam haver mais briefings e ações de sensibilização acerca das RS.

B-8 Caraterização do interesse pelas RSFA

Tabela B-16 - Interesse dos militares pelas RSFA

(30 A) Conhece as RSFA	Sim	88,4%	**86 Militares**
	Não	11,6%	
(31 A) RSFA preferidas *	Facebook	98,7%	**76 Militares (88,4%)**
	YouTube	46,1%	
	Twitter	22,4%	
(32 A) Interesse pelas publicações das RSFA	Sim	79%	
	Não	21%	
(33 A) Sentimento ao ver as publicações *	Orgulho	65,8%	
	Motivação	47,4%	

- 88,4% dos militares conhecem as RSFA;
- A RSFA mais conhecida é o Facebook com 98,7%;
- 79% dos militares demonstram interesse pelas publicações acerca da FA, e os restantes 21% raramente ou nunca vêm as publicações da FA nas RS;
- 65,8% de militares sentem orgulho na FA ao verem as publicações nas RS;
- Essas publicações são um fator motivador para 47,4% militares.

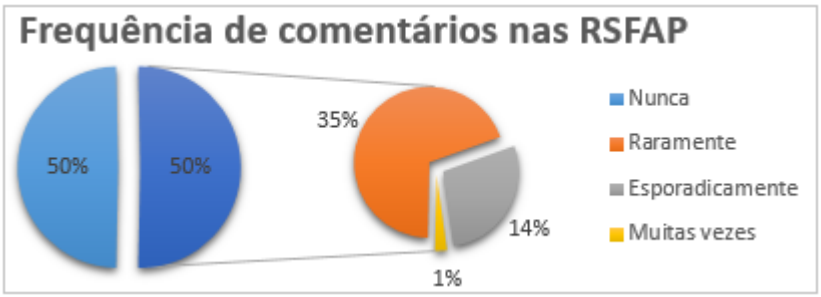


Figura B-6 – (34 A) Frequência com que os militares fazem comentários nas publicações das RSFA.

- 50% do grupo de 76 militares comentam as publicações da FA muitas vezes, esporadicamente ou raramente;
- Segundo a Tabela B-4, 45,6% de todos os militares inquiridos afirmam que as RS permitem influenciar a OP em nosso favor (ver Pergunta 9, Anexo A).

Tabela B-17- Partilha de publicações das RSFA

(35 A) Partilhou as publicações das RSFA	Sim	64,5%	**76 Militares**
	Não	35,5%	
(36 A) Motivo	Promover a imagem da FA à OP	56,6%	
	Promover a missão da FA	53,9%	

- A maioria dos militares já partilhou as publicações da FA nas RS, representando 64,5%;
- A maioria dos militares, 56,6%, partilha as publicações das RSFA "para promover a imagem da FA à OP" e 53,9% "para promover a missão da FA".

Tabela B-18 – (33;35 A) Partilha das publicações das RSFA em função do sentimento de orgulho

		Partilhou as publicações da FA		
		Sim	**Não**	
Sentimento	**Orgulho**	78%	22%	**50 Militares**

- 78% dos militares sentem orgulho ao ver as publicações das RSFA e acabam por partilhar as mesmas nas RS pessoais.

Anexo C - Modelo de Análise

Tabela C-1 - Modelo de Análise

Conceitos	Dimensões	Indicadores	Forma de validação
Comunicação externa	Impacto na missão	Preocupação organizacional	Entrevistas e Inquérito
		Planeamento estratégico	
		Briefings	
	Segurança	Importância hierarquia	Entrevista e Inquérito
		Importância para os militares da FA	Inquérito Interno
Ambiente de Informação	Meios	Quantidade de atores e capacidades das RS	Entrevistas
	Âmbito da Gestão e do Uso	Existência de Política de Gestão e uso	
Situational Awareness	Utilização	Em várias áreas: segurança, informação pública	Entrevistas
Motivação	Âmbito do uso	Realização de Post	Entrevistas e Inquérito
		Esclarecimento de comentários	