Nelson Manuel A. Chapala
Nélido Dinis S. Atumane

Guerra de Informação e Segurança em Redes Sociais

Circundantes, Operações e Armas da Guerra de Informação

Comportamento, Segurança e Situação Operacional em Redes Sociais

Academia Militar Marechal Samora Machel

Guerra de Informação e Segurança em Redes Sociais

Circundantes, Operações e Armas da Guerra de Informação

Comportamento, Segurança e Situação Operacional em Redes Sociais

Ficha técnica

Título	Guerra de Informação e Segurança em Redes Sociais
Subtitulos	Circundantes, Operações e Armas da Guerra de Informação Comportamento, Segurança e Situação Operacional em Redes Sociais
Autores	Coronel Nelson M.Alfredo Chapala Tenente-Cornel Nélido D. Saide Atumane
Revisão Científica	Prof. Doutor Félix Singo
Revisão Linguística	Coronel Alberto Moises
Edição e Impressão:	Imprensa 25 de Setembro
Ano	2022

ÍNDICE

Prefácio

O presente livro expõe uma visão teórica sobre a guerra de informação, a fim de oferecer entendimento aos mais diferentes interessados neste tópico, principalmente para aqueles que trabalham no sector de defesa e segurança.

O livro foi elaborado com a consciência de que, com a evolução tecnológica, tornou-se fácil obter e disseminar as informações, algumas delas com mensagens que criam instabilidade e descredibilizam as instituições e entidades. Daí que, urge a necessidade de reforçar, por um lado, as boas maneiras de utilização das Tecnologias de Informação e Comunicação (TIC) e, por outro, explorar as potencialidades para obtenção das informações operacionais.

A valiosa obra descreve os riscos de uso das tecnologias e fornece algumas dicas e cuidados a serem tomados durante a sua utilização, e foi elaborado no âmbito do projecto da AM denominado “um docente-um manual”.

O livro está dividido em três partes relacionadas. Na primeira parte os autores discutem os conceitos, o enquadramento e as envolventes, as operações e as armas da guerra de informação, em virtude de de

que, actualmente, os termos digitalização do campo de batalha, integração e globalização das comunicações, jogos de guerra, sistemas C^3I (Comando, Controle, Comunicações e inteligência) e C^4I^2 (Comando, Controle, Comunicações, Computador, inteligência e Informação), Internet Militar, *hackers,* e mais, devem ser amplamente discutidos. É nesta visão que acredito, ainda, que o conceito da Guerra de Informção (GI) está ligado à estratégia nacional, uma vez que, com a evolução tecnológica, essa guerra provoca profundas implicações, tanto para a estratégia militar como para a estratégia de segurança nacional

Na segunda parte do livro os autores explicam como os *media* são utilizados para a potencialização de acções da GI. E, pessoalmente, considero óbvia a discussão sobre a influência dos *media* nos conflitos armados, pois eles desempenham um papel importante na GI,por influenciar as opiniões da população e estabelecer um monopólio total sobre o fluxo de informação, processos discursivos que moldam o mundo moderno. Na minha percepção pessoal, o livro vem para alertar os membros de Defesa e segurança e a sociedade em geral a fazerem o ajuizamento da informação que recebem dos *media*, antes de agirem.

Na terceira e última parte discute-se os perigos e as potencialidades das redes sociais em operações

militares. Entretanto, o que não se pode deixar de lado é o facto de que no ambiente das redes sociais, além de informar-se e desinformar-se, ocorre a divergência de ideias, gerando-se conflitos sociais que até influenciam para o surgimento de confrontos, alguns deles com uso de armas.

O Comandante da AM

_____

Francisco Zacarias Mataruca
(Major-General)

PARTE I

Circundantes, Operações e Armas da Guerra de Informação

1. GENERALIDADES

Vive-se, hoje, numa época em que a informação desempenha um papel fundamental para a realização de uma guerra moderna, denominada "Guerra de Informação", uma guerra onde, com as constantes inovações em Tecnologias de Informação e Comunicação, o *modus operandi* e a maneira como as sociedades se preparam para enfrentá-la está-se modificando. Actualmente, qualquer força, pelo menos bem preparada, sempre procura obter as informações relevantes do inimigo, para explorar as suas fragilidades.

Nesta senda, o sector de defesa e segurança de qualquer nação é desafiado e instado a implementar de forma rigorosa as medidas que visam proteger a sua informação estratégica e os seus sistemas de informação e comunicação. Os desafios não podem se resumir apenas no cumprimento das medidas de segurança e aquisição de meios tecnológicos, como também na formação, criando-se (em vários níveis) cursos específicos de segurança de informação.

Entretanto, os actuais sistemas de auxílio à decisão são destacados pela pluralidade e efemeridade dos vectores de informação que os alimentam e o seu universo de aplicação é largo e decisivo no campo de batalha moderno, onde são empregues, de forma extensiva, equipamentos tecnológicos avançados[1].Trata-se de cenários que

[1] Dinis, J. A. H. (2003). *A guerra de informação: perspectivas de segurança e competitividade*. Revista Militar, Lisboa.

não podem ser ignorados e, para isso, é imperioso que o sector de defesa e segurança controle e delineie (sempre) as directrizes de utilização das suas tecnologias, principalmente aquelas que armazenam e movimentam as informações de carácter crítico e com influência nos sistemas de comando e controle.

Importa ressaltar que a ideia não é colocar em causa a importância das tecnologias - até porque, dentro deste contexto, elas são importantes para o garante da eficácia dos sistemas de informação existentes - mas há que sublinhar que, por vários factores, tais como a falta de ética dos usuários e algumas fragilidades dos próprios sistemas de informação, as informações estratégicas ficaram mais vulneráveis e fáceis de tornarem inoperacionais os sistemas de informação de qualquer força, surgindo um novo conceito denominado por “Guerra de Informação (GI)”[2].

Com os expressivos progressos tecnológicos na área da Informática e das Telecomunicações, as armas de GI tornaram-se mais perigosas, havendo necessidade de definirem-se e reestruturarem-se novas e antigas ideias ligadas ao porte e ao uso da informação, sendo imperioso trazer os termos digitalização do campo de batalha, integração e

---

[2] Nunes, P.FV. (1999). *Impacto das Nova Tecnologias no Meio Militar: A Guerra de Informação.* Revista Militar. Lisboa

globalização das comunicações, jogos de guerra, sistemas C^3I (Comando, Controle, Comunicações e inteligência) e C^4I^2 (Comando, Controle, Comunicações, Computador, inteligência e Informação), Internet Militar, *hackers,* e mais[3] [4].

O conceito de GI é discutido neste livro porque, por conta da sua relevância, tornou-se o epicentro de debates alargados, no âmbito quer militar, quer civil.

2. SISTEMA DE INFORMAÇÃO E INTEGRADO C3I/C4I

Na era da internet, da globalização e do trabalho centrado em rede, a actividade humana tende a inserir-se mais em espaços virtuais do que em locais físicos[5]. Neste novo contexto, a Informação e o conhecimento tendem a difundir-se e a dispersar-se num determinado espaço, ainda que associado a pessoas, processos e tecnologias, o que necessariamente suscita um novo tipo de gestão adequada e específica - por exemplo, a Gestão do Conhecimento[6].

---

[3] Damjanović, D. Z. (2017). *Types of information warfare and examples of malicious programs of information warfare*. Zrenjanin, Republic of Serbia. Vojnotehni čki glasnik / military technical courier, Volume 65.

[4] Nunes, P. F. V. (2004). *Ciberterrorismo: aspectos de segurança*. Revista Militar

[5] Kuehl, D.T. (2002*). Information Operations, Information Warfare, and Computer Network Attack*. International Law studies. Volume 76

[6] Ibid 1.

Neste contexto, é importante distinguir os conceitos associados aos termos “Sistema de Informações” e “Sistema de Informação”. Um “Sistema de Informações” processa informação classificada, cujo acesso é permitido apenas a pessoas credenciadas para o efeito, e que, face às funções que exercem, também se deve cumprir rigorosamente a regra de necessidade de conhecer[7]. Enquanto um “Sistema de Informação” constitui a plataforma de processamento da informação, composto por determinadas “tecnologias de informação”, um tipo de gestão” e uma organização adequada[8], e, em geral, refere-se a um sistema que processa informação não-classificada, embora o seu acesso possa ser restringido a determinados utilizadores da informação, através de um perfil adequado e correspondente à respectiva função numa determinada organização[9]. Nestes termos, um “Sistema de Informações” necessita obviamente de um “Sistema de Informação” adequado, onde a segurança da informação deve ser um requisito essencial[10].

Qualquer operação militar é caracterizada por um Comando bem definido, com Controlo das acções que se vão desenvolvendo, e é indispensável um Sistema de Informações (*Intelligence*), apto a responder com informação

---

7 Ibid.
8 Ibid 5.
9 Ibid 5.
10 Ibid 1.

adequada e oportuna sobre a situação, e de apoio aos seus diversos níveis - táctico, operacional e estratégico[11]. Por outro lado, um Sistema de Comunicações fiável, de confiança e com segurança adequada, é outra componente imprescindível na composição de um Sistema Integrado de Comando, Controlo, Comunicações e Informações, designado pelo termo abreviado de "Sistema C3I"[12]. Um Sistema C3I, que também se designa por "Sistema C4I", deve possibilitar o melhor desempenho do respectivo Sistema de Forças. Com base nos seus meios disponíveis, um Sistema C4I deve permitir a integração do Conhecimento a todos os níveis do dispositivo da força, e em particular aos seus elementos fundamentais, de modo a conseguir-se alcançar o sucesso das operações[13].

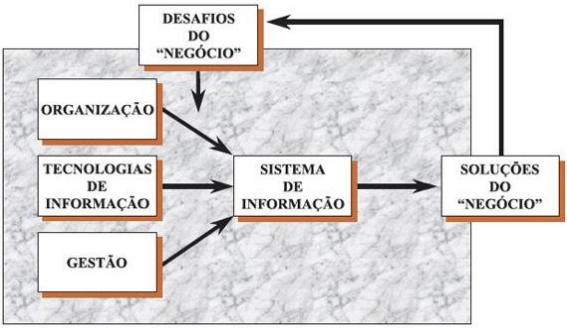

Figura 1.1. Modelo de um Sistema de informação[14]

[11] Ibid.
[12] Ibid.
[13] Ibid 1.
[14] Ibid.

Os conceitos de “Sistema de Informação” e de “Sistema Integrado C3I/C4I”, apresentam-se nas Figuras 1.1 e 1.2, e refira-se que um Sistema C3I/C4I considera-se um tipo particular e específico de um “Sistema de Informação”[15].

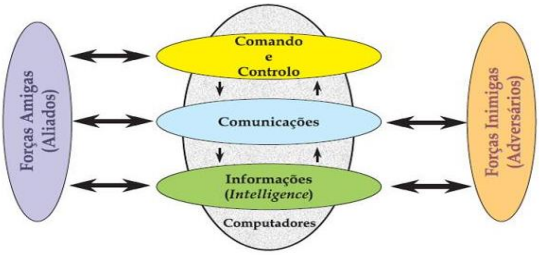

Figura 1.2. Modelo de um Sistema Integrado C3I/C4[16]

A concepção do modelo de um Sistema Integrado C3I/C4I[17], embora se aplique, em particular, no âmbito das Forças Armadas (FFAA), considera-se, no entanto, poder adaptar-se também às actividades e circunstâncias do tecido empresarial, onde a “Informação” se considera como um novo factor de produção[18].

Numa organização – militar, em particular -, a informação constitui um alicerce sem o qual uma

---

[15] Chapala, N. (2021). Efeitos físicos, sintaxe e semânticos da guerra de informação na era tecnológica: ameaças e desafios para as Forças Armadas de Defesa de Moçambique. Revista Científica do Instituto Superior de Estudos de Defesa Tenente-General Armando Emílio Guebuza: Série Defesa & Segurança: Vol.1, p. 72-88.

[16] Ibid 1.

[17] Ibid.

[18] Ibid15.

organização fica desprotegida e com dificuldade para sobreviver e fazer face às mudanças operadas no seu meio envolvente[19]. A Figura 1.3 ilustra que a competitividade de uma organização militar passa por tirar partido das forças e das oportunidades, no sentido de minimizar as suas fraquezas e reduzir as ameaças, de forma adequada e em tempo oportuno[20]. Assim sendo, qualquer organização militar que pretenda ser competitiva em função dos seus opositores, deve possuir um Sistema de Informação eficaz e eficiente.

Figura 1.3. Sistema nervoso digital versus compectividade[21]

As mudanças tecnológicas que tiveram lugar nas últimas décadas deram um lugar de destaque à utilização da informação no nosso dia-a-dia, quer a nível profissional e mesmo familiar[22]. A informação passou a ser um elemento fundamental na nossa vida, e deve pensar-se e não deixar de reflectir-se

[19] Ibid 5
[20] Ibid.
[21] Ibid.
[22] Ibid 1.

sobre a sua importância, quanto aos diversos aspectos e sectores que influencia, e, neste caso particular, no âmbito da Segurança e Defesa[23].

No entanto, é uma realidade que a amplitude e o valor da informação, hoje, numa sociedade globalizante, têm impacto aos seus diversos níveis - económico, político, cultural, social e também militar. Há que considerar e reflectir quanto aos aspectos conflituais da informação, e que se enquadram no tipo de Guerra de Informação[24].

3. O CONCEITO E ENQUADRAMENTO DA GI

O conceito de GI está ligado às operações de informação, conduzidas durante o tempo de crise ou conflito para alcançar-se os objectivos específicos sobre um adversário específico ou vários. Fora da esfera militar, a GI já foi alargada e está sendo aplicada nas diversas áreas de interesse[25]. Na sua essência, é uma guerra ligada às transacções ou maneio de informação, acções que são tomadas para afectar a informação e os sistemas de informação do adversário, enquanto se defende a nossa informação e os nossos sistemas de informação.

Actualmente, a GI está sendo mais perigosa e os riscos aumentaram com o uso indevido de novas tecnologias, onde a utilização do Ciberespaço

---

[23] Ibid 5.

[24] Ibid 1.

[25] Gery, W. R., SeYoung Lee & Ninas, J. (2017). *Information Warfare in an Information Age*. JFQ 85, 2nd Quarter. USA.

constitui a nova estratégia de fazer a guerra. É um tipo de guerra que possui uma área de acção ampla e com as seguintes principais características[26,27]:

- ❖ Grande dificuldade de identificar-se o autor da agressão;
- ❖ A evolução do arsenal da GI desenvolve-se de acordo com a velocidade de surgimento de novas tecnologias de informação e comunicação (NTIC).

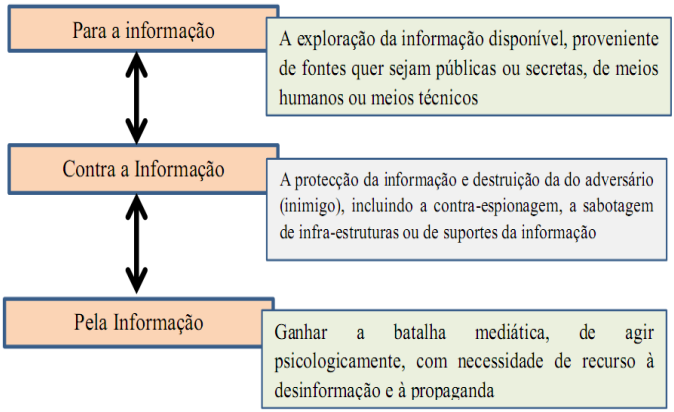

Figura 1.4. Principais características da GI. Adaptado[28]

Com a disseminação e utilização massiva das NTIC, a informação ficou mais vulgarizada, dando a supremacia do seu uso àqueles que dominam estes meios tecnológicos ou que possuem muito dinheiro

---

[26] Ibid 1.
[27] Ibid 5.
[28] Ibid 1.

para a sua aquisição[29]. A GI tem como elemento de apoio a “informação” e é complementada por três elementos, vide a Figura 1.4[30].

Até então, as definições existentes de GI estão ligadas à área militar, mas, na verdade, elas também podem ser associadas a várias outras áreas. A visão principal desta guerra é a utilização de informação e do equipamento que a manipula como ferramentas (armas) contra os adversários. Ela pode ser desenvolvida no sector industrial, onde, por meio de agentes governamentais ou privados, procura-se obter uma vantagem competitiva sobre um certo adversário[31]. No entanto, não se pode descartar que se estes espiões ou fazedores da GI escolherem como foco da sua actividade a tecnologia militar, esta situação pode criar um efeito militar directo e grave[32].

A GI não desenvolve-se com as armas de destruição física. Embora, por vezes, tal se possa verificar, a maior parte das ferramentas utilizadas na GI são de carácter não-violento, porque a informação materializa-se em dados, ainda que, à miúde, se encontrem ligados aos sistemas de informação militares[33].

Neste contexto, o que faz com que a GI se torne mais perigosa é o facto de, na actualidade, as

---

29 Kiyuna, A.; Conyers, L. (2015). *Cyberwarfare sourcebook*. [S.l.]:Lulu.com. ISBN 9781329063945.

30 Ibid 1.

31 Ibid 25.

32 Ibid 5.

33 Ibid 29.

Forças Armadas dos países industrializados dependerem dos sistemas de comunicações e equipamentos electrónicos, e, para eles, são as boas vias para a transferência rápida de dados para o campo de batalha e vice-versa[34].

No âmbito de conflito armado, a GI abrange tudo o que se possa efectuar para preservar os sistemas de informação e comunicação (da exploração), corrupção ou destruição, enquanto, simultaneamente, se explora, corrompe ou destrói os sistemas de informação do inimigo (obter a vantagem de informação - Quadro 1.1)[35]. Entretanto, ainda que, em algumas circunstâncias, se torne fundamental a utilização da força, em caso de se verificar a ocorrência de um combate, a sua utilização não é o epicentro da GI, como já foi referenciado anteriormente. A essência da guerra de informação é obter a informação mais rapidamente que o inimigo e examiná-la de uma forma mais cuidadosa e eficiente[3637].

No mais, a ideia principal da GI é utilizar a informação para derrotar ou atingir negativamente um inimigo. Por um lado, a operação é desencadeada de forma a alterar as informações do sistema de defesa do inimigo, com vista a despistá-

---

[34] Libicki, M. C. (2017). *The Convergence of Information Warfare. Strategic Studies Quarterly*.

[35] Ibid 5.

[36] Ibid 29.

[37] Neto, R. B. G. (2017). *Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interacção*. Revista Política Hoje - Volume 26.

lo e desinformar, e por outro, tratando-se de que estamos na era tecnológica, este conceito vai mais além, pois não só afecta a informação do adversário, mas também os seus Sistemas de Comunicação e Informação.

A GI é desencadeada em três componentes de operações: domínio ou exploração, defesa e ataque de informação (quadro 1.1)[38]. O domínio de informação refere-se à consciência que os utilizadores devem ter sobre a importância desta, sobretudo na criação de mecanismos tecnológicos para a sua obtenção, exploração e distribuição para acções operacionais[39]. No domínio de defesa, consiste na protecção, recuperação e detecção de toda informação estratégica ou importante para o âmbito de defesa. O último componente é a contra-informação, que consiste em negar, perturbar, destruir e explorar toda a informação do inimigo, com vista a obter uma superioridade de informação no campo de batalha[40].

A guerra de informação pode apresentar-se num prisma de âmbito restrito militar assim como da sociedade, em geral. Mas, com a aplicação do ciclo "Observar", "Orientar", "Decidir", "Agir (OODA)", desenvolvido pelo Coronel John Boyd, da Força Aérea dos EUA, como modelo de Comando e Controlo, pode concluir-se que, no âmbito restrito e

---

38 Ibid 2.

39 Ibid 34.

40 Santos, G. A. (2010). *Novo Ano, Novos Desafios: Ciberataques e Ciberdefesas*. Revista Militar. nº 2496.Portugal.

alargado, o conceito de GI está directamente ligado às acções militares (Figura 1.5)[41].

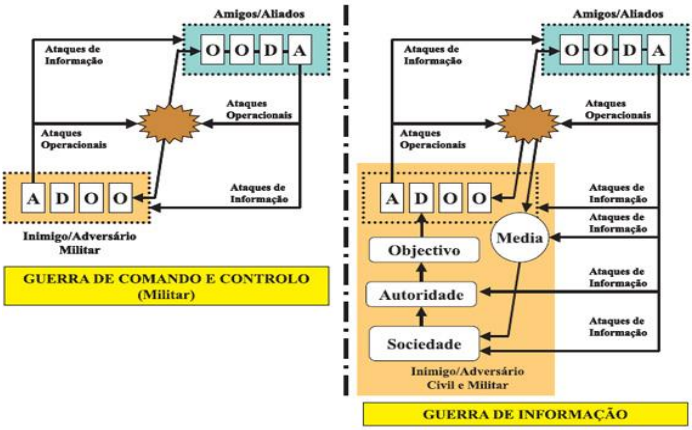

Figura 1.5. Extensão do espaço de batalha de GI[42]

Ainda da Figura 1.5, pode inferir-se que um estudo profundo do inimigo é bastante necessário em GI, pois, enquanto nos preparamos para atacar os meios de comunicação do nosso inimigo, este, por sua vez, também vai desencadeando acções contrárias. Numa perspectiva operacional, o conceito alargado de guerra de informação pode ser aplicada ao longo de todas as fases de operações, que abrangem a competição, o conflito até à guerra propriamente dita, conforme se representa na Figura 1.6 [43].

---

41 Ibid 4.

42 Ibid 1.

43 Lima, A. S. (2009). *Tecnologia de Guerra Electrónica vis à vis Uso de Ferramentas Empresariais*

Da Figura 1.6, aduz-se que as infra-estruturas políticas, económicas e físicas de muitos países pertencem ao sector privado e assim como ao sector público. Mas, a defesa dos bens que não sejam públicos ou militares, em tempo de paz, consideram-se ser uma responsabilidade conjunta e partilhada entre o sector público e o sector privado[44].

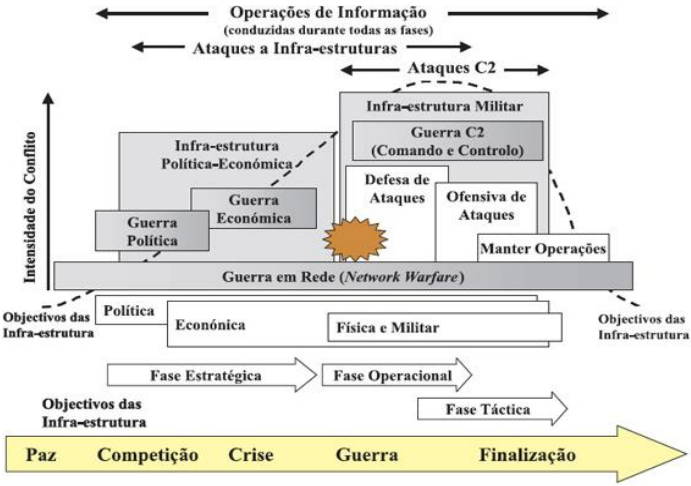

Figura 1.6. Extensão das actividades de GI[45]

Enquanto no tempo de guerra são exclusivamente os militares que protegem todos bens económicos nacionais, e uma vez que os ataques à informação ocorrem também em tempo de paz, os sectores público e privado devem

[44] Allinson, J. (2015). *The Necropolis of Drones. International Political Sociology*. Vol. 02.

[45] Ibid 43.

desenvolver uma nova relação com o sector de defesa e segurança para executarem as funções de indicação e aviso, segurança e resposta[46]. Nos EUA, este assunto está bem explícito num documento sobre a segurança do ciberespaço, publicado pela Casa Branca, em que num esforço nacional, o governo federal, convida a criação de parcerias entre o sector público e privado, e a sua participação para aumentar a consciência da segurança do ciberespaço, formar pessoal, estimular as forças do mercado, melhorar a tecnologia, identificar e remediar vulnerabilidades, trocar a informação e planear operações de recuperação[47].

A guerra de informação é um tipo de guerra especial que[48]:

- Se desenvolve num espaço de batalha quase virtual, em vez de ter lugar num campo de batalha de natureza física;
- Tem limites que não se distinguem entre os níveis de agressão e os tipos de ataques provocados pelo anonimato na rede, que complicam as

[46] Amarante, J. C. A. (2010). *A Batalha Automatizada: um sonho possível?" Cadernos de Estudos Estratégicos*. Vol. 09.

[47] Marlatt, G. E.(2008). *Information warfare and information operations: a bibliography*. Dudley Knox Library. Naval Postgraduate School Revised.

[48] Seven, C. (1996). *U.S. military opportunities: informationwarfare concepts of operation*. Brian Nichiporuk. USA.

funções de alerta e a capacidade de distinguir os ataques internos dos estrangeiros;

- ❖ É considerada como uma ajuda potencial às ameaças transnacionais, proporcionando apoio para levar a cabo ataques físicos, com armas de destruição maciça, por exemplo.
- ❖ Em operações de informação, sempre procura-se desenvolver as acções para elevar o impacto psicológico, aumentar o pânico e impedir a resposta dos serviços de emergência.

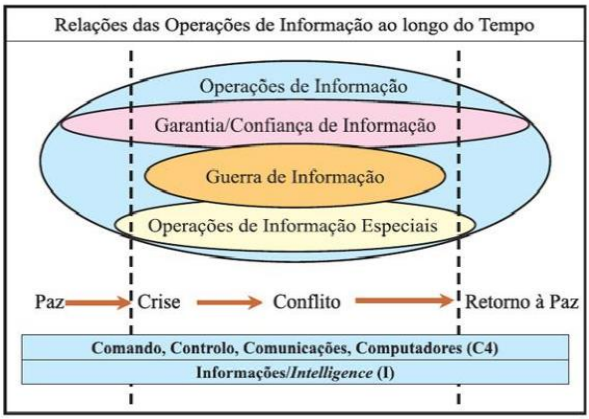

Figura 1.7. Relações das operações de informação ao longo do tempo[49]

[49] Ibid 1.

Quadro 1.1. Componentes das operações de informação[50].

<table>
<tr><td>Objectivo Inf>>>>></td><td colspan="10">SUPERIORIDADE DA INFORMAÇÃO</td></tr>
<tr><td>Contribuição da informação</td><td colspan="3">Domínio sobre a consciência/conhecimento do espaço de batalha</td><td colspan="7">Domínio sobre o controle da informação</td></tr>
<tr><td></td><td colspan="3">Consciência /Conhecimento</td><td colspan="3">Garantia/Confiança</td><td colspan="4">Contra-informação</td></tr>
<tr><td>Componentes das operações de informação</td><td colspan="3">Exploração da informação</td><td colspan="3">Defesa da informação</td><td colspan="4">Ataque da informação</td></tr>
<tr><td rowspan="2">Funções</td><td>Adquirir</td><td>Explorar</td><td>Distribuir</td><td>Proteger</td><td>Detectar</td><td>Recuperar</td><td>Negar</td><td>Perturbar</td><td>Explorar</td><td>Destruir</td></tr>
<tr><td colspan="10">  </td></tr>
<tr><td rowspan="3"></td><td colspan="3">Domínio</td><td colspan="3">Defesa</td><td colspan="4">Ofensiva</td></tr>
<tr><td colspan="3">Guerra baseada na informação</td><td colspan="7"></td></tr>
<tr><td colspan="10">GUERRA DE INFORMAÇÃO</td></tr>
</table>

[50] Ibid 1.

O que se vê na Figura 1.7 é o relacionamento, ao longo do tempo, das diversas fases de desenvolvimentos de operações de informação, com a garantia e confiança de informação, com as operações de informação especiais e com a própria guerra de informação. No entanto, este relacionamento é feito desde a situação de paz, passando pelo estado de crise, conflito até ao regresso novamente à situação de paz.

4. ENVOLVENTES DA GUERRA DE INFORMAÇÃO

A GI ajusta-se no âmbito da visão dos conflitos armados, com as determinadas especificidades perante os tipos de guerra convencionais[51]. Ela está muito associada à utilização do Ciberespaço e diz respeito as questões internacionais, numa sociedade caracterizada pela globalização, mas que afecta também o simples cidadão[52]. Isto verifica-se na actual sociedade da informação, nas suas interacções efectuadas, quer a nível profissional quer a nível individual ou familiar.

No entanto, para a informação satisfazer às necessidades actuais, ela deve circular com toda a

---

[51] Nunes, P. F. V. (2006). Operações de informação: enquadramento e impacto nacional. Revista Militar. Lisboa.

[52] Bellintani, A. e Bellintani, M. (2014). *A Guerra: do século XIX aos nossos dias*. Boa Vista: Editora UFRR.

facilidade e ser acedida em tempo real. Com isso, não se pode deixar de lado o desencadeamento de mecanismos para a sua análise e controlo, com a implementação de medidas adequadas de segurança e de protecção, as formas e condições de acesso e de disponibilidade.

A envolvente da guerra de informação apresenta-se perante um impasse: por um lado, a segurança da informação carece de medidas que devem ser tomadas ao nível internacional, de forma coordenada e em cooperação com diversas instituições públicas e privadas. Mas por outro lado, cada uma destas instituições (públicas e privadas) necessita de preservar a sua informação, muitas vezes incompatível com a colaboração e cooperação externa[53].

Entretanto, a GI é efectuada para defender os interesses políticos, diplomáticos, económicos, comerciais e financeiros, com o desencadeamento de acções relativas às operações de segurança, decepção, psicológicas, electrónicas e físicas[54]. Da Figura 1.8, pode aferir-se que esta guerra está ligada directamente com as acções de natureza militar, mas que a finalidade é defender meios e interesses de natureza económica, financeira, comercial, política e diplomática. Nela, o campo de análise é alargado e, numa perspectiva de

---

[53] Taddeo, M. (2011). *Information Warfare: A Philosophical Perspective***.** University of Oxford. Philosophy and Geography, Volume 25, 105-120.

[54] C*larke*, R. & Knake, R. *Cyberwar: the next threat to national security and what to do about i*t. New York: HarperCollins.

segurança e defesa, associa-se à segurança dos cidadãos e das instituições, e, mais estritamente, associa-se às próprias operações militares[55].

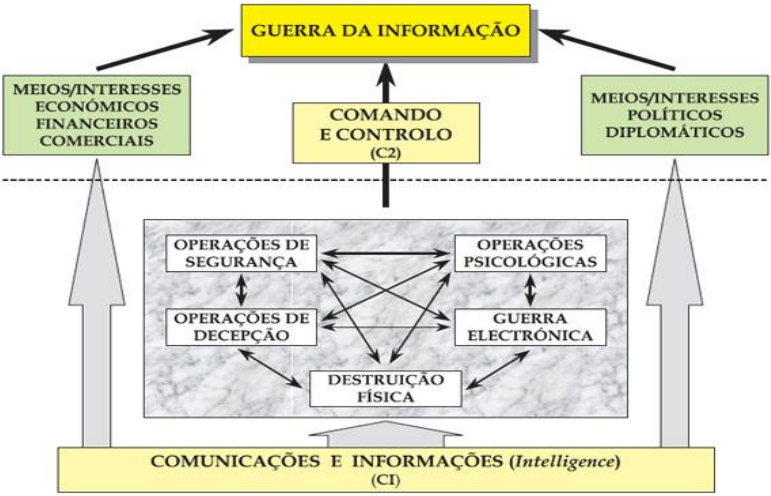

Figura 1.8. Enquadramento e envolventes da guerra de informação[56].

A GI pode apresentar diversos modos de acção, onde se destacam os seguintes[57]:

- A manipulação da informação – cuja finalidade é obrigar o adversário a tomar medidas da nossa vontade sem que se aperceba desse facto.
- A destruição da informação - que consiste em destruir (através de vírus informáticos, bombas lógicas, radiações electromagnéticas da guerra

[55] Theohary, C. A. (2018). *Information Warfare: Issues for Congress. Congressional Research Service*
[56] Ibid 52.
[57] Ibid 47.

electrónica, etc…) a informação de que o adversário (inimigo) depende.

- ❖ A desorganização de informação - com ataques concebidos para atingir um dado objectivo táctico (por exemplo, o ataque a um sistema bancário de um país inimigo).
- ❖ O ataque semântico - em que o sistema integrado de Comando do inimigo parece funcionar normalmente, mas que está a ser controlado por um operador da guerra de informação.

Contudo, quanto maior for a sofisticação de um Sistema de Informação, mais alargado será o seu âmbito de aplicação e maior a dependência da sua utilização[58]. Ainda nestes casos, maiores serão as respectivas vulnerabilidades e eventuais ameaças, pois passa a verificar-se uma maior recompensa do objectivo a alcançar por parte de potenciais adversários ou inimigos.

4.1. Combate aos sistemas de comando e controle

O combate aos sistemas de comando e controle desenvolve-se através de acções que tornem mais difícil ao inimigo controlar as suas forças através da comunicação. Para isso, exige-se uma capacidade rápida de tomada de decisões que o adversário e passar, em seguida, à acção com base nessas decisões[59]. E o ciclo de decisão não é nada

---

[58] Ibid 48.

[59] _____UNITED STATES ARMY. (2014). *Cyber Eletromagnetic Activities. FM 3-38*.

enigmático, porque é um acontecimento da nossa vida[60]. Tudo aquilo que fazemos é resultado de uma decisão, e, no meio militar, a decisão é enquadrada no acrónimo OODA (Observar, Orientar a nossa atenção para o que acabou de acontecer, Decidir como actuar e Agir) [61]. A guerra de informação pode, por exemplo, evitar que consigamos observar o inimigo, e a falta dessa informação não nos permite orientar de uma forma adequada a nossa atenção, tomar uma decisão e nem agir de forma eficaz.

A título de exemplo, pode assumir-se que um pirata informático (*hacker*) inimigo apagou alguma informação e alterou dados de forma a criar uma falsa visão sobre o que se passa no nosso campo de batalha. Após esta operação, realmente passaríamos a observar uma falsa versão da realidade e acabaríamos, de forma fatal, a tomar decisões desastrosas, como bombardear em áreas onde se supunha existir o arsenal do inimigo ou mesmo o próprio inimigo enquanto, na realidade, quem está (estava) lá é a população ou nada[62].

Também pode ter-se a informação de que o inimigo "B" encontra-se ou na hora "H" encontrar-se-ia na posição "T", uma informação que pode ser elaborada para, apenas, deslocar a nossa força para um ponto de vulnerabilidade. Daí que, realmente, é importante, antes de tomar qualquer decisão, analisar de forma cuidadosa qualquer informação na nossa posse.

---

60 Ibid 51.
61 Ibid 53.
62 Ibid 2.

4.2. Segurança operacional

Esta actividade destina-se a garantir a preservação dos segredos assim como do local onde eles residem[63]. A segurança operacional obtém-se guardando os documentos secretos em locais seguros, garantindo que as mensagens electrónicas sejam codificadas e não sejam facilmente acessíveis ao inimigo, e ainda treinando as tropas para guardarem a informação importante apenas para elas[64][65].

É importante analisar-se quem deve ter as informações, as informações que devem ser fornecidas quando estamos numa posição e com que meio ou em que via essas informações devem ser transmitidas, pois actualmente os inimigos utilizam as tecnologias para obterem as informações operacionais.

Na área dos negócios, a segurança operacional também pode ser conhecida como OPSEC (*Operational Security*) e trata-se de um conceito que está na origem de alguns dos famosos *slogans,* como: *"Loose lips sink ships"* (lábios soltos afundam navios) e "*The enemy is listening*" (O inimigo está na escuta)[66]. Em segurança operacional, recomenda-se que a informação e os meios de armazenamento,

---

63 Ibid 25.

64 Sine, J. (2006). *Definir 'Arma de Precisão' em Termos de Basear-se em Feitos. Air & Space Power.*

65 Ibid 4.

66 Ibid 34.

gestão e controlo de informação estejam na posse de militares com a extrema confiança, pois os indivíduos caçadores de informação sempre apresentam-se com boa face e como se de amigos se tratasse.

A economia e a segurança nacional (ao nível global) estão criticamente dependentes das tecnologias e são elas que controlam determinadas infra-estruturas críticas, não só a nível dos sectores públicos como também dos privados[67]. Para isso, é importante que pelo menos as infra-estruturas nacionais de informação e tecnologia vitais para a segurança e defesa sejam do domínio do sector de defesa e segurança. É sempre importante estar-se atento a actores que conduzem ou tenham a pretensão de desencadear ataques contra essas infra-estruturas, que transmitem a informação crítica e respectivos sistemas de informação. Uma pequena distração pode colocar-se em perigo o funcionamento e a prestação de serviços de primeira necessidade aos cidadãos[68].

Face às ameaças e vulnerabilidades conhecidas e associadas à prestação de serviços à comunidade, por entidades públicas ou privadas, é necessário reunir as condições para garantir com eficácia e eficiência o funcionamento dos referidos sistemas de informação, que são baseados essencialmente em complexas redes de computadores inseridos no ciberespaço, através de

---

67 Ibid 1.
68 Ibid 47.

políticas e procedimentos de protecção apropriados[69].

A Segurança de Informação (INFOSEC, sigla em inglês) consiste na protecção e defesa de informação e sistemas de informação contra acessos não autorizados ou modificação de informação, quer em armazenamento, processamento ou trânsito e contra a rejeição do serviço a utilizadores não autorizados[70]. Com a INFOSEC, conseguem-se tomar as medidas necessárias para detectar, documentar e contrariar tais ameaças de que a informação e os sistemas de informação são sujeitos.

4.3. Guerra electrónica

A Guerra electrónica (GE) é aquela que é desencadeada utilizando-se meios electrónicos, para neutralizar os sistemas de comando e controle dos inimigos, actuando-se sobre as suas comunicações e sistemas electrónicos, enquanto se assegura a integridade dos nossos próprios sistemas[71]. Ela é o resultado directo da evolução da tecnologia de detecção e comunicações, ocorrido durante e depois da segunda Guerra Mundial, uma guerra que já foi revolucionada com a invenção dos radares, aperfeiçoamento dos sistemas de

---

69 Ibid 2.
70 Ibid 34.
71 Ibid 37.

interceptação e interferência de ondas de rádio e da criptografia[72].

O espectro electromagnético é campo de batalha da guerra electrónica e os seus objectivos são distribuídos em três áreas: Medidas de Apoio de Guerra Electrónica, Medidas de Ataque Electrónico e Medidas de Protecção Electrónica[73].

Pese embora que a guerra electrónica seja classificada como o uso do espectro electromagnético, neste tipo de guerra são importantes as armas cinéticas como mísseis anti-radiação (por exemplo MAR-1 e AGM-88C) e instrumentos operacionais para suprimir fisicamente os radares[74]. Além destes, sublinhe-se que todos os tipos de veículos, navios e aeronaves militares modernos possuem uma suíte de guerra electrónica integrada. Como exemplos dos navios, temos o *Black Fox* (Israelita), para tanques de guerra, a *Spectra* do caça Francês Rafale e o sistema LIG NEX1 SLQ-200 das Fragatas sul-coreanas da classe *Sejong*[75]. No entanto, actualmente quase todos tipos dos equipamentos estão sendo preparados para a guerra electrónica. Na área de aviação, por exemplo, temos aviões radares ou com a missão específica de supressão de defesa (exemplo o EA-F18 *Growler*)[76].

---

72 Ibid 43.

73 Ibid 4.

74 Ibid 25.

75 Bastos, E. (2005). *Vietnã - Maioridade da Guerra Electrónica*.

76 Carr, J. (2010). *Inside Cyber Walfare. Sebastopol: O'Reilly*.

Figura 1.9. Navio de guerra Jamming[77]

Após o fim da 2ª Guerra Mundial, cada conflito militar exprimiu uma nova revolução na guerra electrónica e ela foi mais sentida no conflito entre o Vietname e os EUA. Este conflito foi caracterizado pelo uso intenso de radares e mísseis antiaéreos, pelos norte-vietnamitas, e mísseis anti-radiação e o desenvolvimento de uma enorme gama de sistemas de detecção, interferência electrónica e navegação por parte dos EUA[78].

Outro marco importante foi a utilização (pela Marinha israelita) combinada de contra-medidas *jamming* e mísseis anti-navio Gabriel durante a

[77] Imgem retirada em: https://www.google.com/search?q=Navio+de+guerra+Jamming&sxsrf=ALeKk02RnhIOSXlRrinMImlofJwcHJQLaQ:1624008901245&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjmmq7N8KDxAhWrhv0HHS6YD9oQ_AUoAXoECAEQAw&biw=1517&bih=694

[78] Ibid 46.

Guerra do Yom Kippur (1973), contra navios de guerra da Síria e do Egipto[79].

Os conflitos anteriores, embora marcantes para a evolução da GE, nenhum destes superou os conflitos de Iraque (1991 e 2003), que, realmente, foi sentida a evolução da guerra electrónica e os seus impactos. Durante estes conflitos, os EUA e seus aliados apresentaram em todas as dimensões do combate uma tecnologia impressionante[80].

Com efeito, na Guerra do Golfo, devido à alta tecnologia, os iraquianos foram imobilizados e incapazes de actuarem. Sensores e actuadores, operando no espectro electromagnético, interferiram nas comunicações iranianas, neutralizando sistemas de defesa e garantindo uma supremacia electromagnética com vista à anulação de pontos vitais de defesa e do sistema logístico.Como resultado, foi o envolvimento quadri-dimensional, caracterizado pelo domínio das três dimensões espaciais e da dimensão electromagnética estabelecidas pelos aliados que inibiram o poder militar de Saddam Hussein e que induziu o Iraque a um contendor cego, surdo, mudo, imobilizado e desprovido de vontade de lutar. Como consequência, os iraquianos incondicionalmente renderam-se[81].

---

79 Arquilla, J. e Ronfeldt, D. (1993). *Cyberwar is coming!* Santa Monica: Rand Corporation.

80 Carr, J. (2010). *Inside Cyber Walfare. Sebastopol: O'Reilly.*

81 Damjanović, D. Z. (2017). *Types of information warfare and examples of malicious programs of information warfare*

Figura 1.10. Avião EF - F111 Raven[82]

E mais, antes do ataque das forças de coalização ao Iraque (1993), foram introduzidos nos sistemas de defesa anti-aérea iraquiana um vírus que fornecia aos radares informações erradas e aviões especializados em guerra electrónica (EF - F111 Raven), para criar corredores por onde aviões F-16, Tornado, F-15 e F-18 penetravam no que restou das defesas inimigas, e o mesmo padrão ocorreu em 2003[83].

O que se sublinha mais nesta história é que, em vez de os americanos buscarem alvos a serem

---

[82] Imagem obtida em: https://www.google.com/search?sxsrf=ALeKk02IFYGwlrL01gDQuuix4tTQImRMqg:1624009402720&source=univ&tbm=isch&q=Avi%C3%A3o+EF+-+F111+Raven&sa=X&ved=2ahUKEwjRgr688qDxAhWK-aQKHS35DBMQjJkEegQICBAC&biw=1517&bih=694

[83] Bastos, E. (2005). *Vietnã - Maioridade da Guerra Electrónica*

meramente destruídos com os sistemas de comando e controle, passou a ser, em muitos casos, localizar e desactivar os eixos fundamentais que ligavam os sistemas e torná-los inoperantes[84]. Um cenário análogo foi visto nas redes de electricidade e de comunicação, onde, em vez de serem destruídos, foram desligados ou isolados. Após esta fase, aconteceram ataques cinéticos com mísseis de cruzeiros e ataques aéreos com bombas inteligentes contra alvos específicos, especialmente as tropas inimigas em solo[85]. Todavia, o avanço dos exércitos aliados somente aconteceu quando as forças terrestres iraquianas estavam virtualmente destruídas e sem capacidade coordenada de reacção, uma táctica que foi eleita para[86]:

- Diminuir as perdas de vidas civis, o que evitou que oficiais militares destes países pudessem sofrer processos por violarem o protocolo I da Convenção de Genebra;
- Reduzir a exposição dos soldados ao combate, que ocorre somente depois de boa parte da capacidade militar do adversário estar inoperante ou destruída;
- Diminuir os custos com o uso de bombas e mísseis inteligentes, que são cada vez mais caros e que podem ser direccionados, mais

---

84 Ibid.
85 Ibid 52.
86 Ibid 46.

efectivamente, contra as Forças Armadas adversárias;

- ❖ Permitir que as forças ocupantes possam recuperar a estrutura danificada e usar a seu favor durante a fase de ocupação e, por fim, permitir que o país, após, o conflito, possa retomar as actividades o mais rápido possível.

No entanto, a utilização da GE e das armas cibernéticas tem passado por uma forte transformação. Mesmo sendo instrumentos/armas diferentes, a sua lógica de acção e o desenvolvimento do padrão da tecnologia e das novas exigências do combate moderno têm tornado a sua separação pouco considerável, gerando uma nova abordagem chamada Actividades Ciber-Electromagnéticas[87].

4.3.1. Objectivos ou acções em Guerra Electrónica

4.3.1.1. Medidas de apoio de guerra electrónica

As medidas de apoio de guerra electrónica (MAE) são as acções levadas a cabo para detectar, interceptar, identificar ou localizar as fontes de energia electromagnética irradiada, de forma intencional ou não intencional pelo inimigo[88]. São acções de reconhecimento, vulgarmente conhecidas como acções de

[87] Ibid 46.
[88] Ibid 34.

inteligência/informações, vigilância, aquisição de objectivos/alvos e reconhecimento.

É com as MAE que são interceptadas, recolhidas, analisadas e identificadas transmissões, cujas fontes são radiocomunicações, telefonia celular, radares e comunicações por micro-ondas[89]. Em MAE são exigidas a inteligência electrónica, inteligência de comunicações e inteligência de sinais de instrumentação. Os parâmetros mais avaliados são a frequência, a largura de banda, a modulação e a polarização electromagnética[90]. Os principais objectivos em MAE são recolher as informações tácticas e estratégicas, e são operações que devem ser conduzidas por um comandante táctico com o propósito de obtenção de informações, incluindo as de natureza estratégica, destinadas à identificação, priorização, localização, neutralização e evitar as ameaças imediatas[91].

4.3.1.2. Ataque electrónico

As medidas de ataque electrónico ou ataque electrónico são acções que permitem impedir ou reduzir o uso efectivo do espectro electromagnético pelo inimigo, que também fazem parte as acções não destrutivas e destrutivas contra os sistemas inimigos, através do emprego de energia electromagnética, de energia dirigida e de armas

---

89 Ibid 2.
90 Ibid.
91 Ibid 3.

anti-radiação[92]. Os objectivos destas medidas são empastelar, decepcionar e neutralizar o inimigo.

O empastelamento ou bloqueio consiste na radiação deliberada, ré-radiação ou reflexão de energia electromagnética, com a finalidade de reduzir a eficácia dos sistemas electrónicos do inimigo, dificultando a utilização do seu espectro electromagnético[93], e abrange o uso de meios activos (ou electrónicos) e passivos (ou mecânicos). Estas medidas são, ocasionalmente, referidas como interferência, pese embora este termo se aplique mais quando se trata da degradação não intencional (por anomalia técnica ou razões acidentais) de sistemas de comunicação e radar. A decepção ou despistamento consiste na radiação, ré-radiação, alteração, absorção ou reflexão da energia electromagnética com a intenção principal de induzir o inimigo a cometer o erro durante a interpretação ou uso das informações recebidas pelos seus sistemas electrónicos, confundindo-o, distraindo-o ou atraindo-o[94]. A neutralização consiste no uso de armas de energia dirigida ou de anti-radiação, com o objectivo de danificar ou destruir os equipamentos inimigos que utilizam o espectro electromagnético[95].

4.3.1.3. Medidas de protecção electrónica

As medidas de protecção electrónica (MPE) ou contra-contra-medidas electrónica são acções

---

92 Ibid 4.
93 Ibid 43.
94 Ibid 25.
95 Ibid 2.

tendentes a garantir o efectivo uso do espectro electromagnético pelas forças amigas, contrariando as medidas de ataque electrónico levadas a cabo pelo inimigo, as acções que podem ser activas ou passivas[96]. As MPE activas consistem em acções detectáveis, tais como a alteração dos parâmetros dos equipamentos activos das forças amigas. As MPE passivas consistem em acções não detectáveis, como, por exemplo, os procedimentos ou características técnicas dos equipamentos das forças amigas.

As prioridades das MPE são a minimização da possibilidade de detecção, a protecção dos conteúdos dos sinais e a redução da susceptibilidade para com as medidas de ataque electrónico[97].

4.3.1.4. Ciberguerra

A ciberguerra é uma parte integrante da GE, guerra ciber-electromagnética em particular. A ciberguerra utiliza as ferramentas disponíveis ao nível da electrónica e da informática para derrubar sistemas electrónicos e de comunicações inimigos, e manter os nossos próprios sistemas operacionais[98].

Quase que todas as acções desenvolvidas nesta área encontram-se ainda pouco definidas, devido fundamentalmente ao facto de se verificar

---

96 Ibid 53.
97 Ibid 46.
98 Bento, A. (2008). Ciber-Guerra: Ciber-Ameaças. Lisboa

um aparecimento contínuo de novos equipamentos e de ter sido apenas recentemente que os militares começaram a encarar esta área tecnológica como uma nova forma de (fazer) guerra[99]. Alguns elementos característicos da ciberguerra aparecem à medida que os ensejos da sua utilização vão surgindo. Normalmente, os soldados envolvidos neste tipo de guerra encontram-se confinados aos centros de informação de combate, equipados com monitores, computadores e outros equipamentos de alta tecnologia, mantidos por técnicos especializados. A sua missão consiste em fazer chegar aos respectivos comandantes os dados actualizados da situação verificada no campo de batalha.

4.3.1.5. Pirataria electrónica

A pirataria electrónica (*hacking*) é uma guerra de guerrilha electrónica em que qualquer pessoa e em qualquer lugar do mundo podem participar. Tudo o que é necessário é um computador, um *modem* e alguma determinação. Este fenómeno é algo recente, devido ao facto de apenas há uns anos para cá ter-se assistido à introdução de redes de computadores internacionais a que praticamente qualquer pessoa pode aceder[100]. A internet constitui o melhor exemplo desta situação e uma grande quantidade de programadores, técnicos e curiosos da informática, com tempo disponível e intenções

[99] Ibid 4.
[100] Ibid 55.

maldosas, cruzam as redes de computadores à procura de falhas ou quebras de segurança dos sistemas de informação, quer das Forças Armadas assim como das grandes empresas.

Há mais de uma década que esta situação verifica-se de forma consistente, aproveitando alguma falta de organização existente na estrutura das redes governamentais e de algumas empresas[101]. Ao longo desta última década têm sido efectuadas algumas tentativas para transformar o problema dos *hackers* numa "arma militar". Todavia, do momento este tipo de guerra parece uma ficção, mas muitos países já estão trabalhando no sentido de tornar este cenário real no próximo conflito em que participarem. Do momento a pirataria electrónica constitui uma estratégia de acção muito atractiva para o terrorismo internacional.

4.3.1.6. Bloqueio de informação

Devido à extrema importância que a informação actualmente assume, torna-se possível efectuar um autêntico "bloqueio de informação", abatendo os satélites e destruindo as ligações por cabo e as torres de microondas que canalizam a informação para o interior do território inimigo[102]. Espera-se que, no futuro, esta situação seja extremamente difícil de superar, especialmente nas áreas mais técnicas.

---

[101] Ibid 47.
[102] Ibid 51.

4.3.1.7. Guerra psicológica

Constitui o objectivo desta guerra difundir a informação enganosa, destinada a desmoralizar o inimigo[103]. No entanto, o aspecto mais importante a considerar na GP é como se utiliza a informação como uma arma contra as forças inimigas. Dentro do contexto da guerra psicológica, pode actuar-se sobre a informação que circula nos sistemas inimigos, vedando-lhe a utilização, ou defender-se contra este tipo de acções, tentando eliminar a informação manipulada pelo inimigo por via computador, telefone ou mesmo por qualquer outra via de forma camuflada[104].

A Guerra do Golfo, citada frequentemente como a primeira guerra de informação, constitui um bom exemplo ilustrativo deste tipo de acções. A coligação aliada levou a cabo uma campanha de guerra psicológica extremamente eficiente sobre as forças iraquianas, onde muitos soldados com veemência se renderam. Tratou-se de uma acção planeada, uma vez que os panfletos lançados sobre as tropas iraquianas lhes transmitiram exactamente como se deveriam render e demonstravam as vantagens de se renderem (tornando-se hóspedes de honra dos sauditas) [105]. Como reforço desta operação, os meios de comunicação social foram também utilizados por ambas as partes, procurando

[103] Ibid 37.
[104] Ibid 2.
[105] Ibid 37.

influenciar a disposição para o combate das forças inimigas.

Figura 1.11. Exemplo de uma acção psicológica[106].

Em Moçambique, os cenários iguais também são vividos, ou seja, as redes sociais estão a desempenhar um grande papel para a desinformação. A título de exemplo, no princípio de Setembro de 2019, numa tentativa de decepcionar os fazedores da campanha eleitorais e a população, em geral, nos *Facebooks* e *whatsaps* dos moçambicanos inundou uma mensagem a desinformar que o Nhongo atacou uma brigada de campanha eleitoral da FRELIMO (Figura 1.11).

Sem dúvida, a mensagem terá sido esboçada com o objectivo de enfraquecer a campanha eleitoral, afectando psicologicamente os

[106] In Facebook

moçambicanos, principalmente os apoiantes da FRELIMO.

4.3.2. A convergência entre a Guerra Electrónica, Cibernética e Ciberguerra

Para uma boa implementação das operações Ciber-electromagnéticas e alcance dos efeitos desejados em apoio às operações terrestres unificadas, os comandantes, apoiados por suas equipes, devem integrar e sincronizar as operações do ciberespaço, a guerra electrónica, as operações de gestão do espectro e as capacidades relacionadas[107].

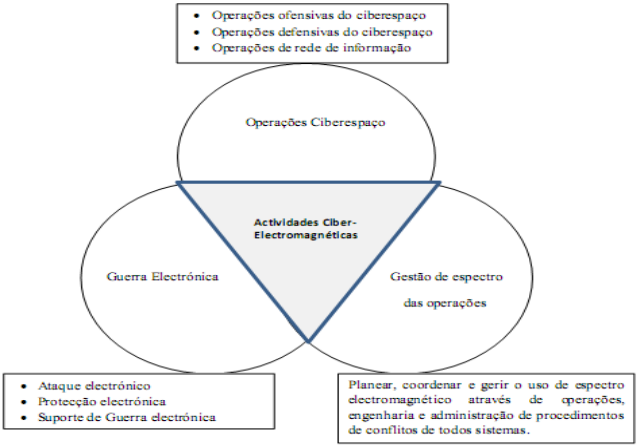

Figura 1.12. Actividades Ciber- Electromagnéticas[108].

[107] Ibid 59.
[108] Ibid.

As actividades Ciber-electromagnéticas são consequência da mais nova abordagem de interacção entre as diferentes formas de acção militar, uma guerra centrada em rede[109]. Trata-se de um conceito que teve origem nas Forças Armadas norte-americanas e é uma nova direcção na forma como as forças terrestres devem operar o ciberespaço e o espectro electromagnético.

O ciberespaço e as emissões electromagnéticas do momento são os principais meios de transmissão de informações e conhecimento, sejam elas individuais, colectivas, civis, ou militares[110]. E denota-se que existe uma ampla convergência tecnológica entre computadores, comunicações, equipamentos electrónicos, *software* e criptografia, ou seja, as redes de computadores e de comunicação tornaram-se a mesma coisa[111].

Em termos mais simples, a guerra centrada em rede (Ciber-electromagnética) é aquela que busca utilizar toda a tecnologia electromagnética e de rede para conseguir a maior consciência situacional (domínio de informações) no campo de batalha, permitindo maior conhecimento da evolução do conflito e sincronização das acções e, ao mesmo tempo, impedir que o adversário tenha acesso ao seu arsenal de guerra electrónica e cibernética[112].

---

[109] Ibid.
[110] Ibid 53.
[111] Ibid 25.
[112] Ibid 59.

Todos os elementos das forças, tais como soldados, navios, aviões, helicópteros, etc... fazem parte desta rede, trocando informações em tempo real[113]. A guerra centrada em rede busca o total domínio informacional e cognitivo. Os elementos centrais desta abordagem são: troca de informações através de rede wireless, computadores, criptografia, data *link*, furtividade, detecção antecipada, comando descentralizado e uso de armas inteligentes. A guerra deixa de ser centralizada e hierarquizada para ser integrada.

Os novos riscos à segurança cibernética, advindos do uso intensivo da tecnologia *wireless*, trazem à guerra electrónica ameaças antes impensáveis. Em 2014, cientistas da Universidade de Liverpool conseguiram criar um vírus conceito (Chameleon) que pode ser transferido via redes *wifi* abertas e não mais apenas entre computadores ou por meio físico[114]. Este *malware*, depois de conectar- se a um ponto, espalhou-se rapidamente por outras redes, atacando *rooters e* colectando informações dos seus usuários. Um vírus deste tipo poderia, se direccionado, atacar sistemas de data *link* contaminando toda uma rede, inviabilizando a troca de informações e negando completamente o conhecimento situacional no campo de batalha[115].

A importância das redes de computadores, *softwares*, a dependência cada vez maior da comunicação wireless e da criptografia para as

---

[113] Ibid 98.

[114] Ibid 5.

[115] Ibid 29.

Forças Armadas no mundo tem aumentado bastante a zona cinzenta que separava a guerra electrónica da guerra cibernética[116]. Conceitos, antes vistos como ambientes completamente diferentes, têm sido percebidos cada vez mais como partes de uma mesma forma de conceber a guerra.

Além disso, a possibilidade da utilização de técnicas de emissão electromagnética para permitir o roubo de informações em computadores através de modens e *rooters wifi* abre novos desafios à tecnologia de encriptação de dados como os de data *link*[117]. É claro que o facto mais importante é a necessidade de os comandantes terem o máximo de informação possível em tempo real, serem capazes de processar esta avalanche de informações e tomar a decisão que acreditam ser a mais correta para chegar ao único objectivo que importa: vencer a guerra.

5. OPERAÇÕES E ARMAS DE GI

5.1. Operações em GI

As acções de guerra de informação podem ser concretizadas graças aos apoios das informações (*Intelligence*) e das Comunicações, elementos essenciais e críticos para se poder executar OpInfo, quer de natureza ofensiva ou defensiva[118].

---

116 Ibid 48.

117 Ibid 51.

118 Ibid 1.

As OpInfo ofensivas incluem operações de segurança (OPSEC), decepção militar, operações psicológicas, guerra electrónica (GE), ataque/destruição física e operações especiais de informação, podendo também incluir ataques a redes de computadores[119]. As OpInfo defensivas são conduzidas através de garantia da informação, segurança física, segurança de operações, contra decepção, contra propaganda, contra informações, guerra electrónica (GE) e operações especiais de informação.

A nomenclatura GI aplica-se a três domínios da sociedade (Quadro 1.2)[120]:

- Pessoal;
- Corporativo (ou institucional); e
- Nacional (ou global).

Do quadro 1.2 pode inferir-se que a GI possui três componentes operacionais, nomeadamente: exploração, defesa e ataque de informação. A exploração refere-se à análise que deve ser feita para com a informação obtida, para que se tome uma decisão genuína e na hora certa. Enquanto a defesa e o ataque são acções que garantem a segurança e a fiabilidade da nossa informação e a confiança que ela nos oferece quando empregada em acções ofensivas.

---

[119] Ibid 47.
[120] Ibid.

O conceito de GI apresenta três aspectos principais[121]:

- O domínio da informação;
- A protecção da informação; e
- Ataque à informação

Porém, para o alcance do sucesso em GI e em quaisquer outros tipos de guerra, é necessário manter a superioridade de informação. Neste caso, qualquer guerra moderna deve ser baseada na informação e é essa informação que contribui para ter-se uma consciência e conhecimento dominantes do campo de batalha, através da sua aquisição, processamento, distribuição e exploração[122].

Na actualidade, a GI constitui uma grande preocupação para qualquer sector de defesa, porque, com a massificação das tecnologias, reduziu-se o poder do controlo e protecção da informação e, para minimizar os danos, estão sendo desenvolvidas acções para incrementar as medidas para sua protecção.

Qualquer força que possui o controlo da informação marca a diferença perante os seus adversários, pois possui um melhor conhecimento sobre o espaço de batalha em que opera[123].

---

[121] Ibid 1.
[122] Ibid 48.
[123] Ibid 1.

Quadro 1.2. Domínio de conflitos e alguns exemplos de agressões[124].

DOMÍNIO DE CONFLITO	ALGUNS EXEMPLOS DE AGRESSÕES DE INFORMAÇÃO
Nacional (Global e sector público)	❖ Guerra na rede, económica, política e de comando e controlo
Corporativo (institucional e sector privado)	❖ Espionagem e sabotagem de fontes de informações e informação por agentes internos e externos da organização; ❖ Destruição e roubo de meios das comunicações incluindo computadores; ❖ Incêndio premeditado;
Pessoal (sector pessoal)	❖ Fraude de comércio electrónico; ❖ Difamação e desinformação por via da rede, incluindo as sociais; ❖ Escutas telefónicas e intercepção de telemóveis; ❖ Imitação e roubo de cartões bancários; ❖ Roubo de PINs e base de dados ❖ Destruição de computadores

O controlo da informação consegue-se através de operações defensivas (defesa) e ofensivas (ataque) de informação. As operações defensivas permitem obter garantia e confiança na respectiva informação através de medidas de protecção, detecção e recuperação da própria informação.

[124] Ibid 1.

Enquanto as operações ofensivas (de ataque) de informação tem-se como objectivo atacar (com acções de contra-informação) para negar, perturbar ou explorar a possibilidade de utilização da informação ou destruir a informação do adversário[125].

A GI é uma guerra que apresenta três propriedades essenciais de segurança para uma infra-estrutura de informação (info-estrutura) e os respectivos objectivos das contra-medidas para cada uma delas[126]. A info-estrutura deve apresentar características e propriedades de segurança adequadas para que se acautelem aos efeitos dos objectivos da GI e assim se permita a disponibilidade, a integridade e a confidencialidade de informação aos órgãos que necessitam de a utilizar de forma eficiente e com eficácia[127]. Mas uma informação proveniente ou manipulada num computador ou numa rede de computadores só é segura se satisfizer aos três requisitos básicos anteriores (disponibilidade, integridade e confidencialidade).

5.2. As armas em GI

Muito tem sido recentemente escrito sobre as várias formas que uma guerra de informação poderá adoptar[128]. Dentro deste âmbito são desenvolvidos

---

[125] Ibid 43.
[126] Ibid 79.
[127] Ibid 1.
[128] Ibid 80.

cenários que envolvem guerras de *hackers,* guerra electrónica, bloqueios de informação, etc[129]. Este tipo de aproximações é resultado de uma análise vertical que tem na sua origem apenas algumas capacidades específicas, não existindo uma aproximação sistemática a uma taxonomia ajustada às armas da GI.

Quadro 1.3. Matriz das Armas da Guerra de Informação[130].

Efeito das armas	Foco do atque	Efeito primário	Tipo de armas	Complexidade do modelo
Físico	Físico	Negação do serviço	Destruição física	Baixa (linear)
Sintaxe	Estrutural	Obstrução e corrupção operacional lógica	Vírus, agentes e Filtros	Média
Semântica	Comportamental	Afetação da confiança dos utilizadores dos sistemas	Simulação de uma falsa realidade e Informação multimídia enganosa	Elevada (Caótica)

Actualmente, existem três grandes classes de armas susceptíveis de serem utilizadas para empreender uma GI, cujos efeitos podem ser físicos (estratégias para a não fácil acessibilidade dos nossos sistemas de informação e comunicação), de sintaxe (ataque funcional dos sistemas), ou semânticos (ataque psicológico) (quadro 1.3).

[129] Ibid 48.
[130] Ibid 51.

5.2.1. Efeito físico da GI

A maior acção deste efeito é criar um sistema de comunicação que não seja acessível por indivíduos desconhecidos ou sem autorização[131]. Por sua vez, esses indivíduos não autorizados, utilizando as suas habilidades técnicas, fazem proveito das tecnologias para acederem aos sistemas dos outros. No entanto, porque também os inimigos possuem grandes engenheiros, controlar este efeito torna-se difícil, e a maior solução é aquisição de equipamentos de protecção adequados[132]. Para os equipamentos que funcionam em rede é necessário bloquear as entradas através da utilização de *firewalls* de fabrico ou fornecidos pelas empresas de alta confiança, sem deixar de lado o pensamento de que, neste momento, quase que não há nenhuma ferramenta eficiente contra o efeito físico, embora haja evidências do empenho das áreas académica e industrial na busca de soluções para evitar e mitigar tais ataques[133]. No mais, os instrumentos existentes apenas atenuam os ataques pouco refinados e sendo que, na maioria, os ataques físicos são bem-sucedidos[134]. Actualmente, consegue-se entrar nos sistemas dos outros por via de uma mensagem que parece benéfica, mas com intenção maléfica e, em

---

131 Ibid 54.
132 Ibid 1.
133 Ibid.
134 Ibid 54.

algumas situações, essas mensagens, de forma propositada, são enviadas para constranger com veemência os sistemas de comunicação dos inimigos.

Para o sector de defesa e segurança, o mais importante é prevenir-se, actualizando regularmente os seus *softwares, para* suportar um ataque sem prejudicar os seus usuários legítimos, e aprimorar regularmente as habilidades dos seus técnicos. São medidas que devem ser frequentes, pois cada dia que passa surgem novas vulnerabilidades e, mesmo em sistemas de comunicação superdimensionados, não é possível garantir a imunidade quando o tráfego de ataque é gerado por diversos atacantes[135].

Para a remediação dos efeitos físicos é importante, por um lado, aprimorar as infra-estruturas tecnológicas que garantem a defesa e segurança, avaliando-as sob ponto de vista do seu funcionamento, confiabilidade e prontidão, incluindo aqueles que dependem das radiações para o seu funcionamento. Por outro, é importante aprimorar regularmente os conhecimentos dos engenheiros e técnicos existentes no sector de defesa e segurança, o que inclui a revisão dos curriculas dos cursos militares, pois só os técnicos bem treinados serão capazes de mitigar este tipo de efeitos.

---

[135] Ibid 29.

5.2.2. Efeito de sintaxe

"Comunicações sem inteligência são ruído; Inteligência sem comunicações é irrelevante".[136]

A arma de sintaxe tem como objectivo atacar a lógica operacional de um sistema de informação, introduzindo atrasos ou comportamentos inesperados no seu funcionamento[137]. Esta classe de armas procura adquirir o controlo ou desactivar a lógica das redes e dos sistemas de informação visados. Com a utilização do *software* do sistema operativo ou das outras ferramentas do sistema, o vírus pode fazer com que o sistema actue de forma diferente da prevista ou sofra grandes retardações na sua execução e funcionamento[138]. Tal como as outras armas, o seu efeito também é perigoso, porque pode facilmente obstruir e corromper a operação lógica de qualquer sistema de comunicação[139]. Como medida, é importante implementar ou adoptar as medidas de segurança nos equipamentos tecnológicos em uso. E o sector de defesa e segurança, em particular, antes de adquirir qualquer equipamento tecnológico para o seu uso, deve questionar-se o seguinte[140]:

- Que tipo de equipamento tecnológico se pretende adquirir ou a adquirir?

---

[136] Ibid 51.
[137] Lima 43.
[138] Ibid 3.
[139] Ibid.
[140] Ibid 15.

- Que tipo de informação ou dados vão ser produzidos, armazenados, geridos e transmitidos no equipamento que se pretende adquirir?
- Como será adquirido? Quem está ou vai fornecer o equipamento?
- No caso de doação. Quais são as possíveis intenções dos doadores?
- Quem desenvolveu (no caso de *software)*?.
- Quem vai fazer a gestão, manutenção e reparação?
- Qual é o conhecimento técnico dos militares (usuários e gestores)?

Porém, uma vez satisfeitas as questões acima descritas, é possível controlar os efeitos desta arma. No caso vertente dos quartéis, o mais essencial é - por difícil que pareça - , criar-se condições para que os meios tecnológicos sejam controlados, programados e reparados pelos militares preparados tecnicamente, sem excluir os aspectos éticos[141]. O contrário disso é expor as vulnerabilidades dos sistemas de informação e comunicação, “entregar de bandeja” as informações ou dados aos indivíduos desconhecidos, para além das facilidades e oportunidades que os mesmos terão para alterar qualquer informação ou viciar o funcionamento dos sistemas[142].

---

[141] Ibid 3.
[142] Ibid 15.

Por um lado, reconhece-se que o equipamento tecnológico é caro e, muitas vezes, as Forças Armadas das nações não desenvolvidas dependem estritamente dos países desenvolvidos para o seu apetrechamento tecnológico. E este cenário torna-as mais vulneráveis, porque, às vezes, por falta de militares capacitados, os doadores indicam os seus técnicos para a manutenção e reparação dos equipamentos.

A dependência dos sistemas de comunicações civis é outro cenário que pode colocar na situação de vulnerabilidade as Forças Armadas[143]. É verdade que, a esse respeito, pode faltar dinheiro para que se estabeleça um sistema de comunicação para as FADM, mas nada obsta, por questões estratégicas e de segurança, colocar alguns militares a trabalharem nas instituições civis estratégicas, como nas telecomunicações ou no Instituto Nacional das Comunicações de Moçambique[144].

O mais inquietante ainda é o facto de, mesmo com tantas instituições de ensino militar e tantos militares formados no estrangeiro na área de tecnologias, para estabelecer-se ou fazer-se a manutenção de uma simples rede de computadores num quartel, por exemplo, depender-se de civis ou militares estrangeiros. E isto chama a atenção para a necessidade de os programas dos cursos das instituições de ensino militar serem revistos, para que estejam de acordo com a nova realidade, pois estamos numa era em que, por força da evolução

[143] Ibid 25.
[144] Ibid 15.

tecnológica, podemos ser aniquilados severamente por um inimigo que esteja desencadeando as suas operações remotamente.

Entende-se, também, que valorizar os conhecimentos tecnológicos modernos, nos cursos actuais, é assumir que estamos atentos aos efeitos das armas de GI[145]. Para os cursos do exterior, é importante, por um lado, junto aos parceiros, escolherem-se ou negociarem-se aqueles que respondam aos desafios actuais de interesse para as FADM. Por outro, é necessário seleccionar candidatos competentes e comprometidos com a causa nacional e que estejam profissionalmente ligados às tecnologias de comunicação.

Ainda no âmbito da formação, é pertinente que alguns cursos relacionados com a segurança de informação deixem de depender tanto dos estrangeiros. Para isso, devem potenciar-se os quadros formados nas nossas instituições militares de ensino e formação, sem excluir os que, anualmente, são formados no estrangeiro. O que acontece é que, durante o processo de formação, os estudantes realizam pesquisas nos quartéis, de ondem trazem resultados que, de certo modo, podem expor o potencial tecnológico nacional ou ideologias tecnológicas. E, muitas vezes, o inimigo é um individuo sem rosto.

---

145 Ibid 34.

5.2.3. Efeitos de semântica

Esta acção tem como efeito primário afectar a confiança dos utilizadores dos sistemas, tendo como arma a simulação de uma falsa realidade e informação multimídia enganosa[146]. Trata-se de mais uma arma perigosa, e, para a sua mitigação, os técnicos devem ser preparados psicologicamente, em matéria de preservação de informação estratégica militar perante os indivíduos de conduta duvidosa, para que não sejam influenciados a interpretarem de forma errónea as informações que circulam nos sistemas e a desacreditarem a qualidade do próprio sistema.

Neste efeito, a maior preocupação dos indivíduos mal-intencionados é influenciar os operadores dos sistemas de informação - às vezes, com promessas de melhorá-los -, a interpretarem a informação de forma errada ou de forma fluente de modo a que o adversário tenha toda informação que lhes interessa.

A complexidade associada à arma semântica é elevada, porque ela não procura afectar o sistema de informação, mas sim o comportamento dos seus utilizadores, influenciando-os nas suas decisões[147]. No entanto, num futuro próximo, os sistemas de informação, em ambientes multimídia, constituirão a principal ferramenta de gestão de informação e o utilizador terá de confiar ainda mais em processos automatizados para procurar, aceder, compilar e

---

[146] Ibid 2.
[147] Ibid 51.

apresentar a informação durante a fase crítica de processamento intensivo da informação que, em geral, ocorre numa situação de crise[148]. O perigo ou oportunidade para com esta arma reside no facto de o que acreditamos ser uma informação objectiva residir sempre num ponto de vista específico e ser aberto à manipulação[149], uma situação que pode afectar de forma determinante o funcionamento correto do ciclo de decisão de qualquer força militar.

A tecnologia associada às armas da GI não constitui actualmente um factor limitador, pois a sua limitação de utilização deve-se apenas à existência de alguma falta de conhecimento organizacional, doutrinário e legal sobre estes assuntos[150].

A definição da forma de utilização de cada uma das armas da GI, em termos defensivos ou ofensivos, faz surgir uma discussão sobre a legitimidade das actividades classificadas como acções de GI[151]. Entretanto, os EUA resolveram este dilema separando a guerra de informação em dois componentes distintos: guerra de informação ofensiva (GIO) e guerra de informação defensiva (GID).

E os militares norte-americanos estão especialmente empenhados no desenvolvimento de uma capacidade defensiva, e esta opção é encarada como aceitável, sendo por muitos

---

148 Ibid 40.

149 Ibid.

150 Waltz, K. N. (1988). *The Origins of War in Neorealist Theory". Journal of Inter- disciplinary History*, vol. 18

151 Ibid 59.

classificada como uma actividade de GI legítima[152]. No entanto, a condução de acções de GI defensiva não nega a necessidade do desenvolvimento de processos de pesquisa e de acções de contornos agressivos[153].

Estas capacidades são activadas devido à exigência de se saber até que ponto existem vulnerabilidades dentro dos seus próprios sistemas[154]. O que é real é, somos levados a concluir que o desenvolvimento deste tipo de acções requer uma capacidade de GI ofensiva. Assim, se se falar de GI defensiva, sem se referir também à GI ofensiva, está-se examinando apenas uma das faces da moeda e desprezando a sinergia que se exige de quem pretende manter uma superioridade estratégica na GI[155].

Uma capacidade de análise de vulnerabilidades constitui um dos meios que asseguram que um sistema de informação foi configurado de forma eficiente e segura[156]. E classificar as redes de acordo com a sua dimensão, localizar todos os seus elementos estruturais, determinar todos os pontos de acesso, instalar sensores para efectuar a monitorização e exploração dos processos são algumas das actividades essenciais que têm de ser executadas para concretizar uma correta análise de vulnerabilidades. Para a simulação e a realização de

---

[152] Ibid 54.
[153] Ibid 59.
[154] Ibid 4.
[155] Ibid 150.
[156] Ibid 25.

jogos de guerra (*wargaming*), a GI defensiva precisa de uma capacidade de GI ofensiva, para alcançar um nível de gestão de risco relativamente seguro[157].

6. DIMENSÃO ESTRATÉGICA DA GI

O termo "guerra de informação" tem vindo a ser utilizado cada vez mais para designar, de forma abrangente, um amplo conjunto de conceitos ligados ao fenómeno da guerra da era da informação[158]. Esses novos conceitos emergentes da guerra estão directamente relacionados com a perspectiva de que a evolução rápida do ciberespaço e a infra-estrutura de informação global podem trazer tanto novas oportunidades como novas vulnerabilidades. Alguns autores salientam que uma dessas vulnerabilidades é o facto de que esta situação possa pôr em risco recursos nacionais de grande valor, tradicionalmente situados fora do campo de batalha e do teatro de projecção do poder de um país, de tal forma que afecte tanto a sua estratégia militar como a sua estratégia de segurança nacional[159]***.***

A guerra de informação é reconhecida pelo seu carácter dinâmico, tal que existe um elemento emergente que parece ser comum a quase todas as utilizações desta guerra, que está evoluindo de forma contínua. Classifica-se este domínio

---

[157] Ibid 3.

[158] Ibid 2.

[159] Allinson, J. (2015). *The Necropolis of Drones.* International Political Sociology. Vol. 02.

emergente do conflito em que as nações usam o ciberespaço para afectar operações militares estratégicas e infligir danos nas infra-estruturas de informação nacional, como guerra de informação estratégica, conforme se pode observar na Figura 1.13[160].

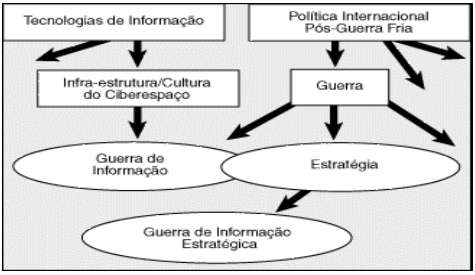

Figura 5.13. GI Estratégica[161].

Acredita-se que a GI estratégica justifica uma atenção e reconhecimento especial como uma legítima nova face da guerra, com profundas implicações*.*

Ultimamente, a nova cultura e infra-estrutura do ciberespaço tem evoluído quase que exclusivamente fora do contexto militar, e sendo que a internet é aquela que trouxe mais novas oportunidades para a execução da guerra de informação[162]. Paralelamente, assiste-se à contínua evolução da política internacional e, dentro desse contexto, é visível a evolução da GI como um

[160] Ibid 4.
[161] Ibid 2.
[162] Ibid 34.

instrumento da política, onde os políticos fazem o uso de quase todas as potencialidades tecnológicas para atingirem os seus objectivos. Pode citar-se o uso de medias e das redes sociais, tópicos em discussão na parte 2 do presente livro.

Neste ambiente, surgem, naturalmente, novos interesses para as várias nações, produzindo-se novos dilemas e novos alvos estratégicos sobre os quais se deve exercer influência, inclusive com a ameaça do emprego de novos (e velhos) tipos de forças estratégicas[163]. E, desta maneira, nascem novas ameaças e vulnerabilidades estratégicas. Agora, torna-se cada vez mais claro que a evolução da guerra estratégica incluirá uma dimensão de ameaças e vulnerabilidades no ciberespaço dignas de serem classificadas como “GI estratégica.

6.1. GI estratégica

Actualmente, a maior parte dos países industrializados, como os EUA, já contam com um expressivo número de recursos baseados em informação, inclusive sistemas complexos de gestão que abarcam o controlo do fornecimento de energia eléctrica, do fluxo de circulação da moeda, do tráfego aéreo, do petróleo, do gás e de outros artigos dependentes da informação[164][165]. Os aliados

---

163 Ibid 4.

164 Ibid 2.

165 Van, C. M. (2010). *Technology and War: from 2000 BC to the present*. New York: Free Press.

e possíveis parceiros de coligação dos EUA encontram-se igualmente dependentes de várias infra-estruturas de informação[166]. Conceptualmente, quando um potencial adversário tenta danificar esses sistemas, por meio de técnicas de guerra de informação, esta assume inevitavelmente um aspecto estratégico.

Alvos estratégicos situados nos EUA podem ser tão vulneráveis a este tipo de ataques, como os alvos dos seus sistemas C3I (comando, controle, comunicações e inteligência) posicionados no teatro de operações[167].

Quando se responde a ataques de GI deste tipo, a estratégia militar não se pode dar ao luxo de ter como foco na condução e apoio de operações apenas à sua região de interesse[168]. E, actualmente, é necessário examinar com rigor as implicações da GI nas infra-estruturas existentes e que se encontram dependentes de uma livre gestão de informação.

6.2. Envolventes da GI estratégica

As redes que se encontram interligadas entre si estão sujeitas a ataques e interrupções, não apenas por parte de Estados constituídos, mas também por

---

166 Ibid 34.
167 Ibid 53.
168 Ibid 150.

parte de organizações privadas, incluindo grupos dispersos e até mesmo indivíduos[169].

Acredita-se que o grau de dificuldade de acesso aos sistemas, sugerido nos vários tipos de ataques de guerra de informação, poderá subir se for negado o fácil acesso às redes e sistemas de controlo, através da exploração de novas técnicas de criptografia por *software*. Reconhece-se ainda que tal facto poderia mitigar algumas ameaças, mas chamam a atenção para o facto de que esta abordagem não removeria outras ameaças a um sistema de rede feitas por um operador corrupto, um ataque físico directo ou ambos[170]. Igualmente, aumentaria na sua natureza (estratégica, operacional e táctica) a dificuldade do desenvolvimento de acções de *intelligence* relativamente aos adversários da GI estratégica[171].

A grande variedade de possíveis inimigos, armamentos e estratégias dificulta cada vez mais a distinção entre as fontes interna e externa de acções e ameaças de guerra de informação. A característica desta guerra apresenta fundamentalmente novos problemas num ambiente do ciberespaço. Um problema básico é distinguir entre um ataque e outros acontecimentos, tais como acidentes, falhas de sistemas ou acções de *hackers*[172]. A principal consequência desta

[169] Ibid 34.
[170] Ibid 34.
[171] Ibid 2.
[172] Ibid 40.

característica da GI estratégica é a de que eventualmente não se consiga detectar quando um ataque está ocorrendo, quem está atacando ou como o ataque está sendo conduzido[173]. Outra consequência da indefinição da ameaça é o desaparecimento de uma identificação clara dos diferentes níveis de acções anti-Estado, que variam desde o crime até à guerra.

Em virtude desta indefinição, nações-Estado contrários aos interesses estratégicos de um dado país poderiam abster-se de realizar acções militares ou terroristas tradicionais, e ao invés disso, explorar indivíduos ou organizações criminosas transnacionais destinadas a conduzir operações criminosas[174], provavelmente o que está acontecendo em Cabo Delgado.

Existe também uma possibilidade progressiva de que agentes da GI manipulem a informação-chave destinada à difusão pública. Por exemplo, grupos políticos e outras agências não-governamentais podem usar a internet para galvanizar o apoio político[175].

Existe ainda a probabilidade de os factos de um determinado acontecimento serem manipulados e amplamente disseminados, utilizando-se técnicas de multimídia[176]. O certo é, poderá existir uma reduzida capacidade de construir e manter o apoio interno das populações, para o desenvolvimento de

---

[173] Ibid.
[174] Ibid 4.
[175] Ibid 40.
[176] Ibid 40.

acções políticas controversas, levadas à cabo pelos seus governantes. E uma boa possibilidade de se conseguir gerir convenientemente este problema passa pela utilização da internet como parte de qualquer campanha de informação pública.

7. REFERÊNCIAS

UNITED STATES ARMY. (2014). *Cyber Eletromagnetic Activities. FM 3-38*. Acedido no dia 28 de Abril de 2018 em :< http:// ar-mypubs.army.mil/doctrine/DR_pubs/dr_a/pdf /fm3_38.pdf >

Amarante, J. C. A. (2010). *A Batalha Automatizada: um sonho possível?" Cadernos de Estudos Estratégicos*. Vol. 09.

Allinson, J. (2015). *The Necropolis of Drones.* International Political Sociology. Vol. 02.

Arquilla, J. e Ronfeldt, D. (1993). *Cyberwar is coming!* Santa Monica: Rand Corporation.

Bastos, E. (2005). *Vietnã - Maioridade da Guerra Electrónica*. Acedido no dia 20 de Novembro de 2018 em: http:// www.ecsbdefesa.com.br/fts/Vietn%E3.pdf >

Bento, A. (2008). *Ciber-Guerra: Ciber-Ameaças.* Lisboa. Acedido no dia 27 de Julho de 2019 em: https://comum.rcaap.pt/bitstream/10400.26/8059/1/Microsoft%20Word%20-%20TIA.pdf

Bellintani, A. e Bellintani, M. (2014). *A Guerra: do século XIX aos nossos dias*. Boa Vista: Editora UFRR.

Carr, J. (2010). *Inside Cyber Walfare. Sebastopol: O'Reilly.*ho, P. J. S. (2015). *A utilização das redes sociais por elementos militar: o uso*

Chapala, N.M. (2021). Efeitos Físicos, Sintaxe e Semânticos da Guerra de Informação na era Tecnológica: Ameaças e Desafios para as Forças Armadas de Defesa de Moçambique. Revista Científica do Instituto Superior de Estudos de Defesa Tenente-General Armando Emílio Guebuza: Série Defesa & Segurança: Vol.1, p. 72-88. Disponível em: https://isedef.ac.mz/wp-content/uploads/2021/02/revista-revista.pdf

C*larke*, R. & Knake, R. *Cyberwar: the next threat to national security and what to do about i*t. New York: HarperCollins.

Damjanović, D. Z. (2017). *Types of information warfare and examples of malicious programs of information warfare*. Zrenjanin, Republic of Serbia. Vojnotehni čki glasnik / military technical courier, Volume 65. Acedido no dia 27 de Agosto de 2018 em: https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2017/0042-84691704044D.pdf

Dinis, J. A. H. (2003). *A guerra de informação: perspectivas de segurança e competitividade*. Revista Militar, Lisboa.

Gery, W. R., SeYoung Lee & Ninas, J. (2017). *Information Warfare in an Information Age*. JFQ 85, 2nd Quarter. USA. Acedido no dia 09 de Maio de 2018 em: https://ndupress.ndu.edu/Portals/68/Docume

nts/jfq/jfq-85/jfq-85_22-29_Gery-Lee-Ninas.pdf

Kiyuna, A. Conyers, L. (2015). *Cyberwarfare sourcebook*. [S.l.]:Lulu.com. ISBN 9781329063945. Acedido no dia 28 de Novembro de 2017 em: https://books.google.co.mz/books?id=riH5CQAAQBAJ&pg=PA183&dq=he+enemy+and+the+public,+undermining+the+quality+of+opposing+force+information+and+denial+of+information-collection+opportunities+to+opposing+forces.+Information+warfare+is+closely+linked+to+psychological+warfare&redir_esc=y&hl=pt.

Kuehl, D.T. (2002). I*nformation Operations, Information Warfare, and Computer Network Attack*. International Law studies. Volume 76. Acedido no dia 12 de Agosto de 2019 em: https://digital-commons.usnwc.edu/ils/vol76/iss1/23/.

Libicki, M. C. (2017). *The Convergence of Information Warfare. Strategic Studies Quarterly*. Acedido no dia 23 de Maio de 2018 em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf

Lima, A. S. (2009). *Tecnologia de Guerra Electrónica vis à vis Uso de Ferramentas Empresariais.* Brasil.

Marlatt, G. E.(2008). *Information warfare and information operations: a bibliography*.

Dudley Knox Library. Naval Postgraduate School Revised. Acedido no dia 23 de Maio de 2018 em: https://library.nps.edu/

Neto, R. B. G. (2017). *Guerra cibernética / guerra electrónica – conceitos, desafios e espaços de interacção*. Revista Política Hoje - Volume 26.

Nunes, P.FV. (1999). *Impacto das Nova Tecnologias no Meio Militar: A Guerra de Informação.* Revista Militar. Acedido no dia 7 de Julho de 2018 em: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-p/2000/2tri00/nunes.htm.

Nunes, P. F. V. (2004). *Ciberterrorismo: aspectos de segurança*. Revista Militar. Acedido no dia 7 de Julho de 2019 em em: https://www.revistamilitar.pt/artigo/428

Nunes, P. F. V. (2006). Operações de informação: enquadramento e impacto nacional. Revista Militar. Acedido no dia 20 de Novembro de 2019 em: https://www.revistamilitar.pt/artigo/137

Santos, G. A. (2010). *Novo Ano, Novos Desafios: Ciberataques e Ciberdefesas*. Revista Militar. nº 2496.Portugal. Acedido em Setembro de 2019 em : http://www.revistamilitar.pt/artigo.php?art_id=533.

Seven, C. (1996). *U.S. military opportunities: informationwarfare concepts of operation*. Brian Nichiporuk. USA. Acedido no dia 23 de Agosto de 2018 em:

https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap7.pdf.

Sine, J. (2006). *Definir 'Arma de Precisão' em Termos de Basear-se em Feitos. Air & Space Power*. Acedido no dia 2 de Agosto de 2019 em : < http://www.airpower.maxwell.af.mil/apjinternational/ apj-p/2006/4tri06/sine.html.

Taddeo, M. (2011). *Information Warfare: A Philosophical Perspective***.** University of Oxford. Philosophy and Geography, Volume 25, 105-120. Acedido no dia 23 de Agosto de 2018 em: https://www.researchgate.net/publication/234627039_Information_Warfare_A_Philosophical_Perspective.

Theohary, C. A. (2018). *Information Warfare: Issues for Congress. Congressional Research Service*. Acedido no dia 12 de Agosto de 2019 em: https://fas.org/sgp/crs/natsec/R45142.pdf.

Van, C. M. (2010). *Technology and War: from 2000 BC to the present*. New York: Free Press.

Waltz, K. N. (1988). *The Origins of War in Neorealist Theory". Journal of Inter- disciplinary History*, vol. 18.

PARTE 2

A midia e a Internet na Guerra de Informação

1. GENERALIDADES

Sem dúvidas, actualmente a informação desempenha um papel fundamental para a tomada de decisão ou para a fragilização de um certo inimigo. Na primeira parte do presente livro, foi referenciado que os *midia* e a internet são os elementos que são mais utilizados na estratégia da GI. No entanto, as duas tecnologias são, em algumas situações, exploradas simultaneamente, ou seja, um certo actor pode solicitar a imprensa para transmitir uma certa mensagem e, segundos depois, a mesma estar em redes sociais. Trata-se de potencialidades que são vistas como um ganho, mas que, quando usadas sem consciência, podem trazer más consequências, tais como o surgimento de conflitos, tribalismo, regionalismo, etc. E é decorrente do receio do surgimento desses conflitos que se apresenta o historial da utilização dos *midia* e da internet e e seus efeitos, como forma de alertar a sociedade a fazer um ajuizamento de qualquer informação que circula nos midia antes de agir.

2. O PAPEL DA MIDIA NA GUERRA DE INFORMAÇÃO

Alguns conflitos começam dos *media* e depois influenciam para o surgimento de uma guerra real. Nos *media*, o maior objectivo da GI é usar o discurso para influenciar as opiniões da população e estabelecer um monopólio total sobre o fluxo de

informação, as percepções das audiências e os processos discursivos que moldam o mundo moderno[177].

2.1. Uso dos *media* para a construção das percepções públicas

Para a construção das percepções públicas, sempre procura-se utilizar o poder e os relacionamentos dos *media* de massas. As mensagens e ideias que os meios de comunicação de massa transmitem, através da comunicação de massa, são construídas por aqueles que controlam os media e, em sequência, usadas por eles para construir as percepções do público[178]. Os *media* são usados para levar o público a formar certas opiniões e tomar as suas decisões com base nessas opiniões. E mais, as mensagens entregues ao público, por via dos *media* e redes de informação, são, geralmente, uma forma de acção social, porque a entrega de informações por esses meios leva em consideração as reacções do público antes que qualquer informação seja divulgada[179]. Essas

---

[177] Nazemroaya, M. D. (2014). *Controlling the Lens: The Media War Being Fought Over Ukraine Between the Western Bloc and Russia.*

[178] Happer, C. & Philo, G. (2013). *The Role of the Media in the Construction of Public Belief and Social Change.* Journal of Social and Political Psichology, Volume 1. Glasgow

[179] Ibid 165.

reacções incluem as físicas ou processos materiais. Isso também inclui considerações sobre a manifestação de protestos como uma reacção às informações fornecidas ou considerações económicas, tais como retiradas de investidores, desvalorização da moeda e mudanças de mercado[180].

Abarcar a narrativa que é entregue ao público e desacreditar narrativas alternativas ou rivais, sejam elas verdadeiras ou falsas, é um aspecto importante da GI com a utilização dos *media*[181]. Embora essa forma de guerra não seja nova, ela está se tornando cada vez mais sofisticada e intensificada à medida que se torna uma táctica importante na caixa de ferramentas da guerra não convencional, que está se transformando característica do século XXI[182].

O tipo de gestão de informações que, tanto as redes de notícias privadas quanto as de propriedade pública, procuram e criam o entendimento comum é que informa as acções e reacções das audiências em relação a assuntos e situações particulares[183]. Essas suposições do senso comum

---

[180] Media Awareness Network. (2005). Detecting bias in the news. Retrieved April 4, 2005, from http://www.media-awareness.ca/english/index.cfm

[181] _____ (2014). *Controlling the Lens: The Media War Being Fought Over Ukraine Between the Western Bloc and Russia.*

[182] Ibid 52.

[183] Ibid178.

não se baseiam em factos reais existentes no mundo real, mas são formadas com base no que tem sido repetidamente apresentado como facto e conhecimento combinado.

No relato internacional, existiram mensagens politizadas e que foram entregues ao público e, por sua vez, levaram a atitudes de senso comum de acreditar que os muçulmanos xiitas e sunitas são inimigos amargos de sangue, ou que Hugo Chávez era um autocrata ou que há um ódio profundo entre sérvios e croatas[184]. Nenhuma dessas suposições foi fundamentada na realidade, mas lentamente entraram no preceito de falsas suposições que informam um segmento de audiências internacionais sobre questões internacionais. Além disso, essas mensagens, em muitos casos, são entregues sob o disfarce da objectividade neutra à política, o que impede que grandes partes da audiência questionem os motivos e implicações das mensagens que estão sendo transmitidas[185].

Como exemplo 1, a Ucrânia, a Síria e a Venezuela formaram uma frente numa guerra de informação global, que foi sendo reflectida através de uma batalha das redes internacionais dos *media*[186]. O objectivo da guerra dos *media* era de

[184] Ibid177.

[185] Ibid.

[186] Ibid 52.

assegurar e administrar a opinião pública nacional e internacional em apoio ou oposição ao golpe que ocorreu em Kiev e ao novo governo transitório ucraniano.

O exemplo 2, da GI nos *media*, está relacionado com o fracasso da *BBC World e CNN International*, verificado depois da Rússia, Irão, China e Venezuela implantarem as suas redes de notícias internacionais, como Russia TV (RT), a *Press* TV, a *Chinese Central Television* (CCTV) e a *Pan-latino-americana La Nueva Televisora del Sur* (telesur), cujo objectivo era desafiar, de forma clara, as redes dos *media* internacionais dos EUA e seus aliados. As narrativas da *Cable News Network* (CNN), sediada em Atlanta, e a *British Broadcasting Corporation* (BBC), que detinham quase o monopólio internacional, foram interrompidas e lentamente corroídas[187].

As novas redes RT e *Press* TV foram muito eficazes e realmente começaram a desafiar os discursos veiculados na *CNN, BBC, Fox News* e *Sky News,* respectivamente[188]*.* Porém, essa situação contribuiu para que as autoridades americanas e britânicas reconsiderassem as suas estratégias de mídia e examinassem maneiras de desafiar e enfraquecer as redes internacionais de notícias RT,

[187] Ibid 177.
[188] Ibid 180.

Press TV, CCTV e *telesur*, desafiando o seu controle sobre o fluxo de informações[189]. Em resposta, os EUA e seus aliados bloquearam a *Press* TV em língua inglesa, a *Al-Alam* em língua árabe e outras estações iranianas estatais na Europa e em outros lugares[190].

O domínio dos EUA e da Grã-Bretanha de desfrutarem dos *media* internacionais foi, sem dúvida nenhuma, rompido em 2011, quando muitos espectadores começaram a diversificar as suas fontes de informação. Entretanto, as estações como a CNN e a BBC foram evidentemente desacreditadas sobre a sua cobertura da guerra da OTAN, liderada pelos EUA contra a Jamahiriya Árabe Líbia[191].

Como resultado, Hillary Clinton foi forçada a descrever publicamente a importância das redes de notícias internacionais e os meios de comunicação de massa para o sucesso da política externa dos EUA[192]. Ao falar a um comité do congresso de 2011, Clinton declarou que Washington estava perdendo

---

189 Tsfati, Y. & Cohen, J. (2013). Perceptions of Media and Media Eff ects: The Third - Person Eff ect, Trust in Media, and Hostile Media Perceptions

190 Informação obtida no site: https://www.britannica.com/topic/public-opinion/The-mass-media

191 Ibid 177.

192 Ibid 192.

a guerra de informação global. Clinton disse, ainda, ao comité, que estava testemunhando que os EUA precisavam reverter as transmissões dos *media*, ao estilo da "Guerra Fria" e métodos de divulgação, e solicitar o aumento do financiamento para operações dos *media* estadunidenses, como meio de travar uma GI contra redes dos *media* estrangeiros que transmitem mensagens divergentes[193]. Clinton acusou o RT de ser um canal desestabilizador da política americana, descrevendo-o como o canal de língua inglesa dos russos.

A secretária Clinton lamentou ainda que os EUA e a BBC estatal estivessem reduzindo as suas operações nos *media* internacionais e que Washington precisava reverter os cortes para divulgar a mensagem dos EUA[194]. Ela deduziu que os recursos é que eram o maior problema, mas, na verdade, o número decrescente de audiências que sintonizavam estações como a *CNN International* ou a *BBC World* era o verdadeiro problema.

---

[193] Da cruz, T. M. F. (2009). *A influência da mídia na percepção da violência: as comunicações e denúncias à Central de Emergência 190*. Dissertação de Mestrado. Florianópolis

[194] Informação obtida no site: http://artepolitica.com/lecturas/controlling-the-lens-the-media-war-being-fought-over-ukraine-between-the-western-bloc-and-russia/

Contudo, as afirmações de Clinton ressoaram a agência federal dos EUA, que administrava a Rádio Europa Livre, Voz da América (VOA), Alhurra no Iraque e toda a transmissão internacional dos Estados Unidos[195]. Walter Isaacson, depois de alguns meses, declarou que os EUA estavam travando uma guerra de informação e que os Estados Unidos não podem se deixar ser comunicados por seus inimigos. Isaacson, que era ex-CEO da CNN, também enfatizou que a notícia de cima para baixo precisa de ser complementada por uma nova abordagem e que catalise as redes sociais[196]. Com isso, foi muito importante ter em mente ou considerar a interface entre os protestos antigovernamentais, os *media* sociais e os *media* tradicionais.

A declaração de 2011, de Clinton, sobre o envolvimento dos EUA numa GI global, caiu como se fosse uma bomba, que até a cobertura dos *media* nos EUA sobre essas declarações foi selectiva e distorcida para retratar uma imagem amigável e inocente do governo dos EUA[197]. Em vez de mostrar qualquer reflectividade ou fazer quaisquer relatórios analíticos substantivos, explicando que, o que estava ocorrendo era uma discussão das

[195] Ibid 192.
[196] Ibid 193
[197] Ibid 177.

autoridades americanas sobre o aprimoramento da propaganda do governo dos EUA no exterior e o domínio da informação disponível ao público internacional, os meios de comunicação dos EUA desprezaram a secretária e as declarações de Clinton foram totalmente ignoradas[198].

O Washington Post , por exemplo, não fez nenhuma tentativa nas suas reportagens de analisar o que Clinton e os senadores americanos estavam discutindo. Por exemplo, quando o senador Richard Lugar, um falcão de guerra conhecido e expansionista militar, disse que as operações de *media* internacional do Conselho de Governadores de Radiodifusão ainda são uma grande força de diplomacia, para transmitir-se essa mensagem o repórter de *The Washington Post* 's *Pulitzer* nem sequer explicou que, o que estava falando era que o governo dos EUA exercia o seu poder sobre outras nações, usando os *media* de massa para influenciar os seus governos por meio de um fluxo de informações sob *medida* para as suas populações[199].

Essa passividade de grande media que a cobertura do depoimento de Clinton demonstrou é,

---

[198] Informação retirada em: https://www.dw.com/pt-br/crise-da-ucr%C3%A2nia-%C3%A9-tamb%C3%A9m-guerra-entre-m%C3%ADdia-nacional-e-russa/a-17620042

[199] Ibid 177.

geralmente, justificada com base numa incerta objectividade. No entanto, isso é muito comum quando se trata de questões importantes, envolvendo governos, corporações, indivíduos ou entidades que a grande *media* não quer criticar ou prejudicar[200]. A alegação é que os factos estão sendo simplesmente relatados sem preconceitos ou interpretações subjectivas. A cobertura da *media* norte-americana sobre o evento teria sido muito diferente se fosse um funcionário russo falando a uma comissão parlamentar da Duma sobre o uso da *media* russa, para influenciar países estrangeiros[201]. E os mesmos padrões não são aplicados quando esses lindam com os pontos relacionados com entidades rivais. Em vez disso, uma reportagem assertiva, que envolve uma voz activa ou, ainda, assertiva de *media* convencional, sobre a cobertura da notícia, é então aplicada para atacar ou minar as decisões e acções dessas entidades rivais em nome do jornalismo investigativo e da análise crítica[202].

O terceiro exemplo refere à *media* ocidental, que atacou a *media* iraniana, chinesa e russa sobre fracassos na Síria[203]. Embora tenha havido uma

[200] Ibid 178.
[201] Ibid 189.
[202] Ibid 177.
[203] Ibid 52.

guerra de informação contínua, uma guerra de *media* muito distinta começou a tornar-se visível em 2011. Como destaque, foi a guerra da OTAN contra a Líbia, onde as redes internacionais de *media* desempenharam um papel importante no esforço da guerra. As novas redes de notícias "*antiestablishment"* amadureceram o suficiente para desafiar a propaganda dos EUA e fornecer narrativas alternativas, que desafiavam a legitimidade das transmissões da CNN e da BBC, até prejudicando a sua credibilidade e reduzindo as suas visualizações internacionais e domésticas[204]. E a Líbia foi apenas o começo, porque a Síria exibiu um conflito aberto e intenso entre essas redes de notícias, sendo travadas, principalmente nos idiomas inglês, árabe e espanhol. A eficácia das redes de *media anti-establishmentarian* em desafiar o discurso de redes como CNN, BBC, Fox News e Al Jazeera sobre a Síria demonstrou que os EUA não estrangulavam o fluxo de informações[205].

Como resultado, os meios de comunicação norte-americanos e britânicos começaram a condenar as redes internacionais de *media* chinesas, iranianas e russas, pelas suas narrativas

---

[204] Informação obtida no site: https://www.britannica.com/topic/public-opinion/The-mass-media

[205] Ibid 177.

sobre a Síria no início de 2012. Atacando as perspectivas de *media* chinesa, iraniana e russa, a imprensa americana e britânica negligenciou os segmentos de *media* africana, árabe, asiática, europeia e latino-americana, que partilhavam as mesmas opiniões dos meios de comunicação iranianos, chineses e russos, em países como Argélia, Argentina, Bielorrússia, Bolívia, Brasil, Cuba, Equador, El Salvador, Índia, Iraque, Líbano, Namíbia, Sérvia, África do Sul, Ucrânia e Venezuela[206]. Enquanto tentavam deliberadamente minar e subestimar o apoio que a Síria desfrutava de um segmento da comunidade internacional, para o seu público, os meios de comunicação americanos e britânicos traíam a frustração das agendas políticas das directorias que controlavam o seu discurso[207].

Como se pode observar, a guerra de *media* é um reflexo das rivalidades entre actores poderosos no mundo real. E é por isso que não deveria ser surpresa que tenha sido na mesma conjuntura que Hillary Clinton começou a exibir publicamente a frustração dos EUA contra os russos e os chineses. A secretária Clinton começou a dar palestras para os seus colegas chanceleres de outros países, reunidos nas conferências

[206] Ibid 189.
[207] Ibid 52.

internacionais, que apoiavam a mudança de regime e as operações militares contra a Síria[208]. Ela chegou a dizer aos outros ministros das Relações Exteriores que os russos e chineses tiveram que pagar um preço por se opor à ideia de progresso de Washington.

Em Julho de 2012 , Clinton chegou a dizer o seguinte: “Eu não acho que a Rússia e a China acreditam que estão pagando qualquer preço, nada, pois estão se identificando com o regime de Assad”[209]. A única maneira que vai mudar é se todas as nações representadas aqui (na conferência) directa e urgentemente deixarem claro que a Rússia e a China pagarão um preço, pois estão bloqueando o progresso, que não é mais tolerável ”[210].

A definição de Clinton sobre o progresso na Síria significa mudança de regime em Damasco e uma campanha de bombardeio militar contra os sírios. Na verdade, o que se denota é, ela estava expressando a raiva de Washington, porque fez a declaração depois que Moscovo e Pequim se recusaram a permitir que os EUA, a Grã-Bretanha e a França conseguissem que o Conselho de

[208] Ibid 177.
[209] Ibid.
[210] Ibid 189.

Segurança da ONU autorizasse uma guerra contra a Síria[211].

Depois que Washington mostrou a sua irritação com a Rússia, por impedir a mudança de regime na Síria, os EUA começaram a pensar seriamente em aplicar sanções contra os russos e em métodos de atacar as redes de *media* russas[212]. Essas considerações foram se materializando ou activadas com a crise na Ucrânia. No entanto, os pedidos de sanções contra os russos não são apenas o resultado da crise na Ucrânia; eles são parte de uma tendência que Washington já teve e até mesmo uma consideração pelas autoridades dos EUA, sobre como minar o mega-acordo de comércio de petróleo-por-mercadoria, que os russos e iranianos vinham negociando.

Já no âmbito nacional, nos últimos anos, a GI também está-se tornando uma realidade. Os actores, principalmente os políticos, ou aqueles que, por várias razões, pretendem atingir negativamente uma individualidade, utilizam os *media* para manietar a liberdade de pensamento da população moçambicana, sobretudo em momentos de campanha eleitoral. No entanto, em todo o mundo, os *media* são vistos como solução para, facilmente, disseminar informações falsas, num contexto em

[211] Ibid 177.
[212] Ibid.

que os actores da GI estão cientes que, com a evolução tecnológica (de Comunicação e Informação) e a massificação das redes sociais, em particular, em pouco tempo a sua informação pode desaguar nos ouvintes/leitores/telespectadores.

A GI tornou-se uma realidade tanto na esfera militar, como no seio político. Vejamos, a seguir, alguns exemplos do recurso aos *media* para fins políticos no contexto moçambicano:

- ❖ Incêndio na casa da mãe do Edil de Quelimane

Na madrugada do dia 16 de Setembro de 2019, cinco (05) homens armados atiraram fogo contra a casa da mãe do Edil de Quelimane, na altura, candidato da Renamo ao cargo de governador da Zambézia, nas eleições gerais de 2019[213]. Manuel de Araújo, sem, antes, fazer uma investigação, acusou a FRELIMO de ter praticado este crime. No mais, o candidato presidencial da RENAMO, recorrendo aos *media* para lograr objectivos políticos e tirar vantagens do crime, também alinhou com o seu edil, ao afirmar que o partido no poder pretendia desmoralizar a *perdiz* de fazer parte da campanha eleitoral, para as eleições de 15 de Outubro. O Presidente da Renamo utilizou a Televisão para assumir que o incêndio à casa da

[213] In jornal da Tarde da STV, 17 de Setembro de 2019.

mãe de Manuel de Araújo é parte de uma velha artimanha da FRELIMO, para enfraquecer a RENAMO[214], uma informação que em pouco tempo inundou as redes sociais.

Sem provas, essas alegações são falsas, porquanto visavam moldar a mente da sociedade moçambicana de que a FRELIMO é uma organização assassina/criminosa, e que, sem medir as consequências, desgraçou a família do edil de Quelimane. Por sua vez, e numa autêntica GI, a FRELIMO, no 17 de Setembro, convocou os *media* para contra-informar a mesma sociedade, tendo considerando que se tratava de um acto de vitimização, numa altura em que a RENAMO encontrava-se em conflito interno e que, por isso, tinha motivos para praticar este crime.

❖ Suposta activação dos esquadrões de morte

No dia 12 de Novembro de 2019, no Jornal da tarde da STV, o porta-voz da RENAMO informou que a FRELIMO tinha reactivado os esquadrões de morte, para aniquilar os seus simpatizantes. Novamente, pela mesma via e na mesma data, o porta-voz da FRELIMO veio contrapor, dizendo que as declarações da RENAMO eram infundadas e típicas de um perdedor.

---

[214] Ibid 213.

Como se pode observar, os *media* têm desempenhado um papel importante para a evolução da GI estratégica, pois são utilizados para informar e desinformar a sociedade. Sendo que o povo é o principal alvo, estas acções acabam tendo um maior impacto, sobretudo, nas populações rurais e menos escolarizadas, que, vezes sem conta, são levadas a confundir as declarações veiculadas, assumindo como reais, as falsas, e falsas, as verdadeiras, e vice-versa.

Trata-se de uma guerra tão real quanto desenfredada para a qual alguns actores vão criando os seus próprios meios de comunicação de massas. Outros - principalmente aqueles que não se identificam com o partido no poder – optam por filiar-se em organizações da sociedade civil sob a capa das quais se fazem passar por “defensores dos que não têm voz”, numa tremenda manipulação da mente da sociedade. Esta situação, por mais pequena que transpareça, contribui para a desinformação das populações, gerando ódio e revolta no seio das massas, concorrendo, por conseguinte, para o surgimento de conflitos que, em certa medida, ameaçam a paz no país.

Por isso, é importante que a sociedade avalie com serenidade as informações que recebe dos *media* e ou redes sociais antes de agir. As políticas ou leis devem impedir que os *media* e as

organizações civis sejam promotores de conflitos, pois a sua função primária é informar, formar e educar, permitirndo que a sociedade avalie atentamente as informações que circulam nos *media* e nas redes sociais.

2.2. Enquadramento dos *media* ocidentais na crise ucraniana

Normalmente, o que acontece é que os *media* seleccionam quais narrativas e mensagens devem ser publicadas e que conversas devem ser dominantes. Face a isso, certas vozes são ouvidas enquanto outras são excluídas ou totalmente ignoradas da conversa.

A título de exemplo, uma narrativa manipulada que apoiava a expansão da União Europeia e da OTAN, na Ucrânia, foi sendo construída onde uma realidade distorcida estava sendo representada sobre o que aconteceu em Kiev[215]. A cadeia de vocabulário ou a série de palavras relacionadas, que definiam o ritmo do discurso sobre os protestos antigovernamentais, foi muito reveladora e o presidente Viktor Yanukovych, na altura, foi constantemente apresentado como corrupto. O foco da *midia* foi apresentar a riqueza do presidente Viktor e os manifestantes de activistas e democratas

[215] Ibid 177.

(como defensores da população), para favorecer a oposição[216].

A transmissão em massa dessas redes de notícias começou a tornar-se cada vez mais uma imposição psicológica à medida que gradualmente foi aceite pelo público, pois foram constantemente bombardeadas pelos mesmos pontos de vista e narrativas sobre os protestos antigovernamentais na Ucrânia[217].

A narrativa em questão era: um regime pró-russo corrupto foi derrubado por uma revolução democrática, pese embora tal facto, na verdade, não teve relação com o que aconteceu. Entretanto, as mesmas fontes mediáticas, que retratavam Yanukovych como uma figura gananciosa e um autocrata corrupto, não mencionavam que as figuras da oposição, que eram apresentadas como tão favoráveis, eram igualmente ricas e com grandes mansões, arte de valor inestimável, piscinas, colecções de carros e vasta riqueza[218]. Eles também deixaram de mencionar que os principais líderes da oposição, antes, estavam no poder e perderam popularidade por

---

[216] Ibid 177.

[217] Vestena, C. L. B. (2008). *O papel da mídia na formação da opinião pública: a contribuição de Bourdieu*.

[218] Boyd-Barrett, O. (2016). *Western mainstream media and the Ukraine Crisis: A Study in conflict propaganda.* Bowling Green State University

causa da sua má administração e corrupção. Os *media* ocultaram ainda que os líderes da oposição teriam tomado o poder através de um golpe extremamente violento[219].

A linguagem difamatória usada nesses relatos, contra a Rússia e Vladimir Putin, era também muito reveladora. Tratava-se de linguagem que ilustrava ou apresentava as atitudes ou crenças que esses meios de comunicação queriam projectar sobre a Federação Russa e Putin. O presidente Putin foi enquadrado como um autocrata e um militarista. O histórico de Putin foi frequentemente referido como um meio de desinformação, ao passo que os antecedentes da CIA de George W Bush quase nunca foram referidos pelos mesmos meios, quando este era presidente dos EUA. O histórico da CIA de George W Bush Sr. sempre era feito em voz passiva ou positiva[220].

Essas atitudes, de emoldurar o discurso sobre a Rússia e Putin, baseavam-se numa posição adversa em relação à Rússia, como rival económico e geopolítico, estruturalmente enraizado na estrutura de poder que controla os meios de comunicação na América do Norte e na União

[219] Ibid 177.
[220] Ibid.

Europeia[221]. Entretanto, os jornalistas e funcionários do sector de *media* trabalhavam consciente ou inconscientemente em torno dos seus contornos e, consciente ou inconscientemente, serviam os seus objectivos para difamar a Rússia, e, em outras palavras, como um adversário ou estrangeiro[222].

Outro aspecto importante a sublinhar são os *media* ocidentais Segmentar RT e russos, que passaram a controlar a narrativa na Ucrânia. Durante o início das crises na Líbia e na Síria, os EUA e seus aliados se recusaram a admitir que estavam apoiando militantes com visões desviantes e intolerantes, que muitos descreveram como forças da Al-Qaeda ou afiliadas da Al-Qaeda[223]. Com o tempo, os EUA e seus aliados foram lentamente forçados a admitir que essas forças desviantes e intolerantes existiam na Líbia e na Síria. Esse reconhecimento foi o resultado da campanha de informação bem-sucedida, que estava sendo travada pelos *media* de massa de aliados sírios como Irão, China e Rússia. A posição arrogante da Al Jazeera Network, no Qatar, no mundo árabe, foi mesmo arruinada, já que canais como Rusiya Al-

[221] Ahlness, E. (2020).From the Second World to Global South?: Narratives of Tajikistan in Western Media. In book: Deconstructing Images of the Global South Through Media Representations and Communication, 46-66, Wanshigton.
[222] Ibid 44.
[223] Ibid 177.

Yaum, Al-Manar e Al-Mayadeen desafiaram sua cobertura sobre a crise na Síria[224].

Enquanto para o caso da Ucrânia, os EUA e seus aliados tentaram negar o envolvimento ultra-nacionalista e estruturar a história, que beneficiava os seus interesses na Ucrânia. Nesse caso, uma campanha foi iniciada contra os *media* russos, pelos EUA e seus aliados[225]. Como frustração, que se manifestou contra as redes de *media* internacionais russos, sobre sua cobertura na Síria, o objectivo da grande *media* na América do Norte e na União Europeia foi de apresentar a grande *media* russa como não-objectiva e indigna de confiança[226].

A campanha contra os *media* russos teve como alvo particular os seus segmentos de língua inglesa e armas internacionais, a RT América e a RT *International*, todos estes porque desafiavam a narrativa de que Washington e Bruxelas queriam vender a opinião pública sobre o golpe na Ucrânia[227]. Os comentários de dois funcionários da

---

224 Ibid 177.

225 Palmer, L. (2019). Translating" Russia: News Fixers and Foreign Correspondents in an Era of Political Uncertainty. Journalism Studies, volume 20, 1782-1797

226 Kalnes, Ø. & Bjørge, N. M. (2019). Cultures of anarchy: Images of Russia in the narrative of Norwegian mainstream news media during the Ukraine crisis 2014. Media War & Conflict, volume 1, 1-24.

227 Ibid 44.

RT e a questão da autonomia da Crimeia foram usados no ataque contra a RT América e a RT *International*[228].

Em relação ao último ponto, vale a pena notar que, quando parecia haver a possibilidade de o golpe contra o governo ucraniano fracassar (provavelmente porque esperavam que o golpe ocorresse em 20 de Fevereiro de 2014, depois que os franco-atiradores assassinaram manifestantes, os *media* atlânticos começaram a relatar sobre como a parte ocidental da Ucrânia poderia separar-se sem quaisquer vestígios de preocupação[229]. E o *The Guardian* informou essa situação no dia 21 de Fevereiro de 2014.

Enquanto os protestos continuavam nas ruas do centro de Kiev, as cidades, no oeste da Ucrânia, estavam caminhando em direcção à autonomia, com novos governos paralelos e forças de segurança, que admitiram abertamente que desertaram para o lado dos manifestantes[230]. Entretanto, importa notar ainda que o relatório desta ocorrência não mencionava o papel das milícias ultranacionalistas, em dominar as cidades ocidentais e intimidar os seus políticos. A questão é que o movimento da Crimeia em direcção à

---

[228] Ibid 221.
[229] Ibid 177.
[230] Ibid 218.

independência, nos *media* atlânticos, foi tratada abertamente sob um padrão totalmente diferente[231]. Os principais meios de comunicação, na América do Norte e na União Europeia, não tiveram nenhum problema com a autonomia, na metade ocidental da Ucrânia, mas claramente não aplicaram os mesmos padrões à Crimeia e se contrariam a ela. Os mesmos *media* ignoraram e subestimaram a agência do povo da Crimeia.

De forma insistente, a RT foi abertamente criticada pelos *media* da América do Norte e União Europeia, como a BBC, CNN, Fox News, Sky News e France 24, um braço de propaganda do Kremlin, com base no facto de se recusar a relatar a verdade sobre uma invasão russa da Crimeia[232]. No entanto, a BBC, a CNN, a Fox News, a Sky News e a France 24 são canais que tinham um histórico bem conhecido de distorcer os factos. E foram estes canais que fortemente desinformaram o povo da Crimeia, que era pró-russo[233]. O *The Telegraph,* em 11 de Março de 2014, num relatório de autoria de Patrick Reevell e David Blair, chegou a informar que, para a população da Crimeia, a votação na República Autónoma da Crimeia tinha apenas duas opções: juntar-se à Rússia naquele momento ou

---

231 Ibid 177.

232 Ibid.

233 Ibid 177.

mais tarde[234]. Estendendo a sua interpretação da questão nas cédulas, o jornal britânico chegou a dizer que o referendo perguntaria ao povo da Crimeia se eles queriam se juntar à Federação Russa directamente ou através de meios parlamentares. Em vez de dizer directamente que o referendo perguntaria ao povo da Crimeia, se queria juntar-se à Rússia ou permanecer como parte da Ucrânia sob a Constituição da Crimeia de 1994, o que poderia permitir a votação parlamentar da Rússia[235]. Entretanto, como se pode observar, o jornal britânico usou contorções de linguagem, para confundir a opinião pública e desacreditar o referendo.

2.3. Uso dos *media* para manipulação do pensamento do cidadão

As divisões que existiam entre os EUA e a Rússia foram se agudizando à medida que a situação na Ucrânia continuou tensa[236]. Os ramais dessa crise foram sentidos globalmente na Síria, na Península Coreana e nas Nações Unidas, à mesa de negociações sobre o programa nuclear iraniano entre Teerão e o P5 + 1.

---

[234] Mejias, U. A. (2017). Disinformation and the media: the case of Russia and Ukraine

[235] Ibid.

[236] Ibid 234.

Em última análise, o desencadeamento de uma GI entre os EUA e a Rússia pode parecer apropriado para uma conjuntura da história, que foi denominada de “Era da Informação”[237]. O que se pode concluir é que o controlo e a manipulação de informação pelos meios de comunicação de massas impedem que os indivíduos sejam conscientes sobre o mundo ao seu redor e as relações sociais que estão por detrás das estruturas das suas vidas diárias. E este poder de informar decisões, socializar indivíduos e moldar a cultura popular, que os *media* têm, está sendo mal utilizado[238].

A GI não é apenas travada entre potências rivais e blocos económicos, porque o controlo e a manipulação de informações também são usados internamente por governos e corporações contra os escalões mais baixos da sociedade. Na camada social baixa, os *media* são usados como forma de criar divisões sociais ou procurar mudar as mentes desta sociedade, com a mensagem de que ela está esquecida, porque a riqueza, o privilégio e o poder concentram-se na camada de elite[239]. No mais, com o surgimento das redes sociais, a GI tomou proporções preocupantes, e as acções para a sua mitigação também devem ser redobradas.

---

[237] Ibid 177.
[238] Ibid 193.
[239] Ibid 218.

E, às vezes, os que transmitem as informações desviantes são reféns daquilo que as suas próprias mãos semeiam[240]. Como referência, o discurso sobre o poder do Pentágono fez com que os dinamizadores da política norte-americana pensassem que um confronto entre os Estados Unidos e a Federação Russa ou a China teria pequenas consequências e não implicaria a possibilidade de uma guerra nuclear. Mas, sabe-se que a Rússia assim como a China formam uma aliança, com um arsenal mortal de armas nucleares e importantes recursos militares. E um confronto entre os EUA e a Rússia ou a China, poderia, sem dúvida, ter consequências drásticas e inesquecíveis em todo planeta terra[241].

2.4. Perguntas tendenciosas dos *media* e deturpação de imagens

Em GI, com a utilização de *media*, é difícil perceber se as perguntas postas a circular são sérias ou insultuosas, e muitas delas são subtís.

No entanto, alguns *media* não aplicam os mesmos padrões ao lidar com as diversas camadas da sociedade[242]. Para entrevistas tendenciosas, por exemplo, independentemente da gravidade das investigações, as perguntas são profundamente

[240] Ibid 52.
[241] Ibid 177.
[242] Ibid 218.

projectadas para obter resultados específicos do respondente. Na verdade, essas perguntas são projectadas para conduzir as respostas numa determinada direcção, para constranger e desacreditar uma certa instituição ou individualidade. E mais, algumas perguntas são néscias, porque incluem suposições e tentam limitar as respostas, para atender à agenda do repórter e dos objectivos previamente definidos[243].

São exemplos de algumas questões constrangedoras:

"*Quantas vezes fumaram suruma?"*

"*Você parou de bater na sua esposa?"*

Como se pode atentar, são perguntas tendenciosas e constrangedoras, e o seu princípio é baseado numa suposição errada ou visam levar alguém a aceitar o crime que não cometeu. E, na maioria dos casos, não importa o que o respondente diga[244]. As questões são colocadas numa situação incómoda, e oferecem a legitimidade respondendo-as.

Outra prática comum em GI é a utilização de imagens e vídeos fora do contexto real e a sua deturpação. Como exemplo, ainda no âmbito da GI entre Rússia e Ucrânia, outras reivindicações mostraram um mapa da Crimeia descontextualizado, fazendo crer que a RT havia reconhecido isso como parte da Rússia[245]. Foi uma

[243] Ibid 177.
[244] Ibid 234.
[245] Ibid 218.

verdadeira desonestidade e falta de princípios por parte dos profissionais da BBC, que decidiram reproduzir os recursos visuais fora do contexto da RT. E mais, os autores, de forma propositada, deturparam o significado das imagens, apresentando cenários ou capturas de tela que foram tiradas do contexto[246]. Omitiram ainda os factos de que os mapas foram apresentados como parte de um relatório, mostrando rupturas demográficas internas na geografia da Ucrânia ou as diferentes possibilidades, que o povo da Crimeia enfrentava[247].

Durante este conflito, a BBC teve um histórico de deturpar as imagens, e até foi apanhada em flagrante, com esses tipos de fabricação, e muitas vezes enquanto não havia nenhum caso em que a RT estava envolvida neste tipo de relatório[248]. Outro exemplo claro da deturpação de imagem sucedeu em 2008, quando a BBC apresentou uma imagem de espancamento de Monge Tibetano, por forças de segurança indianas, como forma de colocar em causa o governo chinês[249]. Outro caso, ainda envolvendo a BBC, aconteceu quando, num comício, os indianos, agitando bandeiras indianas, foram anunciados ao público como líbios,

---

[246] Ibid 226.

[247] Ibid 177.

[248] Boyd-Barrett, O. (2018). "Fake News:" "RussiaGate" as Disinformation in the Age of Social Media (Based on a series of 12 lectures presented

[249] Teixeira, D. (2015*). O 7 x 1 dos Espiões Chineses*. Revista Veja. Ed. 2340, ano 48.

comemorando a saída do governo líbio em 2011[250]. Mais, em 2013, a BBC foi encontrada a fazer *voice overs,* na sua cobertura da crise da Síria. O mais incrível foi quando um médico foi editado para dar a impressão de que ele estava falando em tempo real na sua voz natural, como tentativa de mudar a opinião pública.

3. A INTERNET COMO ELEMENTO ACTIVO DA GUERRA DE INFORMAÇÃO

As redes locais de internet, em inglês designadas por *Local Area Networks* (LANs) de conheceram uma utilização mais alargada durante os anos setenta. Uma LAN é, como o nome indica, constituída por computadores normalmente situados no mesmo edifício e interligados por cabos eléctricos[251]. Quando um dos computadores de uma LAN se liga à internet, todas as outras máquinas situadas na LAN também se tornam, na maior parte dos casos, acessíveis por qualquer outro computador da Internet[252]. A internet tornou-se mais útil na sociedade, mas também muito arriscado de a utilizar, derivado a alguns usuários mal-intencionados. Esta situação é muito mais perigosa do que era meio século atrás, quando as únicas redes existentes eram as telefónicas.

É verdade que, cada vez mais, dispomos de sistemas automatizados, onde temos máquinas

---

[250] Ibid 2.
[251] Ibid.
[252] Ibid 79

comunicando-se com máquinas, com a mínima intervenção humana [253]. Estas "máquinas" controlam os sistemas de energia eléctrica, as comunicações e uma grande quantidade de tarefas nas fábricas, ou em qualquer lugar onde existem tarefas simples e repetitivas. Mas, se uma destas máquinas comete um erro ou é sabotada, uma cidade pode ficar sem energia eléctrica, a rede telefónica pode ficar inoperacional numa vasta área, ou uma base de dados pode ser roubada[254]. E estas vulnerabilidades têm contribuído para o aumento progressivo da importância da guerra de informação, pois se um ser humano tiver a possibilidade de aceder a um destes robôs, pode, muitas vezes, anular o nosso processo de tomada de decisão.

É certo que este tipo de situação não vai provocar directamente a morte de ninguém, mas o que é facto é que os sistemas militares utilizam muitos destes sistemas automatizados[255]. Por exemplo, estima-se que mais de 90% das comunicações militares utiliza ligações de dados comerciais[256]. Embora muitos destes dados sejam enviados de uma máquina para outra, sem intervenção humana, é possível intervir sobre eles

---

253 Castells, M. (1999). A Sociedade em Rede. Volume 1, 8ª edição

254 Ibid 150.

255 Perry, W. L. ; Button, R. W. ; Bracken, J. ; Sullivan, T. & Mitchell, J. (2002). Measures of effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes. Santa Monica, Rand

256 Ibid 79.

se tivermos acesso ao sistema. É lógico que podemos utilizar um código secreto (cifra), para enviar os dados, mas estes códigos podem ser quebrados. Todo aquele que utiliza uma rede de computadores é vulnerável[257].

Actualmente, não nos podemos dar ao luxo de não utilizarmos as redes de computadores, porque essencialmente a GI consiste na exploração das vulnerabilidades nelas existentes. Muitos dos sistemas de armas, radares e QGs dependem da velocidade e funcionalidade oferecida pelas redes de computadores para garantir a sua operacionalidade[258]. E, mesmo com tantos perigos, o país que gerir as suas Forças Armadas sem estas redes pode ser colocado numa situação de grande desvantagem, face a outro que esteja completamente interligado por redes de comunicações.

Quanto aos perigos, recorde-se que o primeiro objectivo atacado na Guerra do Golfo foram as redes de comunicações iraquianas[259]. Uma vez cortadas essas redes, os iraquianos nunca recuperaram a sua operacionalidade. Isto materializou uma GI, acompanhada pela utilização de bombas *inteligentes*[260].

---

[257] Ibid 248.

[258] Arquilla, J. & Ronfeldt, D. (2001). Network and Netwars: the Future of Terror, Crime and Military; National Defense research Institute- RAND

[259] Ibid 255.

[260] Ibid 2.

Trata-se de um sinal claro que as acções, utilizando-se um computador pessoal e uma linha de telefone, também estão ganhando terreno no conceito da GI. Portanto, hoje assistisse-se a uma situação em que a guerra é aberta com indivíduos anónimos, sentados remotamente às suas secretárias, armados com computadores pessoais e outros dispositivos electrónicos. E até onde se tem conhecimento, não são normalmente os *hackers* organizados que têm vindo a criar todos os vírus de computador existentes, ou que têm vindo a tentar penetrar nas redes, mas é um facto que a maioria deste tipo de situações deve-se a *hackers* individuais e *freelancers*. Alguns destes *hackers* independentes negociam com agências de espiões, por razões de carácter ideológico, monetário ou mesmo por argumentos de natureza pontual e indeterminada[261]. Alguns até são detectados e presos, mas a incerteza sobre quantos não terão sido detectados levanta a necessidade imperiosa de assegurar uma capacidade de comando efectivo sobre a guerra de informação[262].

O que, por vezes, passa despercebido em todo este temor e desespero, relativo à GI, é que a maioria dos danos infligidos aos sistemas de informação é e sempre foi causada através de erro humano[263]. Estes problemas são normalmente provocados pelos usuários, pelos programadores, pelos projectistas de *hardware* ou pelos

---

261 Ibid 249.

262 Ibid 2.

263 Ibid.

"integradores", que reúnem o *hardware* com o *software*[264]. E frequentemente é impossível determinar se um mau funcionamento do sistema é resultante de uma má programação, de um defeito físico do mesmo, ou consequência de alguém ter lançado um ataque de guerra de informação[265].

Esta situação conduziu a um trabalho de desenvolvimento de técnicas de ordenação e triagem das falhas habituais dos sistemas reais, como forma de possibilitar a detecção da ocorrência de ataques de guerra de informação[266]. O que torna esta perspectiva interessante é que um ataque de GI inteligente, às vezes, tenta introduzir falhas nas redes inimigas, para que se pareça com falhas de *hardware* ou problemas de *software*[267].

Mas, o pensamento mais imediato e popular, relativamente à guerra de informação, é atingir o inimigo de uma forma dura e rápida, utilizando todos os meios mais rápidos ao nosso alcance, derrubando os seus sistemas de informação[268]. Porém, muitas nações encaram a GI como um meio para derrubar de forma decisiva o inimigo.

Outro facto importante, que tem influenciado para a existência de mais indivíduos mal-intencionados, é que antigas nações de ideologia comunista conferiam formação a mais pessoas do que aquelas que podem empregar, facto que

---

[264] Ibid248.
[265] Ibid 218.
[266] Ibid 253.
[267] Ibid.
[268] Ibid 2.

originou a existência de muitos especialistas de computadores com tempo disponível e um certo ressentimento contra a sociedade[269]. Por estes motivos, desde os anos oitenta que a Bulgária foi identificada como a fonte de muitos dos vírus de computador existentes.

Nações não comunistas, com um parâmetro social de muitos desempregados e com o nível de formação elevado, como o Paquistão, ao longo dos últimos anos também produziram muitos *hackers* mal intencionados[270]. Como bom exemplo, temos a Índia que apostou em dar trabalho aos programadores de computador, e como resultado apresentam um baixo índice de *hackers* informáticos e um potencial elevado no nível da guerra de informação. Apesar de um punhado de *superhackers,* que trabalha para uma pequena nação, poder infligir elevados danos aos sistemas de informação, de uma superpotência (exemplo: EUA), a probabilidade de esta situação ocorrer é algo remota[271]. Entretanto, as nações industrializadas encaram os perigos relativos à GI de uma forma séria, facto que torna esta situação ainda mais improvável.

Actualmente, os sistemas de informações militares encontram-se constantemente ameaçados por governos estrangeiros, organizações criminosas e *hackers.* E o impacto das actividades dos *hackers* e das suas tentativas de intrusão nos

---

269 Ibid.

270 Ibid 258.

271 Ibid 2.

sistemas de informações, vem aumentando substancialmente devido, em larga escala, ao facto de existir uma maior dependência das organizações militares em relação à internet[272].

Por fim, diga-se que a internet tem contribuído bastante para o derrube das fronteiras, constituindo um dos melhores suportes ao desenvolvimento de acções de guerra de informação.

4. REFERÊNCIAS

_____ (2014). *Controlling the Lens: The Media War Being Fought Over Ukraine Between the Western Bloc and Russia*. Acedido no dia 13 de Maio de 2019 em: https://www.globalresearch.ca/controlling-the-lens-the-media-war-being-fought-over-ukraine-between-the-western-bloc-and-russia/5373364.

Ahlness, E. (2020).From the Second World to Global South?: Narratives of Tajikistan in Western Media. In book: Deconstructing Images of the Global South Through Media Representations and Communication, 46-66, Wanshigton. Acedido no dia 04 de Março de 2020 em: https://www.researchgate.net/publication/338316164_From_the_Second_World_to_Global_South_Narratives_of_Tajikistan_in_Western_Media.

[272] Ibid.

Allinson, J. (2015). *The Necropolis of Drones.* International Political Sociology. Vol. 02.

Arquilla, J. & Ronfeldt, D. (1993). "Cyberwar is Comming." In In Atheana's Camp Preparing for Conflict in the Information Age, Rand. Acedido no dia 26 de Março de 2020 em: https://www.rand.org/pubs/monograph_reports/MR880.html

Arquilla, J. & Ronfeldt, D. (2001). Network and Netwars: the Future of Terror, Crime and Military; National Defense research Institute-RAND. Acedido no dia 26 de Março de 2020 em: https://www.rand.org/pubs/monograph_reports/MR1382.html

Bellintani, A. e Bellintani, M. (2014). *A Guerra: do século XIX aos nossos dias*. Boa Vista: Editora UFRR.

Boyd-Barrett, O. (2016). *Western mainstream media and the Ukraine Crisis: A Study in conflict propaganda.* Bowling Green State University.

Boyd-Barrett, O. (2018). "Fake News:" "RussiaGate" as Disinformation in the Age of Social Media (Based on a series of 12 lectures presented. Acedido no dia 4 de Março de 2020 em: https://www.researchgate.net/publication/326020832_Fake_News_RussiaGate_as_Disinformation_in_the_Age_of_Social_Media_Based_on_a_series_of_12_lectures_presented.

Castells, M. (1999). A Sociedade em Rede. Volume 1, 8ª edição. Acedido no dia 04 de Dezembro

de 2019 em: https://perguntasaopo.files.wordpress.com/2011/02/castells_1999_parte1_cap1.pdf

Happer, C. & Philo, G. (2013). *The Role of the Media in the Construction of Public Belief and Social Change.* Journal of Social and Political Psichology, Volume 1. Glasgow. Acedido no dia 05 de Janeiro de 2020 em: https://jspp.psychopen.eu/article/view/96/37.

Kalnes, Ø. & Bjørge, N. M. (2019). Cultures of anarchy: Images of Russia in the narrative of Norwegian mainstream news media during the Ukraine crisis 2014. Media War & Conflict, volume 1, 1-24 . Acedido no dia 04 de Março de 2020 em: https://www.researchgate.net/publication/334626284_Cultures_of_anarchy_Images_of_Russia_in_the_narrative_of_Norwegian_mainstream_news_media_during_the_Ukraine_crisis_2014.

Media Awareness Network. (2005). *Detecting bias in the news*. Acedido no dia 6 de Março de 2019 em: http://www.media-awareness.ca/english/index.cfm.

Mejias, U. A. (2017). *Disinformation and the media: the case of Russia and Ukraine*. Acedido no dia 4 de Março de 2020 em: https://www.researchgate.net/publication/312149298_Disinformation_and_the_media_the_case_of_Russia_and_Ukraine

Nazemroaya, M. D. (2014). *Controlling the Lens: The Media War Being Fought Over Ukraine*

Between the Western Bloc and Russia. Acedido no dia 12 de Novembro de 2019 em*:* https://www.globalresearch.ca/controlling-the-lens-the-media-war-being-fought-over-ukraine-between-the-western-bloc-and-russia/5373364

Nunes, P.FV. (1999). *Impacto das Nova Tecnologias no Meio Militar: A Guerra de Informação.* Revista Militar. Lisboa. Acedido no dia 7 de Julho de 2018 em: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-p/2000/2tri00/nunes.htm.

Nunes, P. F. V. (2006). *Operações de informação: enquadramento e impacto nacional*. Revista Militar. Lisboa. Acedido no dia 26 de Março de 2020 em: https://www.revistamilitar.pt/artigo/137

Palmer, L. (2019). Translating" Russia: News Fixers and Foreign Correspondents in an Era of Political Uncertainty. Journalism Studies, volume 20, 1782-1797. Acedido no dia 04 de Marco de 2020 em: https://www.researchgate.net/publication/334796191_Translating_Russia_News_Fixers_and_Foreign_Correspondents_in_an_Era_of_Political_Uncertainty.

Perry, W. L. ; Button, R. W. ; Bracken, J. ; Sullivan, T. & Mitchell, J. (2002). *Measures of effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes*. Santa Monica, Rand.

Teixeira, D. (2015*). O 7 x 1 dos Espiões Chineses*. Revista Veja. Ed. 2340, ano 48

Tsfati, Y. & Cohen, J. (2013). *Perceptions of Media and Media Eff ects: The Third - Person Eff ect, Trust in Media, and Hostile Media Perceptions*. Acedido no dia 05 de Janeiro de 2020 em: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781444361506.wbiems995

Tsfati, Y.(2014). Public and Elite Perceptions of News Media in Politics. Acedido no dia 05 de Janeiro de 2020 em: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199793471.001.0001/oxfordhb-9780199793471-e-52

Vestena, C. L. B. (2008). *O papel da mídia na formação da opinião pública: a contribuição de Bourdieu*. Paraná. Acedido no dia 12 de Novembro de 2019 em: https://revistas.unicentro.br/index.php/guaiaraca/article/viewFile/1144/1089

Waltz, K. N. (1988). *The Origins of War in Neorealist Theory". Journal of Inter- disciplinary History*, vol. 18.

PARTE III

Comportamento, Segurança e Situação Operacional em Redes Sociais

1. Generalidades

Actualmente, as redes sociais são o vértice do mundo virtual, pois possibilitam a interligação de indivíduos de todos os locais do mundo, facilitando a interacção social entre as pessoas. As redes sociais são um espaço virtual muito diversificado, onde nem todas as pessoas partilham os mesmos ideais[273]. Entretanto, é real que essa divergência de ideias em algum momento vai gerando conflitos sociais, que até influenciam para o surgimento de confrontos, alguns deles armados.

Os conflitos sociais relativos às redes sociais, devido à impossibilidade de propagação da manifestação de pensamento, limitavam-se aos grupos sociais de convivência e, com a evolução tecnológica e digital, as redes sociais tornaram-se cada vez mais informais e próximas aos seus usuários, comprometendo não só as regras do direito, mas também a segurança militar.

Em redes sociais, os seus usuários expressam as suas opiniões sem qualquer ponderação de limites ao que é postado, comentando e partilhando o que seria reflectido em uma interacção social física[274]. No mais, os usuários das redes sociais tomaram a liberdade de expressar tudo o que pensam e acontece, sendo que as redes tornaram-

---

[273] Cardoso, S. C.; Zago, C. & Silva, b. v.(2018). Discurso de ódio nas redes sociais: dignidade da pessoa humana face o abuso da liberdade de expressão e suas limitações. Brasil.

[274] Abreu, L. F. S. (2015). *A segurança da informação nas redes sociais*. São Paulo

se um espaço onde se noticiam as opiniões preconceituosas, discriminatórias e intolerantes, principalmente com discursos de ódio voltados às minorias sociais (políticos, famosos e outros)[275].

O que se pode constatar, em Moçambique, em particular, é que, em redes sociais, o direito à liberdade de expressão parece estar a ser exercido de forma abusiva e tendenciosa, pois chega-se ao ponto de colocar-se em causa a dignidade humana, princípio fundamental dos direitos humanos e, como consequência disso, alguns lesados acabam reagindo também de forma violenta, o que gera discórdias.

Porém, esta situação não pode estar à margem das Forças de Defesa e Segurança, pois, para além de estarem atentas para repelirem os eventuais conflitos, resultantes da má utilização das redes sociais, também devem estar atentas à situação de segurança de informação. Actualmente, muitos agentes ligados ao sector de defesa e segurança utilizam as redes sociais, mas nem todos avaliam a informação que partilham. Perante este estado de coisas, há toda a necessidade de as forças armadas desenvolverem mecanismos tecnológicos (assim como não), para controlarem as informações operacionais em redes sociais (tendo presente que as redes sociais podem ser utilizadas em operações militares, onde os comandantes podem as utilizar para obterem informações de apoio ao processo de decisão militar).

---

[275] Ibid 274.

2. CONCEITUALIZAÇÃO E ALGUNS RECURSOS DAS REDES SOCIAIS

2.1. Conceito e principais funcionalidades

As redes sociais são plataformas que habitam na internet e que, de entre várias acções, permitem ao seu usuário construir um perfil de índole pública ou privada, gerir a lista de pessoas com quem tenciona conectar-se, visualizar e percorrer a própria lista de conexões e a de cada pessoa dentro desse sistema, partilhar os seus interesses, experiências, informações que podem ser partilhadas e respondidas por outros e também ver, partilhar e responder às publicações dos outros usuários[276].

As redes sociais permitem vários métodos de interacção, através de aplicações associadas como jogos, relações interactivas donde constam os locais visitados pelos usuários, ferramentas de mensagem privadas com vídeos ou através das publicações de fotografias, vídeo ou texto[277].

Actualmente, praticamente todas as redes sociais permitem que os usuários acedam às suas contas por telemóvel, com acesso à internet, a partir de qualquer parte do mundo, actualizar o perfil, fazer publicações com ou sem identificação geográfica,

---

[276] Romi, F. A. B. L. (2013). A *análise das redes sociais informais com foco no crescimento profissional das pessoas: um estudo de caso.* Niterói

[277] Lorenzo, E. M. (2013). *A Utilização das Redes Sociais na Educação.* 3ª ed., Rio de Janeiro

entre outras preferências[278]. As redes sociais (RS) são um fenómeno transversal a toda a sociedade, onde as pessoas e as organizações se expõem. As RS são o campo sublime para a aplicação de técnicas de engenharia social e a propagação de informações prejudiciais e *malwares,* como revelam os constantes ataques a estas plataformas com a quebra das *passwords* de acesso e a divulgação e análise das informações e dos detalhes pessoais dos utilizadores[279].

2.2. Os recursos das redes sociais mais utilizadas em Moçambique

Esta subsecção tem como objectivo principal, dar a conhecer os recursos de algumas plataformas de RS, que, pelas suas características e popularização, merecem o controlo da sua utilização no meio militar. Porém, parte-se do pressuposto que as redes sociais mais utilizadas pelos agentes do sector de defesa e segurança são o *Facebook*, *o YouTube*, o *WhatsApp* e o *Instagram*.

2.2.1. *Facebook*

O *Facebook* é a poderosa ferramenta das redes sociais, porque combina os elementos das outras redes sociais como o *Twitter* e o *YouTube*[280]. O

---

278 Ibid 277.

279 Lima, H. G. A. (2015). *Percepção e riscos na utilização de redes sociais (facebook) por parte dos militares cabo verdianos*. Braga.

280 Muleta, D. M. D. (2015). *O impacto das redes sociais nas operações militares*. Sintra.

Facebook tem sido mais utilizado para fins de negócios *online*, *blogs*, jogos de computador, partilha de fotografias e vídeos e actividades sociais. Até em Janeiro de 2015, esta plataforma tinha mais de um mil milhão de contas activas[281].

No *Facebook,* o usuário é identificado por um perfil por si criado e é possível observar os amigos e os amigos em comum, informações, gostos (por livros, grupos, músicas, filmes, personalidades e tudo o que se possa imaginar), locais frequentados, actividades recentes, fotografias, vídeos, grupos em que o usuário esteja registado, o contacto e morada do usuário (se este tiver disponibilizado) e o mural (donde constam as publicações ou *posts* que tenham sido feitas no perfil pelo próprio ou por terceiros e que podem ser directamente comentadas, fazer gosto ou partilhar)[282].

Os usuários do *facebook* possuem 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[283]. Caso contrário - se for privado - só as pessoas que o usuário autorize podem ver o seu perfil. No entanto, um usuário que queira ver um perfil ou um grupo privado terá que enviar um pedido de amizade ou de acesso ao grupo respectivamente. A procura por pessoas pode ser feita através de um endereço electrónico, por

---

[281] Ibid 277.
[282] Ibid.
[283] Ibid 276.

escola, universidade, trabalho ou escrevendo o nome da pessoa ou a localidade em que vive.

A particularidade mais popular do *Facebook* é a publicação de fotografias que podem ser carregadas e postadas directamente por telemóvel, câmara ou computador, entre outras formas possíveis. É possível, igualmente, publicar fotografias, vídeo e texto no próprio perfil e no de outras pessoas ou grupos. O usuário tem a possibilidade de estabelecer privacidade nas publicações para que as veja apenas quem se quer[284].

O *Facebook* possui o serviço de mensagens privadas e é possível enviar uma mensagem a qualquer pessoa, esteja ou não no núcleo de amigos do usuário. E na secção do *chat* é possível visualizar todos os amigos que se encontram conectados ao *Facebook*[285].

No entanto, o *Facebook* é uma plataforma multifacetada, que disponibiliza infinitas ferramentas, de fácil utilização, e permite a disseminação instantânea de informação sobre formas variadas: texto, imagem e vídeo[286].

2.2.2. *YouTube*

YouTube é um *site* da *web,* que é utilizado para a partilha de vídeos. No *YouTube,* os usuários podem publicar e partilhar vídeos, que vão desde as

[284] Ibid 276.
[285] Ibid.
[286] Ibid.

notícias *online* amadoras até vídeos de música[287]. Os usuários podem criar respostas a vídeos, colocando a hiperligação num comentário a um vídeo, comentar vídeos, assim como classificá-los.

YouTube é uma plataforma que está a transformar os vídeos *online* num fenómeno social, conta com milhares de milhões de utilizadores, disponibilizando um fórum onde as pessoas podem interagir, informar e inspirar outras pessoas em todo o mundo[288]. Trata-se de uma rede social que permite a difusão de vídeos, que podem ser editados, legendados e trabalhados, para depois serem publicados de forma *online*. Permite a publicação de vídeos ao vivo e em directo, e esta vantagem aumenta a simplicidade de uso e torna-o como uma ferramenta de eleição para a disseminação da consciência[289].

2.2.3. *WhatsApp*

WhatsApp é um aplicativo de mensagens multiplataforma, que permite trocar mensagens pelo celular, sem pagar por SMS, e está disponível para *smartphones*, *iPhone*, *BlackBerry*, *Windows Phone*, *Android* e *Nokia*. O termo *WhatsApp* é de origem inglesa “*What's Up*”, que, em português, significa “E aí?”[290].

---

[287] Ibid 277.
[288] Ibid.
[289] Ibid.
[290] Ibid 277.

O aplicativo de *WhatsApp* pode ser baixado gratuitamente em *smartphones*, ou mesmo pelo *site* da empresa, bastando apenas possuir conexão com a internet. Para utilizar as ferramentas da mídia social é necessário ter contactos telefónicos na agenda do celular, que possuem o aplicativo, e é possível o cadastro de um perfil de usuário com informações da conta, definições das formas de conversas, formas de notificação e lista de contactos. No perfil do usuário, é possível adicionar uma foto e um nome, que serão visualizados pelos contactos[291]. O aplicativo emite um alerta sonoro, que pode ser personalizado com uma marcação na caixa de entrada, destacado na cor verde, informando que tem uma mensagem enviada por uma pessoa da sua rede de contactos[292].

WhatsApp utiliza formato de mensagens de textos simples e, quando enviada, também notifica ao emissor da recepção da mensagem ou arquivo. O próprio aplicativo organiza as mensagens por data e hora, oferecendo a opção de carregamento de informações anteriores, para além de oferecer, em seus recursos, um bloco com vários *emoticons* e desenho para agrupar as conversas, que tornam a forma de interacção mais agradável[293].

O *WhatsApp* oferece a possibilidade de criação de grupos de qualquer esfera, discussão, amigos, parentes, que também se valem das informações

---

[291] Ibid.
[292] Ibid.
[293] Ibid 276.

dos contactos telefónicos do celular. Para isso, é necessário existir um administrador, que convida as pessoas para o grupo sem a necessidade prévia de aceitação da pessoa convidada[294].

Além das mensagens simples, o aplicativo *WhatsApp* também permite o envio e recepção de várias opções de arquivos, tais como: fotos, videos, *links*, localizações e mensagens por voz. Mas, há também a possibilidade de troca de mensagens de áudio, que depende apenas de um clique, gravando a voz do emissor para envio ao receptor[295].

2.2.4. *Instagram*

O *Instagram* foi lançado em 2010, pelo norte-americano Kevin Systrom e pelo brasileiro Mike Krieger, ambos engenheiros de *software*. No dia do lançamento, o aplicativo tornou-se o mais baixado na *Apple Store,* e, em Dezembro do mesmo ano, já contava com 1 milhão de usuários[296].

Em 2011, a empresa, que tinha apenas 6 funcionários, já possuía 10 milhões de usuários na rede. E, no ano de 2012, após o lançamento do aplicativo na versão para Android, o *Instagram* foi comprado pelo *Facebook,* por 1 bilhão dólares[297]. Actualmente, o *Instagram* conta com mais de 500 milhões de usuários, em todo o mundo.

Além dos filtros originais inspirados na câmara *Polaroid*, o *Instagram* apresenta uma série de

---

[294] Ibid 277.
[295] Ibid.
[296] Ibid.
[297] Ibid.

recursos atraentes, que contribuem para a experiência do usuário no aplicativo e foram implementados ao longo de seus 6 anos de existência[298]. Essa rede social conta com os seguintes recursos:
Edição de imagem - permite ajustar o tamanho, o corte ou endireitamento e inserção de efeitos de luz, contraste e cor.

Visualização - onde são ilustradas as famosas *curtidas*, que possuem como um símbolo "um coração", de cor vermelha (se calhar, o recurso mais importante e querido dentro do aplicativo). É com este recurso que é possível medir a popularidade e interacção de *posts* e os gostos de pessoas.

Comentários - outra boa opção de interacção entre os usuários, são os comentários que podem ser feitos nas publicações. Além de comentar sobre a foto ou vídeo em questão, é possível marcar amigos, para que eles também vejam o conteúdo rapidamente.

Seguindo – com este recurso é possível acompanhar o que seus amigos e outras pessoas, que você segue, estão fazendo na rede. Fotos, pessoas seguidas e comentários em fotos podem ser visualizados nesta opção.

Explorar - disponibiliza uma galeria de fotos de pessoas de todo o mundo, inspiradas nas fotos, que são visualizadas e seguidas. Trata-se de um recurso que possibilita a descoberta de novos perfis e

[298] Ibid 277.

despertam o interesse, já que, de alguma forma, se encaixam nas preferências, dentro da rede.

Marcação em fotos - é a opção de geração e marcação de fotos, dentro do perfil, uma galeria de fotos postadas por outras pessoas, onde o usuário esteja presente e marcado. Caso o usuário não queira, pode seleccionar a opção de ocultar a foto do seu perfil e, desta forma, não aparecer na galeria.

Mensagens directas - as mensagens directas funcionam como uma espécie de *chat,* que conecta usuários. Além desta troca de mensagens, é possível enviar fotos do seu próprio aparelho ou de dentro do *Instagram*.

Localização - ao postar uma foto, pode adicionar-se o local onde ela foi tirada. Isso ajuda outros usuários a saberem a localização daquela imagem e também cria um mapeamento de lugares visitados, que podem ser visualizados no seu próprio perfil. No entanto, é uma maneira interessante de se ter uma visão geral sobre lugares visitados no seu país ou ao redor do mundo.

Instagram Stories - é um recurso mais recente do aplicativo e gerou muitas polémicas. É similar ao *Snapchat* e permite a partilha em tempo real de imagens e vídeos, que desaparecem após 24 horas, e a inclusão de *emojis*, desenhos e manuscritos. Nele, podedeterminar-se a privacidade das suas histórias, para que apenas alguns usuários tenham acesso ou para que qualquer usuário da rede possa ver as suas publicações. Além disso, assim como o *Snapchat*, existe a possibilidade de ter acesso a

quem visualizou as suas publicações. O *Instagram Stories* é um recurso mais valioso para as empresas, pois permite que estas possam interagir com os seus clientes dentro dessa rede social.

3. A SOCIEDADE E A RELAÇÃO DO DISCURSO DE ÓDIO NAS REDES SOCIAIS

Com a massificação das redes sociais, a sociedade ficou cada vez mais conectada, o que tem influenciado para que alguns indivíduos tenham vontade de usar e, não raras vezes, abusar da palavra, uma vez que, neste ambiente, em pouco tempo, a informação ou opinião consegue abranger muitas pessoas ou usuários. Porém, nem todos os discursos, em redes sociais, são construtivos à sociedade, pois alguns incitam à violência, ao divisionismo, ao tribalismo, etc. Estes comportamentos, à miúde, podem gerar conflitos armados. É neste contexto que se sugere a abordagem do assunto na a presente secção, pois revela-se importante, antes de aflorar a segurança e privacidade em redes sociais, descrever (de forma sumária) a relação existente entre a sociedade e essas plataformas.

3.1. A sociedade e as redes sociais

As redes sociais já são palco de grandes manifestações e mobilizações. Quaisquer decisões tomadas por um governo - ou outro acontecimento que se registe - ganham destaque nas redes sociais, onde cada cidadão, movido pelos seus

interesses ou influências, livremente expressa as suas opiniões. Este tópico é analisado neste livro, porque o abuso à liberdade de expressão desestabiliza um país, quando alguns indivíduos proferem discursos de ódio, que incitam a violência, por exemplo, e, quando isso acontece, às vezes, são chamadas as FDS, para manterem a ordem.

Um bom exemplo, sobre como as redes sociais vêm rapidamente mudando os costumes de culturas inteiras, foi a primavera árabe, onda revolucionária de manifestações e protestos que ocorreram no Oriente Médio e no Norte da África, desde 18 de Dezembro de 2010[299]. Até à data, tem havido revoluções na Tunísia e no Egipto, uma guerra civil na Líbia; grandes protestos na Argélia, Bahrein, Djibuti, Iraque, Jordânia, Síria, Omãn e Iémen e protestos menores no Kuwait, Líbano, Mauritânia, Marrocos, Arábia Saudita, Sudão e Saara Ocidental[300].

Os protestos têm partilhado técnicas de resistência civil, em campanhas, sustentadas, envolvendo greves, manifestações, passeatas e comícios, bem como o uso das mídias sociais, como *Facebook*, *Twitter* e *Youtube,* para organizar, comunicar e sensibilizar a população e a comunidade internacional, em face de tentativas de repressão e censura na internet por partes dos Estados.

---

[299] Ibid 273.

[300] Sarlet, W. (2018). Liberdade de expressão e discurso de ódio na internet e a jurisprudência da CEDH

Um outro exemplo recente de manifestação nas redes sociais teve lugar no Brasil, com um abaixo-assinado para a cessação de Jair Bolsonaro, deputado federal do PP-RJ[301]. Por meio do *Twitter* e do *Facebook,* os internautas divulgaram o abaixo-assinado, que pedia a cessação do político, por violação de preceitos institucionais. Com a repercussão do caso, o Conselho de Ética e Decoro Parlamentar abriu um processo disciplinar, para apurar a verdade[302].

No entanto, esse tipo de manifestação, como muitas outras, só servem para comprovar que as redes sociais não são apenas fontes de informação e relacionamentos, mas também uma forma de mobilizar e promover mudanças na sociedade, pois elas potenciam a comunicação e dão força a casos da vida real.

As redes sociais têm o poder de modificar o modo com que a nossa sociedade se comporta, influenciando rapidamente a opinião pública, por meio de partilha rápida de informações, o que está acarretando uma verdadeira revolução. As redes sociais também oferecem aspectos negativos como o *bullying,* que são actos de violência física ou psicológica[303]. Porém, muitas vezes são acções intencionais e repetidas, praticadas por um indivíduo ou grupo de indivíduos, causando dor e angústia.

---

[301] Martins, A. C. L (2019). *Discurso de ódio em redes sociais e reconhecimento do outro: o caso M. Minas Gerais*

[302] Ibid 300.

[303] Gnipper, P. (2017). *Uma análise sobre a propagação do ódio pela internet e suas consequências*

Trata-se de acções executadas dentro de uma relação desigual de poder e podem ainda fraudar a segurança de computadores ou redes empresariais[304].

Um outro problema está ligado com a disseminação de vírus, que colectam *e-mails* para venda de *mailing*; distribuição do material pornográfico (em especial, infantil), fraudes bancárias e violação de propriedade intelectual, ou mera invasão de *sites,* para deixar mensagens difamatórias ou insulto às outras pessoas[305].

Outro efeito colateral da internet e suas redes sociais é a partilha de arquivos de áudio e vídeo, além de livros digitais e outros tipos de propriedades intelectuais, sem a permissão dos legítimos autores. Essa prática vem fazendo com que a indústria, principalmente de entretenimento, crie mecanismos de controlo, que podem vir a ser considerados como censura[306].

3.2. A relação do discurso de ódio

Actualmente, estão disponíveis vários estudos ligados à relação do discurso de ódio nas redes sociais virtuais, com ênfase na dignidade da pessoa humana, face ao abuso da liberdade de expressão e suas limitações, elucidando seu contexto histórico e esclarecendo sua importância social[307]. Contudo, é uma realidade que a manifestação do pensamento

---

[304] Ibid 273.
[305] Ibid 301.
[306] Ibid 300.
[307] Ibid 303.

individual é feita de forma inadequada, sem se respeitarem os ditames éticos, com destaque para a intolerância, que enseja no acto ilícito e no abuso de direito[308]. Existem, ainda, pessoas que pensam e utilizam as redes sociais para exprimir um ponto de vista problemático, contribuindo com a propagação de *sites*, comentários ou publicações de cunho racista, preconceituoso e até mesmo com incitação à violência[309]. Outro revés das redes sociais é que as pessoas se apresentam em anonimato, de quem se escondem por trás das suas narrativas odiosas, vislumbrando os aspectos negativos e colaborativos a reiteração do discurso de ódio. Diante disso, se complementa com o apoio às ilimitações da liberdade de expressão, observando as normas de direito constitucional e as de direito[310].

O discurso de ódio nas redes sociais tem, por muitas vezes, ultrapassado os limites do bom senso, pois tem a finalidade de promover a violência, a discriminação ou o preconceito, em detrimento de um grupo ou classe de pessoas em razão das características inerentes do ser humano[311].

Esse tipo de discurso tem sido um dos grandes problemas da actualidade, pois contribuido para o fomento e incremento do tribalismo e regionalismo. Entretanto, os direitos fundamentais não são absolutos e, por isso, no momento em que outros

---

[308] Ibid.

[309] Ibid 301.

[310] Silva, D. L.(2018). C*rimes contra honra nas redes sociais: aspectos gerais*.

[311] Ibid 273.

direitos garantidos começam a ser ameaçados ou violados, vê-se a necessidade de se estabelecer uma determinada limitação ao uso da livre manifestação de pensamento em redes sociais e desenvolvimento de mais estudos ou pesquisas para a mitigação deste tipo de atitude.

E mais, os juristas não podem ficar longe deste cenário, porque se não forem encontradas formas da sua mitigação, corre-se o risco de estar-se numa sociedade onde se confunde a liberdade de expressão com o abuso de expressão[312].

Na sociedade actual, são certos os pensamentos de exclusão, e sabe-se que não se tem o direito de dizer tudo que não se pode falar de tudo em qualquer circunstância, e qualquer um não pode falar de qualquer coisa[313]. Assim sendo, quem profere discurso de ódio acredita ser permitido a dizer tudo sobre qualquer coisa, para qualquer um, em qualquer situação. Partindo desta lógica, o discurso de ódio e de incitação à violência contradiz os princípios e garantias fundamentais, tendo, por exemplo, que a manifestação odiosa de pensamento ou de incitação à violência não pode ser compreendida como parte legal da garantia constitucional da liberdade de expressão, caracterizando o abuso de direito[314].

As redes sociais são construídas a partir da criação de perfis de cada usuário, ao qual possibilita

---

[312] Ibid 301.

[313] Ibid 273.

[314] Ibid.

que outros usuários façam parte[315]. Sendo assim, o usuário não pode cadastrar-se para criar um mau ambiente ou desinformar, mas sim promover a informação real e relevante para a sociedade, promover entretenimento, gerar debates, viabilizar novos relacionamentos e até gerar negócios, em fim, construir uma grande teia social virtual[316]. E mais, todos nós devemos entender que o discurso é parte necessária para a formação de um grupo, tendo em conta que, através do discurso, permite-se encontrar pessoas com ideais semelhantes, bem como possibilita a criação de novos discursos, novos grupos, novas formas de pensamentos ou até mesmo a divergência de opiniões[317].

Mas, mesmo assim, em Moçambique, as redes sociais têm-se tornado um meio de exposição de opiniões odiosas e o local de externalização de preconceitos, onde cada indivíduo expõe os valores éticos reprováveis que traz, ou com que cresce na sua família. As redes sociais fazem nada mais que amplificar esse ódio e reafirmar os preconceitos que as pessoas já têm[318]. Com efeito, o discurso de ódio ocorre sem que as pessoas se importem com incitações ao crime, violência e possíveis danos morais e materiais, comprovando apenas que a nossa sociedade é extremamente intolerante a determinadas ideologias, género, raça, condição

---

315 Ibid.

316 Ibid 300.

317 Ibid 303.

318 Ibid 273.

sexual, dentre outros factores que sejam distintos do seu modo de pensar[319].

Portanto, podemos observar que as redes sociais se tornaram um ambiente precedido pela ignorância, propício ao discurso de ódio nada inclusivo às minorias sociais, em fim, verdadeiro caos contemporâneo. As redes sociais são, agora, um dos meios mais rápidos e eficazes de espalhar ideologias e posicionamentos de determinados grupos sociais sobre outros e, muitas vezes, se inserem como dominantes em suas condutas[320]. Além do mais, elas possuem um forte aliado para que o discurso de ódio se propague e gere cada vez mais medidas judiciais, e um exemplo disto são os chamados "*haters*", ou mais conhecidos como "aqueles que odeiam"[321].

Em redes sociais, as pessoas conseguem colocar a sua opinião de forma mais segura, justamente pelas possibilidades oferecidas pelo meio, como os *fakes* (perfis falsos que ocultam a identidade verdadeira) e a protecção física, visto que a comunicação é mediada pelos computadores e sempre procura-se encontrar pessoas que pensem da mesma forma, etc[322].

---

[319] Ibid 301.

[320] Ibid 303.

[321] Ibid 301.

[322] Freitas, R. S. & Castro, M. F. (2013). *Liberdade de Expressão e Discurso do Ódio: um exame sobre as possíveis limitações à liberdade de expressão.* Florianópolis.

Além da problemática do anonimato, que não é bom, os discursos de ódio transmitidos pelos *haters* são também influenciáveis aos demais usuários, que, por sua vez, acabam fazendo com que outras pessoas compactuem com a mesma linha de pensamento e participem com a mesma intensidade do discurso de ódio, bem como, os grupos atingidos comecem a defender os seus ideais, tornando-se uma discussão de ideologias entre grupos[323].

Nesta oportunidade, muitas vezes, as discussões ocorrem sem a existência da moral e do bom senso, ferindo, assim, várias garantias e princípios fundamentais, cometendo ilicitudes uns contra os outros e também contra uma colectividade participativa ou não da discussão[324].

A propagação do discurso de ódio nas redes sociais encontra-se num grau alarmante e, diante do crescimento desenfreado de usuários nas redes, depara-se com uma sociedade que acredita que a livre manifestação de pensamento, quando explanada nas redes sociais, não são passíveis de se configurar medidas judiciais, ocorrendo a má interpretação do direito à liberdade de expressão[325]. Assim sendo, não restam dúvidas que há sensação de impunidade quanto aos crimes e ofensas que são cometidos nas redes sociais, proporcionando, deste modo, a maior liberdade para que o ilícito ocorra, situação que é influenciada pela fraca

---

[323] Ibid 310.

[324] Ibid 322.

[325] Ibid.

implementação da lei de crimes virtuais, que, talvez, por meio desta, minimizava-se a propagação deste tipo de discurso, que em algum momento gera conflitos e, consequentemente, guerras[326].

4. ATAQUES E SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

4.1. Privacidade e segurança

Qualquer indivíduo pode, de livre e espontânea vontade, divulgar as informações que o relacionam. Mas existem situações em que, mesmo que este indíviduo queira manter a sua privacidade, a mesma pode ser exibida sem a sua vontade[327]. De entre os casos de invasão de privacidade, podem citar-se os seguintes[328]:

- Pessoas que divulgam informações sobre os outros ou mesmo suas imagens, donde também constam as imagens dos outros, antes de solicitar a autorização prévia destes;
- Indivíduos, sem autorização, colectam informações que circulam na rede, sem estarem

---

[326] Ibid 303.

[327] Campos, M. (2017**).** *Direito à privacidade no uso das redes sociais: Riscos decorrentes do excesso de exposição**.*** Brasil

[328] Francisco, A. F. M. (2012). *Privacidade em redes sociais centrada no utilizador recorrendo à Gestão de Direitos Digitais.* Lisboa

criptografadas, como o conteúdo dos *e-mails* enviados e recebidos por outros;

- ❖ Um atacante ou um código malicioso que obtém acesso dos dados que os outros digitam ou que estão armazenados no seu computador;
- ❖ Pessoas que invadem as contas de *e-mail* dos outros ou da rede social dos outros, com a finalidade de aceder a informações restritas;
- ❖ Os maldosos que invadem os computadores nos quais estão armazenados os dados dos outros, até um servidor de *e-mails*;

Nas redes sociais, assim como na internet, em geral, é preciso ter cautela e evitar fornecer dados pessoais como nome, *e-mail*, endereço e números de documentos para terceiros[329]. Também nunca devem ser fornecidas informações sensíveis, como senhas e números de cartão de crédito, a menos que esteja sendo realizada uma transacção comercial ou financeira e se tenha certeza da idoneidade da instituição que mantém o *site*.

O que se deve saber é que as informações que são geridas ou as que circulam nas redes sociais são, geralmente, armazenadas em servidores das instituições, que mantêm os *sites,* e trata-se de instituições desconhecidas. Com isso, corre-se o risco de estas informações serem repassadas sem a nossa autorização para outras instituições, ou

[329] Ibid 280.

para um atacante, que pode comprometer o nosso servidor ou obter as nossas informações[330].

Um *site* de redes de relacionamentos, normalmente, permite que o usuário cadastre informações pessoais, como nome, endereços residencial e comercial, telefones, *e-mail*, data de nascimento etc., para além de outros dados que irão compor o seu perfil.

Se o usuário não controlar o acesso dos seus dados, todas as suas informações poderão ser visualizadas por qualquer um que utilize o *site*. Com isso, é recomendável que o usuário evite fornecer muita informação a seu respeito ou institucionais, pois nenhum *site* está livre do risco de ser invadido e de ter suas informações furtadas por um individuo com más intenções[331].

É um facto que algumas pessoas expõem, nas redes sociais, toda a informação que as relaciona ou das suas instituições (incluindo as de defesa de segurança), colocando em causa a sua segurança e da sua instituição. São informações que podem ser utilizadas por alguém mal-intencionado e atentar contra a segurança física do próprio usuário ou do Estado[332].

Actualmente, as informações sobre os locais onde determinada pessoa frequenta são facilmente obtidos nas redes sociais. Assim sendo, é muito importante que o usuário esteja atento e avalie com

---

[330] Ibid 328.

[331] Ibid 327.

[332] Ibid 328.

cuidado que informações estarão disponíveis nos *sites* de redes populares, principalmente aquelas que poderão ser vistas por todos[333].

4.2. Ataques e incidentes em redes sociais

Não obstante as redes sociais proporcionarem as inúmeras vantagens para a sociedade, elas são, igualmente, uma séria ameaça à vulnerabilidade, principalmente aquelas de maior dimensão, ou com maior representatividade[334]. Uma das principais ameaças à segurança e privacidade dos usuários é proveniente do tipo de conteúdos e de informação que estes partilham nas redes sociais. Uma fotografia divertida actualmente, partilhada no *Facebook,* por exemplo, pode ser uma foto comprometedora no futuro, ou pode ser editada e transformada em uma outra fotografia extremamente comprometedora[335].

Existe alguma falta de conhecimento, por parte dos usuários, sobre o impacto que a partilha destes conteúdos e outros pode provocar. Os conteúdos partilhados presentemente numa rede social são distribuídos e partilhados por inúmeras pessoas e vão persistir na rede social, mesmo que a conta do usuário seja removida da rede, e não há retorno[336].

Na esteira profissional, estas redes sociais podem ser uma ameaça, uma vez que, actualmente,

---

[333] Ibid 327.
[334] Ibid 274.
[335] Ibid 327.
[336] Ibid 328.

as instituições recorrem às redes sociais como uma forma complementar de verificar o perfil dos candidatos e hábitos de uma certa sociedade. Entretanto, existe o sério perigo de quebra de confidencialidade, pelo facto dos colaboradores de uma organização, tal como quartel, divulgarem informação interna das suas organizações[337].

O *Facebook*, por exemplo, registou um crescimento exponencial nos últimos tempos, passando a ser a maior das redes sociais, com cerca de 400 milhões de utilizadores, em 6 anos de existência, e a sua dimensão torna-o o alvo preferencial para ameaças de diversos tipos. Do ponto de vista de quebra da privacidade consentida, o *Facebook* é extremamente agressivo[338].

Actualmente, o *Facebook* passou a apresentar valores de partilha com toda a rede social de informação pessoal. Porém, se nada for feito por parte do utilizador, todos os seus dados e conteúdos são partilhados com toda a rede e para sempre[339]. Tudo porque há falta de conhecimento por parte dos usuários em relação às implicações da divulgação da sua informação pessoal, privada e das instituições nas redes sociais. A este propósito, no *Facebook,* em particular, é possível constatar[340]:

- ✓ Pessoas que aceitam pedidos de amizade de estranhos;

[337] Ibid 274.
[338] Ibid 328.
[339] Ibid.
[340] Ibid 274.

- ✓ Jovens, da faixa etária entre 15 a 20 anos de idade, que divulgam as suas datas de aniversário;
- ✓ Utilizadores que divulgam o seu endereço de *e-mail* e dados sobre a sua família e amigos;
- ✓ Usuários disponíveis em partilhar ou extrapolar a sua própria informação pessoal, profissional, etc.

Estes factos têm contribuído para a ocorrência de ataques - roubo de identidade ou de engenharia social, por exemplo. Com isso, é pertinente utilizar racional e conscientemente as redes sociais e, sobretudo, ter consciência sobre que dados partilhar e que tipo de conteúdos a disponibilizar e para quem[341][342]. Um pouco de atenção durante a partilha de dados nas redes sociais pode melhorar, e muito, a privacidade e reduzir o risco de exposição às possíveis ameaças. As precauções a serem tomadas em consideração podem ser resumidas no seguinte[343]:

- ✓ Usar correctamente as listas de amigos;
- ✓ Remover os resultados de pesquisa do *Facebook*;
- ✓ Evitar a marcação em fotos e vídeos;
- ✓ Proteger ou restringir os álbuns de fotografias;
- ✓ Evitar que as histórias apareçam no *feed* de notícias dos seus amigos;

---

[341] Ibid 274.
[342] ____US.ARMY. *Social media and operations security.*
[343] Ibid 242.

- ✓ Proteger-se contra histórias publicadas por outras aplicações;
- ✓ Tornar a sua informação de contacto privada;
- ✓ Evitar *posts* que possam ser embaraçosos;
- ✓ Evitar publicar as informações profissionais, de carácter militar em particular.

As ameaças populares nas redes sociais, em particular as de maior dimensão, são cada vez mais perigosas. E uma das ameaças recentes no *Facebook* é quando o usuário é solicitado a instalar uma aplicação chamada "*Unnamed App"*, uma aplicação misteriosa que afecta os usuários[344]. Essas aplicações do *Facebook* são, na sua maioria, provindas de fabricantes terceiros, que se utilizam de dados do usuário[345]. No entanto, muitas vezes, elas podem ter comportamentos diferentes do que o esperado, inclusive enviar *links* indesejados que podem conter códigos maldosos.

4.2.1. As notificações via *chat*

Trata-se de pedidos disfarçados, que podem levar o usuário para outros *sites* na Internet e, alguns desses pedidos, servem para "bombardear" os utilizadores com publicidade não solicitada. E já existem casos concretos: por exemplo, em 2009, alguns *sites* foram afectados e uma destas ameaças deu-se pelo nome de *Koobface*, um *worm* que ataca

[344] Xavier, S. I. R. (2014).*Privacidade em redes sociais: uma análise da experiência dos usuários*. Belo Horizonte
[345] Ibid.

directamente os usuários de redes sociais como o *Facebook*, *MySpace* e *Twitter*[346].

O *Koobface* é muito perigoso, porque tenta, após infectar o sistema da vítima, obter informações diversas do usuário, tal como os números de cartões de crédito. Normalmente, espalha-se através do envio de mensagens do *Facebook* das pessoas amigas de um usuário, previamente infectado. Depois de recebida a mensagem, direcciona o receptor a um *site* Web, onde as vítimas são levadas a pensar na existência de uma actualização de uma versão recente do *software*[347]. Ao instalarem o arquivo, passam a ser, igualmente, infectados com o *Koobface,* passando a estar sob o controle do mesmo e passando a infectar mais usuários.

O Koobface é um *worm* tão sofisticado que é capaz de, entre outras coisas[348]:

- ✓ Registar uma conta no *Facebook*;
- ✓ Activar essa mesma conta através da confirmação do *e-mail* enviado para uma conta do *Gmail*;
- ✓ Fazer-se amigo de várias pessoas na rede social;

O Koobface é inteligente, a ponto de não adicionar muitos amigos por dia, para não chamar a atenção e colocar *posts* no mural de amigos com mensagens com *links* para sites ou para vídeos que são fontes de distribuição de *malware.*

---

[346] Ibid 274.
[347] Ibid.
[348] Ibid 344.

A outra grande ameaça identificada nas redes sociais foi o *worm* "*stalkdaily*", criado por um jovem de 17 anos, chamado Mikeyy Mooney. Este *worm* lançou pânico no *Twitter*, enviando mensagens aos utilizadores para visitarem o *site stalkdaily.com,* que infectava o perfil do visitante com uma conta de *Twitter* associada[349].

Por conseguinte as redes sociais (principalmente o *Facebook* e o *Twitter),* tornaram-se meios preferenciais para lançar diversos tipo de ataques: *phishing*, *malware*, roubo de dados e de identidade, *stalking*, entre outros. Estes atacam não apenas a ingenuidade dos utilizadores, mas, igualmente, a própria infra-estrutura onde assentam estas redes sociais[350]. Para isso, é importante reverem-se as políticas de privacidade dos media sociais, para que os usuários estejam conscientes do âmbito de partilha de informações pelas mesmas plataformas. Além disso, os usuários devem, sempre, desconfiar dos *links* que são partilhados por amigos, conhecidos e desconhecidos, e não instalar indiscriminadamente aplicações por terceiros sem, antes, saber do que se trata[351].

No *WhatsApp,* por exemplo, o maior problema está na facilidade de partilha de informações, e alguns usuários não investigam, antes, a proveniência dessas informações e que possíveis objectivos que, com elas, se pretendem, espalhando

[349] Ibid 274.
[350] Ibid.
[351] Ibid 344.

conteúdos que não interessam à sociedade ou que descredibilizam as instituições[352].

4.2.2. *Social-phishing*

É um ataque cujo objectivo é adquirir de forma fraudulenta informações confidenciais de uma vítima, através da personificação de uma terceira parte confiável[353]. Neste tipo de ataques, empregam-se iscas generalizadas onde, por exemplo, o invasor se faz passar por uma grande corporação bancária, para obter o rendimento monetário, apesar de não conhecer nada sobre a sua vítima, desde que o invasor conheça e confie na corporação bancária pela qual este está se fazendo passar.

4.2.3. Os perigos das redes baseadas em localização

As redes sociais baseadas em localização, como o *Foursquare,* incentivam o usuário a partilhar a sua localização actual com o resto do mundo ou com os seus amigos. E, ao fazer isso, o usuário está dizendo para as pessoas que não está em casa[354]. Existe, inclusive, um *site* na internet, denominado por *PleaseRobMe* (roube-me por favor), que mostra actualizações em tempo real dos usuários do *Foursquare,* que difundem os seus *check-ins* no *Twitter[285]*. Os mentores do *site*, Barry Borsboom,

---

[352] Ibid 344.
[353] Ibid.
[354] Ibid 274.

Frank Groeneveld e Boy van Amstel, tinham como objectivo criar uma consciência do problema e fazer as pessoas pensarem em como eles utilizam estes serviços como o *Foursquare, Brightkite, Google Buzz* etc"[355]. Contudo, na actualização da localização, o usuário informa que está de férias, revelando que deixou a sua casa sem guarnição.

Além disso, existem alguns usuários do *Foursquare* que fazem o *check-in* em lugares como "Casa", "*Home*", "Casa do Fulano", ou seja, em lugares não públicos e, assim, expondo publicamente as suas residências e mostrando aos usuários exactamente o lugar onde moram[356].

Quando se trata de serviços baseados em localização, ou redes geo-sociais, recomenda-se a utilizar serviços que permitam que o usuário envie a sua localização de forma privada para grupos específicos de amigos e para contactos confiáveis.

4.2.4. *Cyberstalking*

Cyberstalking é o assédio ou a comunicação indesejada vinda de alguma forma de tecnologia, incluindo computadores, sistemas de posicionamento global (GPS), telefones móveis, entre outros[357]. *Cyberstalking* é definido pelo *The National Center for Victims of Crime,* como o comportamento ameaçador ou avanços indesejados direccionados a outro, usando a internet e outras formas de comunicação *on-line*[287].

---

[355] Ibid 274.
[356] Ibid344.
[357] Ibid 274.

Em *Cyberstalkers,* os atacantes utilizam *e-mail*, salas de "bate-papo", fóruns de discussão, câmaras escondidas, entre outros, para atingirem as suas vítimas. É um acto de perseguição no *Facebook,* que inclui verificação de perfil de outrem e a adição de estranhos como amigos, para obter-se informações de interesse amoroso, entrar-se em contas de amigos para ter-se acesso a informações e ler-se murais de pessoas não conhecidas[358].

Actualmente, através *do cyberstalkers,* facilmente consegue-se visualizar o paradeiro da vítima, e existem aplicações recentes que utilizam *software* de tecnologia de posicionamento global (GPS) como *Foursquare,* que tornam o acto de encontrar as vítimas ainda mais fácil.

Algumas precauções para *cyberstalkers são*[359]:

- ✓ Considerar a idade da pessoa: aplicativos e *sites* baseados em GPS realmente não são apropriados para crianças. Um pouco de maturidade é um longo caminho à frente para manter-se um membro do *site* seguro. Treze anos considera-se uma idade razoável para conceder a utilização destes serviços às pessoas, mas vários *sites* nem permitem usuários menores de 18 anos.
- ✓ Postar mutações ou fotos de animais de estimação como identificadores para os jovens que fazem uso destes *sites*: não devem postar fotos reais de si mesmos como identificação, uma

[358] Ibid 344.
[359] Ibid.

vez que estas podem representar riscos de segurança.

- ✓ *Check-in* frequente da lista de amigos;
- ✓ Certificar-se que os amigos que recebem actualizações de GPS são-no, na vida real, e não membros de uma rede estendida, que pode incluir inúmeros desconhecidos.
- ✓ Confirmar que as configurações de segurança do *site* do aplicativo permitam somente seguidores desejados.
- ✓ Realizar "*check-in*" num local quando se estiver deixando-o, ao invés do momento da chegada, para minimizar a possibilidade de um encontro indesejado com alguém desconhecido.

5. O PAPEL DOS MÍDIAS SOCIAIS EM CRIMES ONLINE

Os *media* sociais têm tido grande papel nos crimes e, no caso das redes sociais, existem algumas ocasiões em que esses crimes não passam de mal-entendidos ou confusões, causadas por alguns usuários sem informação[360]. Geralmente, são casos sérios, em que a rede foi usada como evidência ou flagrante. Vejamos, a seguir, alguns casos em que o *Facebook* foi utilizado como meio para a prática de crimes[361].

---

[360] Júnior, E. L. (2009). *As redes sociais do crime organizado: a perspectiva da nova sociologia económica*

[361] Ibid 274.

- Uma mulher presa por acusar e notificar uma pessoa via Facebook[362]

Shannon Jackson, do Estado Tennessee, nos Estados Unidos da América, infringiu a lei por acusar outro usuário, via *Facebook.* Ela fez isso com o seu requerente, violando uma medida cautelar. Por isso, Shannon foi interdita a usar telefone para entrar em contacto ou fazer qualquer tipo de comunicação com o requerente, incluindo o *Facebook*.

- Traficante que vendia ecstasy no Facebook[363]

Daniel Izaías dos Santos foi preso após chegar ao Rio de Janeiro, com comprimidos de ecstasy, onde foi abordado por policiais e acabou preso em flagrante. A polícia chegou até a Izaías a partir de uma investigação da esquadra de Copacabana, que monitorava os registos do rapaz, identificado-o como grossista de uma quadrilha de traficantes na Internet. Em alguns *posts,* Izaías e seus amigos usavam códigos. No *Facebook,* por exemplo, os comprimidos de ecstasy eram chamados de laranjas.

- Duas meninas acusadas de *cyberstalking* por invadir a conta do *Facebook* da colega de sala de aulas[364]

---

[362]Informação obtida no site: Ihttps://abcnews.go.com/Technology/AheadoftheCurve/tennessee-woman-arrested-facebook-poke/story?id=8807685

[363] Informação obtida no site https://oglobo.globo.com/rio/preso-traficante-que-vendia-ecstasy-em-redes-sociais-2709110

[364] Ibid 274.

As adolescentes foram acusadas de perseguição *online* e invasão de computador, por entrarem sem permissão na conta do *Facebook* da colega de sala e postarem fotos e mensagens de conteúdo erótico. As meninas (de 11 e 12 anos, respectivamente) foram acusadas pelo Juiz da Infância e Juventude de King County, no Estado de Washington, em 18 de Março de 2011, porque postaram mensagens no mural da colega Leslie Cole, onde marcavam encontros sexuais, inclusive enviaram mensagens privadas a vários amigos, propondo diversos tipos de jogos eróticos.

Leslie, de 12 anos, fez questão de pedir que a *media* usasse o seu nome para chamar atenção ao *bullying* que algumas crianças têm cometido. As três meninas continuaram a assistir as aulas juntas, mas deixaram de se ver com frequência. A menina denigrida (Leslie) conseguiu uma medida cautelar, que impedia as duas invasoras de entrarem no mesmo autocarro escolar e de fazerem contacto por qualquer meio de comunicação.

- ❖ Adolescente preso por admitir ter contratado um assassino profissional pelo Facebook[365]

Corey Christian Adams, de 19 anos, foi preso depois de aceitar um acordo judicial no qual foi acusado de ter contratado um assassino profissional pelo Facebook, para matar uma mulher que o acusara de estupro. Corey também foi condenado por tentativa de assassinato e outras infracções. Depois que a mulher de 20 anos de idade alegou ter

[365] Ibid.

sido estuprada, Adams postou no seu mural uma oferta de 500$ por quem trouxesse sua cabeça.

❖ Homem preso por fazer uma solicitação de amizade no *Facebook*[366]

Dylan Osborn, um inglês de 37 anos, foi preso por um erro muito comum. Assim que entrou no *Facebook,* mandou solicitação de amizade para todos os seus contactos de *e-mail* sem saber, uma acção que é padrão no *Facebook*. No entanto, o problema surge porque, da sua solicitação de amizade, constava o *e-mail* da sua ex-esposa, Claire Tarbox, que já tinha conseguido uma medida cautelar contra o marido.

Dylan já havia sido acusado de abuso, por mandar diversas mensagens e fazer telefonemas sem permissão, e, com isso, o inglês foi mantido na cadeia por dez dias, mas ficou apenas sete, sob a alegação de que foi uma acção involuntária.

Como nota de fecho, importa chamar à colação algumas conclusões importantes sobre a segurança em redes sociais, nomeadamente:

✓ As redes sociais existem a partir do momento em que se formam grupos de pessoas partilhando informações com um objectivo em comum, e não apenas por aquilo que conhecemos como *media* sociais, *sites* de

[366]Informação obtida no site: https://revistaforum.com.br/blogs/mariafro/bmariafro-cuidado-fazer-pedido-de-amizade-ou-cutucar-alguem-no-facebook-pode-dar-cadeia/

relacionamento, ou até mesmo as chamadas redes sociais na *Internet*.

- ✓ As redes sociais funcionam como ferramentas de partilha de informações entre comunidades e estão, cada vez mais, presentes na rotina das pessoas, e podem ser acompanhadas 24 horas por dia e 7 dias por semana, devido à mobilidade da internet e acesso aos *media* por telefone celular ou outros dispositivos móveis.
- ✓ No que se diz respeito à segurança dos usuários, por se tratar de mídias relacionados com a maior rede de computadores, existem considerações quanto aos riscos inerentes ao uso da internet e à segurança da informação.

E os métodos práticos para manter os dados de cada usuário mais protegidos são[367][368][369]:

- ✓ A manutenção adequada do computador ou dispositivo que se conecte e troque informações com servidores de internet;
- ✓ Manter um bom programa de antivírus e actualizado, bem como sistemas de *firewall* que assegurem a integridade, a disponibilidade e a confidencialidade dos dados de cada um, para que eles não sejam alterados por nenhum código malicioso ou por um indivíduo mal-intencionado,

---

[367] Ibid 274,

[368] _____Manual de Exercito Brasileiro. Segurança nas redes sociais.

[369] Roza, A. F. (2016).*As redes sociais no mundo do crime*

de modo que estejam sempre disponíveis para quem, realmente, deve ter acesso na busca de determinadas informações;

Adicionalmente, o alerta é que os dados considerados sensíveis de cada usuário ou instituição, quando identificados na rede por terceiros, podem comprometer, inclusive, a segurança física de pessoas desprevenidas ou dados institucionais. É verdade que existem vantagens no uso da internet, como meio de interacção social utilizando os *media* sociais, com inúmeras opções de entretenimento, busca de informações e *networking*[370]. Mas, o desafio está em manter a consciência e mensurar não só a quantidade de informações e dados disponibilizados ou a disponibilizar na Web, como também a sua qualidade, tendo sempre presente as consequências que os conteúdos partilhados podem causar para a sociedade.

6. AS REDES SOCIAIS NOS AMBIENTES MILITARES OU OPERAÇÕES MILITARES (OPMIL)

Vivemos numa era moderna, onde o acesso às tecnologias de informação é cada vez mais elevado, dando lugar ao surgimento de diferentes atitudes e alianças na população local, que podem ser hostis, neutrais ou amigas[371]. Contudo, existem muitas

[370] Ibid 274.
[371] Ibid 280.

pessoas que criam informação nem sempre com boas intenções e, seguidamente, usam as redes sociais para a difundir. Entretanto, há que reconhecer que alguma dessa informação que circula nas redes sociais pode ser crítica e permitir a optimização da execução das missões militares, tais como missões de manutenção de paz, ajuda humanitária, entre outras[372].

6.1. Obtenção da consciência da situação (Situational Awareness - SA) em OPMIL

As redes sociais podem ser uma poderosa ferramenta para qualquer comandante, ajudando-o a compreender e moldar as áreas de responsabilidade[373]. O mais importante é os comandantes saberem utilizar as redes sociais, explorando as informações que nelas são veiculadas, para ajudar a influenciar as comunidades e melhorar a qualidade e pontualidade da partilha de informações relevantes para as operações[374]. Para isso, é importante que o Comandante procure manter, potenciar e empregar as redes sociais, para obter informações cruciais acerca de ameaças emergentes, compreender o

---

[372] Ibid.

[373] Kase, Sue E; Bowman, E. K ; Al Amin, M. T. & Abdelzaher, T. (2014). Exploiting Social Media for Army Operations: Syrian Civil War Use Case. i*n* Proceedings of SPIE - The International Society for Optical Engineering 9122.

[374] Ibid 280.

terreno do inimigo e enriquecer o quadro situacional do terreno das operações[375].

Na componente táctica e operacional, o comandante, a partir das informações que circulam nas redes sociais, pode tomar decisões mais informadas, sem ter que gastar bens ou recursos. E no nível estratégico, as redes sociais criam oportunidades para o estudo e compreensão da cultura e comportamentos locais, que de outra forma seria difícil interpretá-los ou obtê-los[376].

É evidente que, actualmente, as comunidades locais constituem uma grande fonte de observadores, que superam, em larga escala, os quantitativos de militares na mesma posição. A representação das comunidades locais nas redes sociais pode substituir o trabalho que os militares teriam em observar o ambiente, na busca de situação operacional[377]. E o mais importante de tudo isto é que estas comunidades podem possuir conhecimento linguístico, cultural e contextual, factores que podem apoiar na elaboração do quadro situacional por parte dos comandantes[378], e aqui subjaz a importância das redes sociais, enquanto

---

[375] Mayfield, T. D. (2011). A Commander's Strategy for Social Media**.** USA: U.S. Army.

[376] Zeng, D.;Chen,H.;Lusch,R. & Li, S.(2010). *Social Media Analytics and Intelligence. IEEE Intelligent Systems*,volume 25

[377] Ibid 280.

[378] Goolsby, R. (2010). *Social media as crisis platform: The future of community maps/crisis maps, In ACM Transactions on Intelligent Systems and Technology*, Volume 1

ferramentas que podem ajudar na comunicação intercultural e traduzir linguagens[379].

Outra característica relevante da inclusão das redes sociais nas operações militares é a possibilidade de reconhecer os dados e as informações que são considerados importantes pelas comunidades, os quais, igualmente, podem ser importantes para os comandantes avaliarem os efeitos de determinadas acções[380].

Entretanto, para a exploração das redes sociais, devem, em primeiro lugar, descobrir-se quais as redes mais utilizadas nas zonas operacionais e arrolarem-se as informações que frequentemente nelas circulam e seus potenciais consumidores[381].

Neste âmbito, é importante acompanhar, sempre que possível, as publicações de diversos actores, bem como os *bloggers* que veiculam informação todos os dias e as pessoas que normalmente partilham a informação[382]. Porém, a análise da informação que circula nas redes sociais, principalmente a referente à política, deve ser feita com muita atenção, pois muitas guerras são o resultado da luta pelo poder[383].

O outro grande desafio em utilizar as redes sociais para as OPMIL é separar a esfera pessoal

---

379 Ibid 375.
380 Ibid 342.
381 Ibid 280.
382 Ibid 378.
383 Carvalho, P. J. S. (2015). *A utilização das redes sociais por elementos militar: o uso simultâneo em ambientes de trabalho no âmbito da defesa*. Pedrouços.

da esfera profissional, pois os militares em operações são vários vezes alvos de sedução por parte de outros *users* das redes sociais[384]. Na verdade, muitos desses *users* 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[385]. Por isso, os militares, em nenhum momento, devem partilhar senhas operacionais em redes sociais, pois em um grupo pode haver um infiltrado.

Os EUA reconhecem as potencialidades das redes sociais para a obtenção da situação de consciência[386]. A título de exemplo, 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) obteve uma pista através da observação das redes sociais[387]. O analista falava Russo e encontrou um *post* feito por um separatista pró-russo na Ucrânia, através de um *website* das redes sociais da Rússia, chamado VK . Neste *post,* o separatista afirmava ter abatido um avião de carga militar ucraniano[388]. E, realmente, alguns analistas defendem mesmo que a primeira

[384] Ibid.
[385] Ibid 280.
[386] Ibid 373.
[387] Ibid 383.
[388] Ibid.

indicação de quem o abateu, com que arma, quando e como foi abatido proveio das redes sociais[389]. Adicionalmente, também afirma-se que, no Afeganistão, pode constatar-se a velocidade a que as informações foram injectadas nas redes sociais, sendo numa questão de segundos ou minutos depois do abate do avião da *Malaysia Airlines*)[390].

As redes sociais potenciam, e muito, a consciência da situação em operações militares, e quem não tiver acesso a elas está desactualizado. Nas redes sociais, a celeridade no acesso às informações é evidente, pois elas são publicadas em tempo quase real, logo após os acontecimentos, um dos aspectos que fazem delas uma ferramenta importante nas OPMIL[391].

A segurança dos militares em operações pode depender das redes sociais 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 redes sociais e tomam a sua decisão consoante os *posts* que observam[392].

Mas, refira-se que isto só é possível se existir uma consciência colectiva acerca das potencialidades das redes sociais. Dado que, na generalidade, todos os cidadãos têm necessidade de segurança e quase que todos publicam acerca

---

[389] Ibid.
[390] Ibid 280.
[391] Ibid 375.
[392] Barnes, J.E. (2014). *U.S. Military Plugs Into Social Media for Intelligence Gathering.*Washington

das ameaças e eventos perigosos[393]. No entanto, é importante estar-se ciente que nem todas as informações são fidedignas e, para isso, é necessário gerir a informação para saber identificar a sua veracidade.

As redes sociais ajudam na gestão da informação, pois permitem avaliar a credibilidade dos relatos e o cruzamento dos *posts* das redes sociais, que permitem, também, esclarecer determinados eventos como, por exemplo, distinguir se a informação comentada nas redes sociais é verdadeira ou não, qual é a intenção da pessoa que a publicou[394].

Essas plataformas permitem, ainda, saber se uma dada informação merece investigação e facilitam diferenciar uma ameaça de uma situação real. Através das redes sociais pode ter-se a ideia de como as pessoas pensam e os seus rostos[395]. Mas, uma das problemáticas que incide sobre a importância que se atribui aos conteúdos dos *posts* das redes sociais é saber se a informação não foi publicada por uma criança, numa brincadeira[396]. Mesmo assim, todas as publicações devem ser

---

393 Ibid 280.

394 Waterman, S. (2011). U.S. *Central Command 'friending' the enemy in psychological war: software helps crack terror cells*

395 Ibid 390.

396 Garside, D.; Ponnusamy, A.; Chan, S. & Picking, R. (2012).*Secure Military Social Networking and Rapid Sensemaking in Domain Specific Concept Systems:* Research Issues and Future Solutions.US.

encaradas com a mesma seriedade, mesmo sendo uma falsa e outra verdadeira, pois nunca se sabe ao certo quem está por detrás da publicação e qual a sua intenção com a mesma. E mais, as redes sociais têm bastante ruído, mas qualquer ameaça que tenha sido detectada deverá ser levada a sério[397].

O *Facebook* e o *Twitter* são as redes sociais que permitem 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 elas assumiram ao longo dos anos e escrutinar e filtrar essas fontes de informação, por fiabilidade e interesse[398].

Antes do advento das tecnologias, era necessário ter muito pessoal no terreno para a recolha da informação da situação militar; ao passo que, actualmente, à frente de um computador, é possível fazê-lo sem sair do local de trabalho, como se tivesse pessoal no terreno[399]. Trata-se de replicar aquilo que acontece no terreno e transpor para o mundo digital, porque as pessoas e a forma de funcionar não mudaram, mas o meio e a quantidade de informação, estes sim, mudaram. O mais importante é os analistas da informação terem a

---

[397] Ibid 280.

[398] *European Network and Information Security Agency* (ENISA) (2007)- Security Issues and Recommendations for Online Social Networks

[399] Ibid 394.

capacidade de cruzar a informação do pessoal empenhada no terreno com a informação digital[400].

Como exemplo, os EUAs investiram na concepção de programas computacionais para recolher as informações que são veiculadas nas redes sociais e proteger os seus programas[401]. Com efeito, em 2011 registou-se uma quebra de segurança, onde o *WikiLeaks* conseguiu saber que os EUA estavam a procurar obter um programa de computador, *Persona Management Software*, que iria permitir o comando *online* de unidades de identidades falsas nas redes sociais[402]. O programa dos EUA tem a capacidade de gerir 10 perfis por *user*, em que cada perfil teria uma história, experiência de vida, outros detalhes de apoio e uma ciberpresença consistente em termos técnicos, culturais e geográficos.

Outro exemplo está, igualmente, relacionado com os EUA, que dias depois, a 01 de Março de 2011, o comando militar dos EUA, localizado em Tampa, Florida, que gere os conflitos no Iraque e Afeganistão, comprou um programa de computador que permitia que os militares criassem identidades falsas nas redes sociais[403]. O objectivo, com estas identidades falsas, era dar aos militares a possibilidade de se infiltrarem em determinados grupos e, em certos casos, praticar desinformação

---

400 Ibid 373.
401 Ibid 342.
402 Diana, A.(2011). Air Force Seeks Fake Online Social Media Identities
403 Ibid 280.

dentro de organizações extremistas, como é o caso da *al-Qaeda* e dos *Taliban*, com o intuito de negar as operações[404]. Trata-se de um programa que tinha como objectivo aumentar o potencial da consciência situacional dos militares, através da apresentação, em tempo real, de informações locais pertinentes, para manter as identidades falsas, tais como informações acerca da hora, local, meteorologia e notícias[405]. Essas informações eram relativas à morada em que essa identidade falsa supostamente habita, permitindo que o militar esteja contextualizado e possa actuar em conformidade.

Através de programas computacionais dos EUA, os militares podiam assumir diferentes identidades falsas *online,* com diferentes objectivos operacionais, sem saírem do local de trabalho e sem terem medo de serem descobertos pelos adversários[406]. Estas identidades deviam ter a capacidade de aparecer em qualquer parte do mundo e interagir a partir das plataformas das redes sociais e serviços convencionais da internet. A cada identidade era dado um endereço IP, correspondente a diferentes regiões do globo, o que permitia iludir o inimigo quanto à localização do agente que está por detrás das identidades falsas[407].

O programa dos norte-americanos tinha a capacidade de fazer cruzamento de dados de todas

---

404 Ibid 375.
405 Ibid 390.
406 Ibid 280.
407 Ibid 390.

as redes disponíveis, onde se incluem o *Facebook*, o *Twitter*, o *MySpace*, entre outros, com o intuito de recolher dados pessoais e usá-los para conseguir acesso a outros *users* dentro desses círculos sociais[408].

Contudo, existem várias técnicas que se podem usar para tornar as identidades falsas mais reais. Por exemplo, tendo-se o conhecimento das escolas ou colégios frequentados pelos alvos, ou onde vivem, actuando-se em conformidade como se tivesse ligações reais com esses ambientes, podem obter-se informações úteis para as operações.

Em redes sociais, é fácil os alvos - ou inimigos - se infiltrarem e partilharem informações com as nossas forças, pelo que todo militar deve saber estar nas redes sociais. Porém, para ganhar-se o acesso a grupos privados nas redes sociais, o agente/bandido pode inscrever-se no nosso *website* oficial, fazendo-se passar por um dos nossos. O agente pode, igualmente, fazer-se passar por alguém que não é, podendo obter todas as informações que lhe interessam.

Em jeito conclusivo, referir que algumas redes sociais possuem várias ferramentas públicas, que podem potenciar a consciência da situação operacional militar[409]. Trata-se de ferramentas que podem ser utilizadas para ler o ambiente sociopolítico da área de operação ou onde a força está a operar, obter a percepção e efectuar a leitura de ideias, opiniões e sentimentos das populações

---

[408] Ibid 378.
[409] Ibid 280.

locais, sobre a intervenção militar em causa[410]. As redes sociais permitem, ainda, obter informações pontuais para planeamento de algumas acções militares, tais como a obtenção de informações de carácter ambiental ou de trânsito, manifestações e acções policiais.

6.2. A importância das redes sociais para a motivação dos militares

As redes sociais são uma ferramenta importante as Forças Armadas, pois, quando usadas apropriadamente, podem incrementar a motivação das tropas em OPMIL ou em formação, elevando a moral e o bem-estar dos militares e das suas famílias[411]. Para alguns militares, em missões no estrangeiro ou em pontos distantes das suas famílias, o acesso às redes sociais é uma prioridade, pois permitem manter a proximidade com os familiares e amigos[412].

O valor da integração das redes sociais nas Forças Armadas assenta nos benefícios que elas trazem aos militares em missões e às vantagens estratégicas que se podem explorar[413].

Os militares podem ser destacados para missões longas (em missões de apoio à Paz ou num teatro de operações dentro do território nacional, por exemplo), e, nesse contexto, as redes sociais são

[410] Ibid 390.
[411] Ibid 383.
[412] Ibid 378.
[413] Ibid 400.

uma componente indispensável, por permitir a comunicação destes com os seus familiares, tornando-se extremamente importantes no contexto das operações no estrangeiro e nos Postos de Comando[414]. Aliás, em missão, o *stress* decorrente do afastamento das famílias é notório e, nesse sentido, as redes sociais permitem aproximar os militares das suas famílias, resultando em motivação acrescida. As redes sociais beneficiam as operações, porque elas motivam os militares destacados e, como resultado, acabam se empenhando nas suas funções[415]. No mais, as redes sociais podem permitir ou dar notícias de um enorme espectro de familiares comodamente e com privacidade.

Como exemplo, Gonçalves (2015) afirma que, quando foi nomeado educador cívico 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 passássem o tempo, sempre que não estivessem a trabalhar[416]. Desta forma, os militares não só andavam satisfeitos, porque falavam com as famílias, mas também aliviavam algum *stress*. E mais, os seus familiares conseguiam saber que os parentes estão bem, além de evitar-se que os militares fossem a certos ambientes, como bares, o que os poderia desviar das suas funções

[414] Ibid 280.
[415] Ibid 373.
[416] Ibid 280.

principais[417]. E é importante notar que, se não existirem adequadas condições de *Welfare (bem-estar),* os militares podem tendencialmente procurar formas menos próprias de distraírem-se.

Costa (2015) também revelou as suas experiências, com a introdução das redes sociais em OPMIL[418]. Trata-se de um militar que comandou um destacamento militar, na Islândia, e que, apesar da importância das redes sociais, entretanto, reconhece os perigos associados ao seu uso pelos militares que, não raras vezes, o fazem procurando manter o ânimo, a moral e a motivação desconhecida[419]. Para tanto, contou com o apoio de um oficial das RP, para oferecer aos seus subordinados a possibilidade de publicarem, nas redes sociais, informações acerca do decorrer das operações, de forma controlada e segura, motivando-os e contribuindo para a tranquilidade dos familiares que, dessa forma, sabiam do paradeiro dos militares naquela operação[420].

6.3. (In) segurança Militar nas Redes Sociais

Nas subsecções anteriores, foi referido que as redes sociais são ferramentas de apoio às operações militares, uma vez que podem contribuir para o seu sucesso, embora se reconheçam,

---

417 Ibid 373.
418 Ibid 280.
419 Ibid 375.
420 Ibid 394.

igualmente, os perigos que elas representam, uma vez que o inimigo também está presente nelas, atento para captar informações sensíveis acerca dos objectivos militares[421]. Assim sendo, é um imperativo que todos os militares e as respectivas famílias compreendam a importância de observar boas práticas nas redes sociais, para que não se comprometa a segurança nas operações militares.

6.3.1. Perigos das Redes Sociais

Como referido anteriormente, as redes sociais podem ser um forte apoio na obtenção da consciência situacional (SA) contra o inimigo, mas, ao mesmo tempo, podemos ser nós a fonte de SA do mesmo do adversário. Neste sentido, as Forças Armadas devem proteger-se, observando as medidas de segurança e implementá-las[422]. O que se deve saber é que o ser humano é uma barreira frágil no que toca à segurança cibernética e aos *hackers,* e os manipuladores sociais sabem disso[423]. As suas acções aparentam ser inofensivas e legítimas, mas que, com elas, tentam conseguir enganar as pessoas, por forma a ultrapassarem as barreiras de segurança, que o pode resultar em graves consequências para o militar, para a família ou para as operações militares como um todo.

À partida, reconhece-se que é muito difícil controlar o que os militares publicam nas redes

---

421 Ibid 279.
422 Ibid 394.
423 Ibid 280.

sociais, entretanto, deve saber-se que é fácil que, através de um comentário ou uma fotografia, sejam divulgados dados ou informações que podem comprometer a segurança das operações, ou mesmo a integridade das Forças Armadas[424].

Com a proliferação dos *Smartphones,* com a capacidade de geolocalizar, fotografar, filmar e publicar directamente nas redes sociais, as Forças Armadas devem precaver-se dos riscos e perigos associados ao uso dessas plataformas, tomando as medidas necessárias, num contexto em que as redes sociais e outras tecnologias promovem o comportamento social e encorajam os *users* a partilharem informação e a confiarem naqueles a que estão conectados dentro das redes sociais[425]. O mais agravante é que há pessoas (no caso, militares) que partilham toda informação que lhe aparece, para serem considerados *updated men* (homens actualizados), com o risco de publicarem, de forma inocente, informações que pode comprometer a si mesmos ou à segurança do país.

O que vale ressalvar é que toda a informação que é publicada nas redes sociais deixa de ser privada, e que, mesmo que o *website* tenha boas definições de privacidade, existem muitas aplicações instaladas inconscientemente que permitem aos *hackers* o acesso às informações do equipamento[426].

---

[424] Ibid 394.
[425] Ibid 280.
[426] Ibid 390.

Até mesmo publicações que, à partida, parecem triviais, podem ser perigosas, podendo resultar em fatalidades. Os inimigos sempre procuram todas as informações possíveis em *blogs*, fóruns, *chats* e *websites,* principalmente as que contenham dados pessoais como o *Facebook*, *Twitter*, entre outros, para montarem um *puzzle* informativo, que os possibilite atacar[427].

Para tanto, aconselha-se que uma unidade das Forças Armadas possua uma equipa de especialistas na área de análise da informação em redes sociais e que esteja atenta aos *posts* dos militares, fazendo um mapa de um destacamento com base nas publicações, sejam fotografias, vídeos ou textos publicados[428]. E isso é possível através das técnicas de engenharia social.

Como se sabe, em redes sociais, facilmente se adiciona uma amizade, correndo-se o risco de adicionar um inimigo que, depois de estar dentro da nossa rede social, pode publicar fotografias, fazendo-se passar por um dos nossos, situação que, potencialmente, pode comprometer as operações militares.

No âmbito das redes sociais, de entre outras ameaças à segurança das operações militares, destacam-se as seguintes[429]:

- ✓ Incorporação de dados: os perfis das redes sociais podem ser descarregados para uma base de dados donde podem constar informações

[427] Ibid 280.
[428] Ibid 390.
[429] Ibid.

como: nome, idade, morada, local de trabalho, familiares, amigos, animais de estimação, gostos, locais de preferência, etc. Contudo, o mais importante, para a preservação da segurança, é remover das redes sociais tudo o que pode identificar os usuários como militares, principalmente antes do seu destacamento para a missão.

- ✓ Incorporação de dados secundários: para além da informação constante dos perfis, é possível recolher outros dados de cariz pessoal nas redes sociais, através dos *posts* e fotografias. Através das redes sociais, podem descobrir-se as pegadas dos alvos, na forma de *posts*, *tweets*, dados pessoais e outras informações publicadas pelo público-alvo. Se depois pegar-se em todos esses dados e informações recolhidas e fazer-se a filtragem e cruzamento, pode-se gerar conhecimento. Neste sentido, um adversário que procure informações nas redes sociais, ao analisar uma fotografia de um militar, pode retirar dela tudo o que seja informação classificada – como, por exemplo, armamento, aeronaves e a posição geográfica desse militar ou do quartel.

  Assim, os militares que utilizam as redes sociais, durante uma missão, devem evitar fazer publicações que mencionem o local e com quem estão no momento e/ou identificar os camaradas.
- ✓ Reconhecimento facial: nas redes sociais, as fotografias são muito populares e podem servir para identificar alguém e procurar mais

informações acerca dessa pessoa noutras redes sociais.

- ✓ *Content-based Image Retrieval* (CBIR): é uma tecnologia em ascensão, que permite relacionar características 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 quarto, com características particulares, é possível identificar onde esse quarto se encontra, se este estiver presente nessas bases de dados gigantes.
- ✓ *Click-jacking*: Consiste em disponibilizar hiperligações que aparentam ser inofensivas, mas que, quando *clicadas*, podem significar acções diferentes das pretendidas pela pessoa. E são executadas inconscientemente. 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 redes sociais, algumas tácticas de *click-jacking* foram usadas onde as hiperligações maldosas se encontravam camufladas nos botões de "*Like*" e "*Share*".

- ✓ *Doxing*: publicar informações de identificação pessoal de terceiros, incluindo o nome completo, a data de nascimento, a morada e imagens, retirados das redes sociais. Essas informações podem ser utilizadas para atacar o próprio militar, familiares ou amigos.
- ✓ Aliciação: Conversa estratégica, com o intuito de extrair informações das pessoas, sem que as mesmas sintam que estão a ser interrogadas.

- ✓ *Pharming*: Redireccionamento dos *users* de *websites* legítimos para *websites* fraudulentos, com o propósito de extrair dados confidenciais ou infectar o equipamento.

6.3.2. Comportamento dos Militares nas Redes Sociais

A principal preocupação com o uso das redes sociais é a segurança das operações. A OPSEC (*Operations Security*) é, cada vez mais, importantes pois as redes sociais são um meio de transmissão de informação que está a crescer muito rapidamente[430]. Para garantir a Segurança das Operações, todo o pessoal - incluindo as famílias e amigos do pessoal de serviço - tem a responsabilidade de assegurar-se que nenhuma informação publicada nas redes sociais possa constituir perigo para os militares, ou que possa ser usada pelos adversários como uma oportunidade de causar danos aos militares[431]. Entre os tipos de informações possíveis, destacam-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.

É verdade que as redes sociais dão a possibilidade aos militares de se expressarem, mas, mesmo fora de serviço, eles estão sujeitos a regulamentos próprios, e denegrir a imagem dos outros militares ou publicar informação sensível

---

[430] Ibid 290.

[431] O. C.P.A. (2011). *U.S. Army Social Media Handbook.*

deve ser punível. No entanto, é essencial que todos os militares saibam que, nas redes sociais, também estão a representar as Forças Armadas[432].

Na doutrina norte-americana, por exemplo, o uso das redes sociais pelos militares rege-se pelas normas de conduta[433]. E é severamente punido o militar que fazer comentários ou qualquer tipo de publicações que violem essas normas.

No nosso caso, também as redes sociais devem ser encaradas pelos militares como algo que pode trazer consequências reais e, como tal, os seus comportamentos deverão ser sempre cuidadosos, tal como são no dia-a-dia. Por isso, enquanto membros das FADM, 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. Nesta perspectiva, quem tiver um comportamento impróprio nas redes sociais deve ser punido, tal como se o fizesse num café com amigos[434]. Os militares das FADM devem ter, sempre, a noção dos seus deveres aos quais juraram cumprir, conscientes de que têm o dever de respeitar os regulamentos a que estão sujeitos e do perigo que a comunicação, através das redes sociais, pode representar para a vida instituicao militar.

---

[432] Ibid 383.

[433] U.S. DEPARTMENT OF DEFENSE (DOD) – DoD *Social Media Hub*

[434] Ibid.

Para isso, as Forças Armadas devem criar políticas de sensibilização aos militares, informando-os, sempre, dos perigos reiais das redes sociais. No caso das Forças Armadas dos EUA, as políticas que regulam o uso das redes sociais estão claramente definidas e são acessíveis 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*[435]*.*

Nas publicações feitas pelos órgãos supra-referidos, são mencionados diversos documentos pelos quais os militares se deverão reger, bem como os comportamentos que deverão adoptar nas redes sociais[436]. Dos vários perigos das redes sociais, há um que se destaca - o *Geotagging* – no qual os militares não se podem identificar geograficamente e nem usar aplicações nas redes sociais que possibilitem a geolocalização, seja em operações, treino, ou serviço, em locais cuja identificação espacial em formato de coordenadas possa comprometer as OPMIL[437]. Nesse sentido, durante as operações, os militares devem desactivar a função GPS dos seus *Smartphones*, caso contrário, as OPMIL poderão ser comprometidas.

Outros comportamentos a adoptar pelos militares nas redes sociais, consistem em evitar mencionar o posto, localização da base, datas dos

[435] Ibid 342.
[436] Ibid 430.
[437] Ibid 280.

destacamentos, nomes, especificações e capacidades de equipamento[438].

6.3.3. Consciência dos Militares das Forças Armadas sobre as redes sociais

Em muitas Forças Armadas, ainda há pouca consciência sobre a segurança baseada nas redes sociais, quer por parte dos militares destacados em missões, quer não. Entretanto, este problema, pouca consciência dos militares durante a utilizacao das redes sociais, deve ser encarado como algo sério em que se deve investir com políticas e estratégias acertadas, de modo a reduzir ou anular publicações prejudiciais a segurança[439]. É factual que há militares que publicam, nas redes sociais, imagens ou os vídeos “triturando” os inimigos. Essa acção pode ser vista como uma forma de desencorajar a sociedade a aderir a actos de violência ou a demostração do sucesso nas operações. Mas isto pode criar raiva e revolta nos inimigos, além de expor os acampamentos das nossas forças[440].

6.3.3.1. Experiência

O Coronel Costa, Oficial da Academia Militar da Força Aérea de Portugal, enquanto comandante de destacamento na Islândia, uma das suas grandes preocupações foi controlar a informação que era

[438] Ibid 430
[439] Ibid 394.
[440] Ibid 430.

publicada nas redes sociais pelos militares destacados[441]. O facto deveu-se à quantidade de meios que permitiam veicular informação classificada para essas plataformas e a dificuldade que existia em controlá-la. Para isso, com a cooperação de um oficial das relações públicas, aos militares foi-lhes dada a liberdade de fazerem publicações nas redes sociais, mas, ao mesmo tempo, os conteúdos eram monitorados e filtrados, satisfazendo-se, assim, os membros do destacamento ao publicarem o seu trabalho e as suas experiências, garantindo-se, simultaneamente, o controlo parcial da situação[442].

Uma vez que o controlo das publicações nas redes sociais nunca é supremo, desde a preparação do destacamento até aos *briefings*, os militares sempre foram consciencializados a publicarem informações que não comprometessem a segurança das operações[443]. Neste sentido, as publicações eram, primeiro, monitoradas e avaliadas em termos de segurança para, depois, serem publicadas num *blog* do *website* do Estado-Maior da Força Aérea, criado para o efeito. Neste *website*, desde o início do destacamento, eram publicadas informações sobre a operação, fotografias e entrevistas em que os militares retratavam o seu dia-a-dia e partilhavam com os seus familiares.

---

441 Ibid 280..
442 Ibid 376.
443 Ibid 280.

Muitas das publicações, no *website,* eram depois reproduzidas nas redes sociais da Força Aérea e, eventualmente, nas pessoais de cada militar[444]. O sucesso desta prática deveu-se à formação e sensibilização dos intervenientes em relação à materia.

6.3.3.2. Consciencialização

No âmbito das Forças Armadas, é necessária a sensibilização dos militares e a criação de políticas e guias práticos de utilização das redes sociais e das tecnologias[445]. Entretanto, não basta criar políticas, pois estas só serão eficazes se forem cumpridas. As políticas devem ser capazes de regular o comportamento do militar nas redes sociais. Por conseguintes, além das políticas, deve haver outras acções que levem o militar a saber cumprir as referidas políticas.

Porém, tal só é possível através de exemplos práticos, guias, programas formativos nas instituições militares de ensino, pesquisas, palestras, filmes, entre outros recursos[446]. No fundo, trata-se de consciencializar os militares sobre o uso das redes sociais – no meio castrense - do ponto de vista das suas vantagens e desvantagens.

A cultura de segurança nos quartéis ou Postos de Comando deve ser mantida e controlada, e, muitas vezes, ela traduz-se num problema

---

[444] Ibid.
[445] Ibid 375.
[446] Ibid 430.

organizacional, motivado pela incompreensão e pelo incumprimento dos regulamentos e procedimentos de segurança aprovados[447]. Nesta vertente, se os militares não possuírem a formação e o treino adequados, não poderão prevenir, detectar e reagir aos incidentes de segurança, tornando-se mais vulneráveis a ataques de engenharia social. Se as instituições de defesa e segurança deixarem de lado os aspectos de segurança, tornam-se instituições de lazer, ou humanitárias[448].

Alguns autores olham para a questão da sensibilização dos militares sobre a segurança *versus* uso das redes sociais com muita preocupação. A título ilustrativo, Costa (2015) defende que a ingenuidade é muito grande por parte das pessoas, no que tange às matérias relacionadas com as quebras de segurança, ao nível das redes sociais, e que, na maior parte, são inconscientes. Tal seria facilmente resolvível com explicações, instruções e briefings[449]. Por seu turno, EC (2015) admite que, actualmente, são feitas acções de sensibilização e formação na utilização das redes sociais no âmbito pessoal, o que permite que não se comprometa a segurança da operação (pessoas e bens) e dos militares que vão para as missões, algo que Simões (2015) constata como uma verdade, referindo que, na preparação para a missão que desempenhou no Afeganistão, recebeu uma

[447] Ibid 280.
[448] Ibid 430.
[449] Ibid 431.

palestra acerca das quebras de segurança nas redes sociais.

Entretanto, e apesar de haver mecanismos que possam contribuir para acautelar os riscos de segurança associados às redes sociais, registam-se casos em que os mesmos não são observados. Para elucidar, Gonçalves ressalta a falta destas opções salientando que, enquanto esteve em operações, no Afeganistão, não recebeu e nem soube de ninguém que tivesse recebido qualquer briefing acerca da utilização das redes sociais[450], o que foi mau.

7. REFERÊNCIAS

_____Manual de Exercito Brasileiro. Segurança nas redes sociais.

____US.ARMY. *Social media and operations security*. Acedido no dia 22 de Maio de 2019 em: https://sill-www.army.mil/428thfa/Social_Media/socialmediaopsec810-.pdf

Abreu, L. F. S. (2011). *A segurança da informação nas redes sociais*. São Paulo.

Barnes, J.E. (2014). *U.S. Military Plugs Into Social Media for Intelligence Gathering.*Washington. Acedido no dia 17 de Outubro de 2019 em: https://www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557

[450] Ibid 280.

Carvalho, P. J. S. (2015). *A utilização das redes sociais por elementos militar: o uso simultâneo em ambientes de trabalho no âmbito da defesa*. Pedrouços.

Cardoso, S. C.; Zago, C. & Silva, *b. v.(2018). Discurso de ódio nas redes sociais: dignidade da pessoa humana face o abuso da liberdade de expressão e suas limitações*. Brasil.

Campos, M. (2017). *Direito à privacidade no uso das redes sociais: Riscos decorrentes do excesso de exposição.* Brasil*.*

Diana, A. (2011). Air Force Seeks Fake Online Social Media Identities. Acedido no dia 17 de Outubro de 2019 em: https://www.darkreading.com/risk-management/air-force-seeks-fake-online-social-media-identities/d/d-id/1096228

European Network and Information Security Agency (ENISA) (2007)- Security Issues and Recommendations for Online Social Networks. Acedido no dia 17 de Outubro de 2019 em: https://www.ifap.ru/library/book227.pdf

Francisco, A. F. M. (2012). *Privacidade em redes sociais centrada no utilizador recorrendo à Gestão de Direitos Digitais.* Lisboa

Garside, D.; Ponnusamy, A.; Chan, S. & Picking, R. (2012).*Secure Military Social Networking and Rapid Sensemaking in Domain Specific Concept Systems*: Research Issues and Future Solutions.US. Acedido no dia 17 de Outubro de 2019 em:

https://www.researchgate.net/publication/267202217_Secure_Military_Social_Networking_and_Rapid_Sensemaking_in_Domain_Specific_Concept_Systems_Research_Issues_and_Future_Solutions

Gnipper, P. (2017). *Uma análise sobre a propagação do ódio pela internet e suas consequências.* Acedido no dia 12 de Julho de 2019 em: https://canaltech.com.br/comportamento/uma-analise-sobre-a-propagacao-do-odio-pela-internet-e-suas-consequencias-100018/

Goolsby, R. (2010). *Social media as crisis platform: The future of community maps/crisis maps, In ACM Transactions on Intelligent Systems and Technology,* Volume 1. Acedido no dia 17 de Outubro de 2019 em: https://dl.acm.org/doi/10.1145/1858948.1858955

Júnior, E. L. (2009). *As redes sociais do crime organizado: a perspectiva da nova sociologia económica*. Acedido no dia 20 de Julho de 2019 em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-69092009000100004&lng=pt&nrm=iso&tlng=pt

Kase, Sue E; Bowman, E. K ; Al Amin, M. T. & Abdelzaher, T. (2014). *Exploiting Social Media for Army Operations: Syrian Civil War Use Case*. i*n* Proceedings of SPIE - The International Society for Optical

Engineering 9122. Acedido no dia 22 de Outubro de 2019 em: https://www.researchgate.net/publication/268520959_Exploiting_social_media_for_Army_operations_Syrian_crisis_use_case

Lima, H. G. A. (2015). *Percepção e riscos na utilização de redes sociais (facebook) por parte dos militares cabo verdianos*. Braga.

Lorenzo, E. M. (2013). *A Utilização das Redes Sociais na Educação.* 3ª ed., Rio de Janeiro.

Martins, A. C. L (2019). *Discurso de ódio em redes sociais e reconhecimento do outro: o caso M. Minas Gerais*. Acedido no dia 12 de Julho de 2019 em: https://www.scielo.br/scielo.php?pid=S1808-24322019000100203&script=sci_arttext

Mayfield, T. D. (2011). A Commander's Strategy for Social Media. USA: U.S. Army. Acedido no dia 17 de Outubro de 2019 em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a535374.pdf

Muleta, D. M. D. (2015). *O impacto das redes sociais nas operações militares*. Sintra.

O. C.P.A. (2011). *U.S. Army Social Media Handbook.* Acedido no dia 12 de Agosto de 2019 em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a549468.pdf.

Romi, F. A. B. L.(2013). A *análise das redes sociais informais com foco no crescimento profissional das pessoas: um estudo de caso.* Niterói

Roza, A. F. (2016**).** *As redes sociais no mundo do crime*. Acedido no dia 20 de Julho de 2019 em: https://canalcienciascriminais.jusbrasil.com.br/artigos/344826698/as-redes-sociais-no-mundo-do-crime

Sarlet, W. (2018). *Liberdade de expressão e discurso de ódio na internet e a jurisprudência da CEDH.* Acedido no dia 12 de Julho de 2019 em: https://www.conjur.com.br/2018-out-26/direitos-fundamentais-liberdade-expressao-discurso-odio-redes-sociais

Silva, D. L.(2018). C*rimes contra honra nas redes sociais: aspectos gerais***.** Acedido no dia 20 de Julho de 2019 em: http://iccs.com.br/crimes-contra-honra-nas-redes-sociais-aspectos-gerais-davi-luiz-da-silva/

U.S. DEPARTMENT OF DEFENSE (DOD) – DoD Social Media Hub. Acedido no dia 20 de Julho de 2019 em: https://dodcio.defense.gov/Social-Media/Terms-of-Service-Agreements/

Waterman, S. (2011). *U.S. Central Command 'friending' the enemy in psychological war: software helps crack terror cells.* Acedido no dia 17 de Outubro de 2019 em: https://www.washingtontimes.com/news/2011/mar/1/us-central-command-friending-the-enemy-in-psycholo/

Xavier, S. I. R. (2014).*Privacidade em redes sociais: uma análise da experiência dos usuários*. Belo Horizonte.

Zeng, D.;Chen,H.;Lusch,R. & Li, S.(2010). *Social Media Analytics and Intelligence*. IEEE Intelligent Systems,volume 25. Acedido no dia 17 de Outubro de 2019 em: https://dl.acm.org/doi/10.1109/MIS.2010.151.

Os autores

Nelson Manuel A. Chapala

Coronel das Comunicações, Director Científico da Academia Militar “Marechal Samora Machel”, Investigador nos Centros de Investigação do Instituto Superior de Estudos de Defesa “Tenente-General Armando Emílio Guebuza” (ISEDEF) e de Pesquisas em Energias da Universidade Eduardo Mondlane (UEM), Docente, Doutorado em Ciência e Tecnologia de Energia – Eficiência Energética, Mestrado em Informática pela Escola Superior Técnica da Universidade Pedagógica de Moçambique e Engenheiro Electrotécnico pela Academia Militar “Marechal Samora Moisés Machel” e Faculdade de Engenharia da Universidade Eduardo Mondlane.

Nélido Dinis S. Atumane

Major das Comunicações, Técnico Superior no Serviço de Segurança Informática, na Repartição de Informática, no Departamento de Comunicações/EMG, Investigador, Mestrado em Informática pela Escola Superior Técnica da Universidade Pedagógica de Moçambique e Engenheiro Electrotécnico pela Academia Militar “Marechal Samora Moisés Machel” e Faculdade de Engenharia da Universidade Eduardo