SISFRON

Vetor da Guerra de Informação na fronteira terrestre brasileira

*Dardano do Nascimento Mota**

Introdução

O século XXI vem sendo marcado pelo aumento da velocidade de transmissão de informações provenientes das mais diversas fontes, sejam elas estatais ou não. Tais dados têm transitado por meio de ferramentas de Tecnologia da Informação (TI) cada vez mais complexas e integradas. Esse cenário vem intensificando as disputas entre atores governamentais e não governamentais por poder, influência e recursos financeiros.

Somado a isso, a quantidade de informação, cada vez mais ampla, difusa e variada, está exigindo maiores conhecimentos, capacidades e recursos para armazená-la e manuseá-la. Esse aspecto está conferindo grande dinamismo à realidade atual, marcado pelo grande compartilhamento de informações, impactando todas as expressões do poder, particularmente a econômica, militar e científico-tecnológica.

Como exemplo,

> no ano 2000, o estudo do genoma humano levou vários anos, a um custo de US$ 50 milhões, hoje ele pode ser realizado em um dia, por mil dólares. [...]. O mesmo se aplica à revolução da Informação. Muito mais informações são geradas a cada dois dias que nos últimos 2 mil anos. Essa possibilidade leva a crer que haverá maior volatilidade nos domínios informacional, físico, infraestrutural e conceitual. (JOHNSON, 2015, p. 50)

Nesse contexto de grande complexidade, está inserido o Sistema Integrado de Monitoramento de Fronteiras (SISFRON), um importante instrumento do Estado, conduzido pelo Exército Brasileiro, no combate ao atual cenário de grande trânsito de ilícitos transnacionais que passam pelas fronteiras terrestres do país.

O SISFRON foi oficializado pela Diretriz de Implantação, aprovada pela Portaria nº 193-EME, de 22 de dezembro de 2010. Ele vem sendo implantado, em uma primeira fase, na 4ª Brigada de Cavalaria Mecanizada, sediada em Dourados-MS, com o objetivo de

> prover as estruturas física e lógica apropriadas ao ciclo de Comando e Controle em todos os escalões do processo decisório, contemplando enlaces adequados para as comunicações entre todos os níveis, com capacidade de transmissão coerente com a missão atribuída e com a possibilidade de operar em rede, de acordo com o que estabelece a Estratégia Nacional de Defesa. (BRASIL, 2010b, p. 24)

* Maj Com (AMAN/00), pós-graduado em Ciências Militares (EsAO/09). Atualmente, é aluno do 2º ano da ECEME.

O SISFRON está baseado em três pilares: monitoramento, sensoriamento e apoio à decisão. Essa característica o reveste de grande envergadura tecnológica, uma vez que, para atendê-la, são necessários equipamentos que demandam capacitações específicas para operá-los. Isso impõe a sua compartimentação em subsistemas.

Nesse sentido, o SISFRON, por possuir em seu escopo subsistemas com perfis distintos, mas trabalhando de forma integrada, bem como por seu emprego dual, tem-se mostrado relevante, não só para o Exército Brasileiro, mas também para a sociedade, como gerador de segurança, emprego e renda. Isso o qualifica como um importante agente para as expressões política, econômica e científico-tecnológica do país no combate aos ilícitos transnacionais.

Ainda no contexto de velocidade de transmissão de dados e de disputas por poder e influência no campo informacional, vem ganhando cada vez mais força a chamada Guerra de Informação. É importante ressaltar que esse é um conceito atual e vem sendo estudado em diversas literaturas.

O Livro Branco de Defesa Nacional atesta que

> outros desafios que se apresentam ao país dizem respeito à sua capacidade de fazer face aos chamados "conflitos do futuro", quais sejam, **as guerras de Informação**, e os conflitos de pequena escala, caracterizados por origem imprecisa e estruturas de comando e controle difusas, que operam com o uso de redes sociais. (BRASIL, 2012, p. 28) (grifo nosso)

Da mesma forma,

> a **guerra de Informação** apresenta-se tanto na dimensão militar quanto civil. No meio militar, ela se apresenta na guerra centrada em redes e, no civil, é travada no escopo da sociedade do Conhecimento. Esta última, quando bem empregada, proporciona aos comandantes de todos os níveis a consciência situacional[1] necessária ao seu escalão. Outra maneira de classificar a guerra de Informação é dividi-la em dois grupos: a guerra de comando e controle e a guerra econômica. (FONTENELE, 2008, p. 1) (grifo nosso)

Este artigo tem por objetivo abordar o SISFRON como um sistema que demandará: o envolvimento de outras agências federais, o constante incremento orçamentário do Estado e o seu fortalecimento em pessoal e equipamentos na região da Tríplice Fronteira (Paraguai, Argentina e Uruguai), tudo inserido no contexto da Guerra de Informação.

Desenvolvimento

A Guerra de Informação é muito abrangente, sobretudo no que tange aos perfis dos atores nela envolvidos. Essa abrangência se deve, entre outros fatores, à presença dos meios de TI, que estão ao alcance da maioria das pessoas e têm contribuído para conduzir o Conhecimento a grandes distâncias e a grupos totalmente distintos.

Reto Haeni (1997, p. 3) traz a seguinte definição para Guerra de Informação:

> *Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information based processes, information systems, and computer-based networks.*[2]

As organizações criminosas, por disporem de recursos financeiros e capacitação técnica, também podem empregar os meios de TI na execução de suas ações.

Isso está reforçado na ideia de que:

> O crime organizado não é um fenômeno novo. Não está vinculado a nenhuma religião ou ideologia. Não é próprio de uma cultura ou de um povo em particular, mas sim o resultado da própria história da humanidade. Há muito tempo tem-se convivido com essas ameaças que constituem o caráter variado do crime organizado, como: a lavagem de dinheiro, o contrabando, o tráfico de drogas e armas, a corrupção etc. **O grande diferencial que o caracteriza atualmente é a sua conversão de um fenômeno localizado para um problema transnacional com patamares globais de atuação.**
> Esse tipo de comportamento delitivo teve seu auge e diversificação nas últimas décadas. Aproveitou-se o fenômeno da globalização **e do acelerado avanço tecnológico**, especialmente, nas áreas de transporte e **telecomunicações**, para expandir suas atividades, beneficiando-se, ora das facilidades resultantes do movimento global, como a nova forma da geopolítica, a permeabilidade das fronteiras e o mercado internacional; ora pelas falhas decorrentes desse mesmo processo, como a desregulamentação do sistema financeiro mundial e a deficiência dos Estados no controle referente aos movimentos de desterritorialização. (RODER, 2007, p.20) (grifo nosso)

Dessa maneira, surgem alguns questionamentos. O primeiro deles, ainda que pareça óbvio, se refere à informação. Afinal, o que ela vem a ser?

Para o presente trabalho, "informação" será definida como:

> Representação inteligível de objetos, estados e acontecimentos nos domínios real, virtual e subjetivo. Integra processos para a construção do conhecimento, o que promove a compreensão precisa e atualizada do ambiente operacional. (BRASIL, 2014a, p. 4-17)

Outros aspectos importantes se referem a: em que medida os meios de TI vêm influenciando as ações das diversas organizações criminosas na faixa de fronteira terrestre brasileira?

Muitas respostas e, até mesmo especulações, vêm à tona diante do questionamento apresentado. É notório o emprego de tecnologias da informação também no combate à criminalidade. No entanto, por que os ilícitos transnacionais seguem avançando?

Essa pergunta tem estreita ligação com ameaças como o tráfico de drogas, de armas e de pessoas e o descaminho, entre outros.

A despeito da abrangência do assunto em tela, o presente artigo analisa criticamente o caso brasileiro, tendo o SISFRON como um ator importante inserido no contexto da Guerra de Informação. Nesse sentido, emerge outra questão: em que medida o SISFRON pode atuar dentro da Guerra de Informação, provendo a necessária superioridade de informação ao Estado contra as supracitadas ameaças?

A resposta para este último questionamento é a ideia chave da presente reflexão integradora.

Era da Informação

O mundo do século XXI tem-se mostrado cada vez mais dependente da transmissão de dados por intermédio de meios digitais a grandes distâncias e em curtos espaços de tempo. Dessa forma, dada a gran-

de relevância da informação, como uma ferramenta para a construção de estruturas em todos os campos do poder, analistas de cenários prospectivos como Alvin Toffler e Manuel Castells apresentam a evolução das sociedades humanas em "Eras".

Nesse sentido,

> a "Era da Informação" sucedeu a "Era Industrial". Na "Era da Informação", quem controlar o domínio sobre o conhecimento influenciará decisivamente a sociedade e provocará mudanças tão profundas nesta como as que foram introduzidas na sociedade pela Revolução Industrial. (TOFFLER, 2003)

A Era da Informação está relacionada a três segmentos importantes: tecnologia, cultura e política. Eles estão interconectados, construindo um todo que formou, a partir dos anos 1970, uma nova estruturação social (CASTELLS, 2011). Dentro da linha de pensamento de Manuel Castells,[3] o presente artigo aborda o segmento tecnológico, sendo este diretamente relacionado à Tecnologia da Informação, particularmente às estruturas em rede.

Complementando essa ideia,

> a Era da Informação impôs às organizações a necessidade de funcionarem em Rede e, nestas novas formas de comunicação, desenvolveu-se também uma "nova lógica para o processo decisório – a Rede". (NUNES, 2005)

Aprofundando a análise da Era atual, podemos constatar dois pontos de intersecção desta com a Guerra de Informação. O primeiro se refere ao emprego de ferramentas baseadas em TI, e o segundo, ao fato de que ambas possuem a informação como matéria-prima principal em suas "mecânicas" de funcionamento. Esses pontos estão reforçados na ideia de que a Era da Informação "está caracterizada pela relevância da aplicação dos conceitos associados à TI nas diversas áreas da gestão e das atividades do dia a dia" (BRASIL, 2010a, p.46).

Assim, dados os supracitados pontos de intersecção, é lícito afirmar que o SISFRON está plenamente inserido na Guerra de Informação, uma vez que esse Sistema também possui a informação como matéria-prima essencial que irá alicerçar a chamada Consciência Situacional e está baseado, na sua maior parte, em estruturas de TI. Isso será constatado no tópico que abordará os subsistemas do SISFRON.

O cenário de ilícitos transnacionais

No que se refere aos ilícitos transnacionais, o Livro Branco de Defesa Nacional (2012, p. 259) os divide em

> dois grandes segmentos: o dos crimes contra a pessoa, englobando o narcotráfico, o tráfico de armas e munições, o tráfico de pessoas e o contrabando de migrantes; e o dos crimes financeiros, como a corrupção e a lavagem de dinheiro. **Ainda se destaca o crime cibernético, como manifestação da abrangência global e da crescente complexidade técnica das atividades criminosas.** (grifo nosso)

Essa conceituação apresenta a importância dos meios de Tecnologia da Informação e seu emprego por parte das organizações criminosas na execução dos ilícitos transnacionais. Isso fica ainda mais evidenciado com os crimes cibernéticos.

Isso posto, ao trazermos para a realidade brasileira, particularmente para a sua

País	Fronteira seca (km)	Rios/Lagoas (km)	Total (km)
Guiana Francesa	303	427	730
Suriname	593	-	593
Guiana	908	698	1.606
Venezuela	2.199	-	2.199
Colômbia	835	809	1.644
Peru	992	2.003	2.995
Bolívia	3.423	751	4.174
Paraguai	437	929	1.366
Argentina	25	1.236	1.261
Uruguai	320	749	1.069
Total	**10.035**	**7.602**	**17.637**

Tabela 1 – Extensão da fronteira do Brasil com países limítrofes
Fonte: DANTAS, 2014, p. 27

conformação fronteiriça (conforme **Tabela 1**), observamos a imensidão e a variedade de cenários por onde transitam os ilícitos transnacionais (seja pela fronteira seca, pelos rios ou pelo ar). Isso pode ser constatado, particularmente, nas fronteiras com quatro importantes exportadores mundiais de drogas, como Peru, Bolívia, Paraguai e Colômbia.

Essa realidade, complexa e variada, fortalece a construção de um cenário no qual todos os estados do Brasil que fazem fronteira com outros países apresentem estatísticas de ilícitos (conforme **Tabela 2**) que impactam boa parte do país. Isso é favorecido pelo largo emprego dos meios tecnológicos na consecução dos ilícitos.

Ainda no que se refere à tecnologia, Guilherme Cunha Werner (2009, p. 44) reforça a sua importância para a consumação criminosa ao afirmar que as "alianças celebradas entre os diversos grupos criminosos se inserem no processo de globalização financeira". Acrescenta ainda que "utilizam o incremento de tecnologias da informação e comunicação, articulam-se e se projetam no âmbito transnacional".

Um bom exemplo disso é o uso do acesso de informações confidenciais, a manipulação de algumas informações, a implantação de vírus em sistemas e a destruição de arquivos.

Eventos criminosos	Grau de prioridade de implantação do projeto											Estados presentes
	Alta							Média				
	AP	RS	MS	SC	AM	RR	PR	AC	RO	MT	PA	
Tráfico de drogas	x	x	x	x	x	x	x	x	x	x	x	11
Roubo de cargas, veículos	x	x	x	x	x	x	x		x	x	x	10
Tráfico de armas e munição	x	x	x	x	x		x	x	x	x		9
Crimes ambientais	x		x	x	x	x		x	x	x	x	9
Refúgio de criminosos		x	x	x	x	x	x	x	x	x		9
Contrabando e descaminho	x	x	x	x	x	x	x		x	x		9
Exploração sexual infanto-juvenil	x	x		x		x	x	x	x			7
Tráfico de pessoas	x	x				x		x				4
Rota de veículos roubados			x		x		x			x		4
Abigeato (roubo de gado)		x	x	x			x					4
Pistolagem					x	x		x				3
Evasão de divisas	x	x										2
Turismo sexual	x											1
Eventos criminosos presentes	9	9	8	8	8	8	8	7	7	7	3	

Tabela 2 – Eventos criminosos por estado situado na faixa de fronteira
Fonte: Eventos Criminosos Relacionados à Zona de Fronteira (Brasil, 2008), Secretaria de Segurança Pública de Santa Catarina[4]

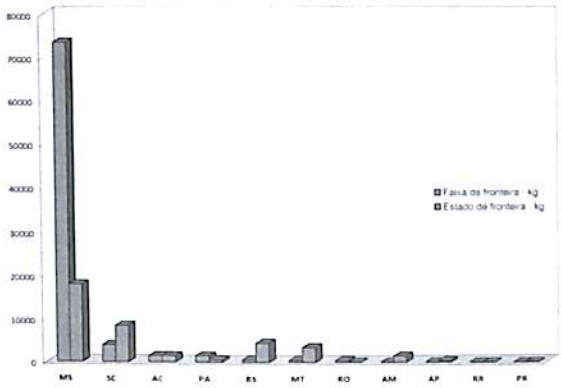

Gráfico 1 – Apreensões de Drogas – Estados da Fronteira 2012
Fonte: Brasil, Ministério da Defesa, 2013 [5]

Assim, ao considerar o nível de impacto dos ilícitos transnacionais, pode-se constatar, ainda na Tabela 2, que o tráfico de drogas se constitui no principal ilícito nos Estados da faixa de fronteira terrestre brasileira.

Além disso, pode-se depreender, pelo **Gráfico 1**, que esse ilícito foi o mais destacado no Estado do Mato Grosso do Sul, que atualmente é o palco da implantação do SISFRON em sua fase piloto.

Outro aspecto que se soma ao potencial das organizações criminosas na consumação dos ilícitos transnacionais está em sua possível ligação com grupos terroristas, particularmente na região da Tríplice Fronteira. Nesse sentido,

> os crimes correlatos ao terrorismo, que, segundo autoridades internacionais, são a principal fonte de levantamento de recursos financeiros, fazem da Tríplice fronteira Sul — Brasil, Argentina e Paraguai — uma região apontada por organizações internacionais como uma área onde pode haver a existência de células terroristas e levantamento de recursos financeiros para financiar ataques terroristas, através da venda de drogas e contrabando de mercadorias. (COSTA, 2013, p.27)

Além disso,

> não se sabe exatamente qual é o papel da tríplice fronteira na atração de grupos terroristas, mas a comunidade árabe e muçulmana da Cidade do Leste tem coletado fundos, através da lavagem de dinheiro, tráfico de armas e drogas, contrabando e pirataria. Supostamente, uma parte destes fundos é enviada para o Hezbollah e o Hamas em apoio aos atos terroristas contra Israel. (ABBOT, 2005, p.22)

Isso reforça, no contexto da Guerra de Informação, a importância do SISFRON como o vetor capaz de prover o indispensável ambiente de superioridade de informação nas fronteiras terrestres do país.

Pelo exposto, considerando a capilaridade fronteiriça e a diversidade de atores com potencial de ameaça à segurança pública, é lícito afirmar a necessidade de envolver outras agências apoiando o Exército Brasileiro na condução do SISFRON. Isso se iniciaria pela Marinha do Brasil e pela Força Aérea Brasileira, no que tange aos Requisitos Operacionais Básicos (ROB) e às aquisições de material, visando ao futuro dos equipamentos que comporão esse Sistema de Vigilância de Fronteiras.

Até este ponto, observam-se duas premissas importantes para o presente trabalho. A primeira refere-se ao emprego dos meios de Tecnologia da Informação por qualquer organização, e a segunda, ao uso da informação como matéria-prima importante para o sucesso ou insucesso de qualquer atividade, seja ela legal ou não. Isso ocorre na Era da Informação, na Guerra de Informação, no SISFRON e

nas ações das organizações criminosas na consumação dos ilícitos transnacionais.

Isso posto, a partir do próximo tópico, serão aprofundados os subsistemas que integram o SISFRON e a Guerra de Informação, particularmente no que diz respeito à superioridade de informação, considerando as supracitadas premissas (que estão em crescente importância na atual conjuntura).

Os subsistemas do SISFRON

O SISFRON,

> por sua complexidade tecnológica e amplitude de emprego, compreende um conjunto amplo e integrado de tecnologias, estruturas organizacionais, processos e pessoas, constituindo um "sistema de sistemas". (BRASIL, 2014b, p.75)

Essas características demandam altos custos financeiros no que tange à implantação do SISFRON, um sistema de informação em rede,[6] baseado em grande quantidade e variedade de equipamentos, além da contratação de empresas com *know-how* para integrá-los (conforme a **Figura 1**).

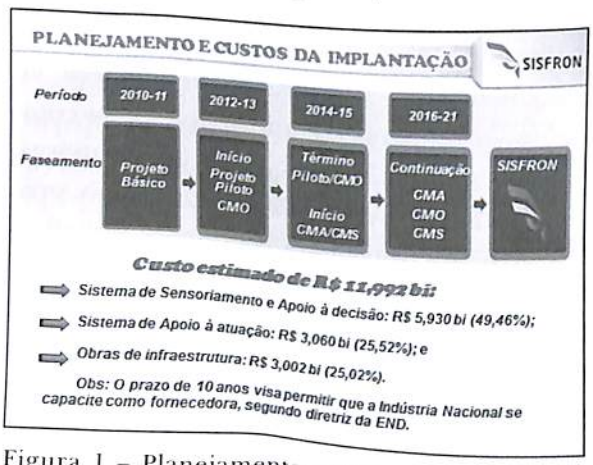

Figura 1 – Planejamento e custos de implantação do SISFRON

Fonte: FRANÇA, 2014, p.26

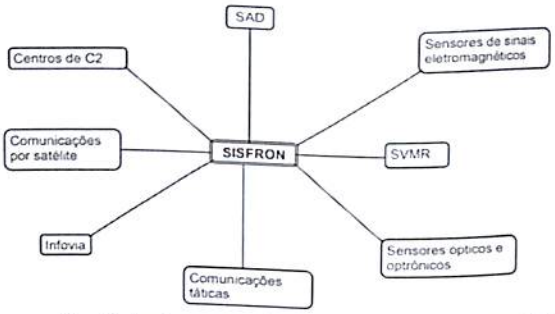

Figura 2 – Subsistemas do SISFRON desenvolvidos no CCOMGEX

Fonte: BRASIL, 2014b, p.75

Assim,

> para o projeto piloto (1ª fase do SISFRON, que vem sendo implantada na 4ª Brigada de Cavalaria Mecanizada), no âmbito do pilar do Sensoriamento,[7] foram estabelecidos, de forma específica, os seguintes subsistemas: Sensores ópticos e optrônicos; Sensores de vigilância, monitoramento e reconhecimento (SVMR); Sensores de sinais eletromagnéticos (Guerra Eletrônica); Comunicações táticas; Comunicações por satélite; Comunicações Estratégicas e Centros de comando e controle (C2). (BRASIL, 2014b, p. 75)

Para cumprir sua finalidade, cada um dos referidos subsistemas (conforme a **Figura 2**) está dotado de capacidades específicas, que contribuirão para, trabalhando de forma integrada, fornecer à sociedade a vigilância necessária das fronteiras terrestres do país.

Dessa forma, importa apresentar, ainda que de forma muito resumida, quais as principais capacidades que cada subsistema possui atualmente. Pode-se destacar o conteúdo apresentado na **Tabela 3**.

Apesar da importância de todos os subsistemas do SISFRON, para o presente trabalho, serão detalhados, por sua pertinência com o assunto, os subsistemas de Comunicações Tá-

Subsistema	Capacidades Atuais
Optrônicos	• ser empregado individualmente nas missões de vigilância, potencializando a eficácia e eficiência da tropa, entretanto sem uma integração direta do sensor em rede com os escalões superiores • integrar-se, por meio das comunicações táticas, ao Subsistema de Apoio à Decisão, possibilitando o aumento da consciência situacional dos escalões superiores e diminuindo o tempo do ciclo de decisão em comando e controle
Vigilância, monitoramento e reconhecimento (SVMR)	• executar a vigilância de áreas extensas pela detecção e reconhecimento de entidades móveis e sua identificação pelas versões dotadas de câmeras • prover a consciência situacional a nivel local e ao nivel de regimento • integrar-se com os recursos de comunicações da Infovia e das Comunicações Táticas, contribuindo para incrementar o processo de consciência situacional
Sensores de sinais eletromagnéticos	• operar relativamente desacoplado dos demais subsistemas de sensores • prover o SAD e os Centros de Comando e Controle com informações levantadas por seus receptores
Apoio à decisão (SAD)	• fornecer o suporte ao Exército Brasileiro para a execução da vigilância da faixa ao longo das fronteiras terrestres brasileiras, especificamente na região das OM (organizações militares) do Comando Militar do Oeste (CMO) que foram contempladas na Fase Piloto do Projeto SISFRON
Comunicações táticas	• possibilitar a comunicação entre e intra organizações militares (OM), em operações e manobras militares, por exemplo, quando uma OM estiver desdobrada no teatro de operações • atuar como elo entre o SAD e diversos subsistemas de sensores inerentes ao SISFRON, permitindo que o SISFRON opere como um sistema integrado • atuar como um sensor, na medida em que todos os rádios possuem um receptor GPS embutido e a posição de seu portador, seja um elemento ou uma viatura
Comunicações estratégicas (Infovia)	• suportar as comunicações em rede entre as OM envolvidas no SISFRON, possibilitando a experimentação e consolidação do conceito de operações centradas em rede no âmbito do SISFRON, provendo a comunicação entre as instâncias do Subsistema de Apoio a Decisão (SAD) instaladas nos regimentos, 4ª Brigada e CMO
Comunicações satelitais	• prover comunicações digitais em regiões sem infraestrutura de comunicações fixas • garantir comunicações entre brigada e comando central em operações de deslocamento em regiões sem infraestrutura, suportando o Subsistema de Apoio a Decisao (SAD) e a cadeia de comando e controle, em consonância com a Estratégia Nacional de Defesa
Infraestrutura	• permitir a operação contínua dos sensores e subsistemas de todo o SISFRON
Centros de comando e controle	• possibilitar a integração das unidades envolvidas no projeto piloto, provendo recursos de transmissão de dados, voz e imagem para todos os nós do sistema na área do Estado do Mato Grosso do Sul • possibilitar a utilização de recursos de telefonia e sistema de monitoramento das unidades remotas, de forma centralizada

Tabela 3 – Capacidades resumidas dos Subsistemas do SISFRON
Fonte: MOTA, 2015

ticas, Estratégicas e Satelitais, além do de Centros de Comando e Controle.

Eles serão abordados nos tópicos a seguir, quando for estabelecido o relacionamento do SISFRON com a superioridade de informação.

Superioridade de informação

Está cada vez mais evidenciada a importância de deter a capacidade de transmitir informações de forma oportuna e efetiva, desde o nível tático até o político. A História descortina episódios importantes, nos quais a referida capacidade ficou patente. Um bom exemplo que ilustra esse aspecto ocorreu durante a Guerra das Malvinas (1982), quando os Estados Unidos da América se mostraram um importante aliado da Inglaterra, inclusive transmitindo-lhe informações obtidas por seus satélites, ainda que sem intervir militarmente.

Esse apoio contribuiu para garantir a vitória britânica, uma vez que

> os argentinos, sem informações providas por satélites, não poderiam realizar um contra-ataque eficaz contra a Grã-Bretanha. A sua maior possibilidade de obter na União Soviética um aliado importante foi frustrada pelas negociações secretas desta com os norte-americanos, o que impossibilitou o uso do arsenal militar soviético pelas forças argentinas. (CARVALHO, 2014)

Assim, dado o exemplo das Malvinas, pode-se constatar a importância da superioridade de informações da Inglaterra, provida por meios tecnológicos, em detrimento da Argentina, para o resultado do conflito.

O detentor de superioridade de informação encontra-se em melhores condições de vencer o seu opositor, uma vez que tal superioridade se constitui em uma importante parte da Guerra de Informação. Isso está evidenciado na própria definição de Guerra de Informação adotada pelo Ministério da Defesa:

> Conjunto de ações destinadas a obter a **superioridade das informações**, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos. (BRASIL, 2007, p.124)

Complementado o disposto acima, está evidenciado que a superioridade de informação

> é traduzida como uma vantagem operativa advinda da habilidade de reunir, processar, difundir, explorar e preservar um fluxo ininterrupto de informações aos comandantes em todos os escalões, ao mesmo tempo em que se busca tirar vantagem das informações do oponente e/ou negar-lhe essas habilidades. É possuir mais e melhores informações do que o adversário sobre o ambiente operacional. Permite o domínio da dimensão informacional (espectros eletromagnético, cibernético e outros) por determinado tempo e lugar. (BRASIL, 2014a, p. 3-1)

Ao verificarmos o supracitado conceito, pode-se afirmar que a superioridade de informação é condição indispensável para adquirir e manter qualquer vantagem operativa.

Não basta deter tecnologias adequadas ao êxito em qualquer ambiente operacional. É necessário, também, possuir as capaci-

dades técnicas e efetivamente empregar os meios para isso, uma vez que, superioridade de informação é, em outra definição,

> a capacidade de adquirir, processar e disseminar os dados indispensáveis para a obtenção do conhecimento sobre a situação no tempo devido. Ela é fundamental para a conquista e manutenção da iniciativa no emprego das demais capacidades operacionais. (BRASIL, 2010, p. 46)

Além das referidas capacidades técnicas, também é necessário deter a condição de explorar de forma eficiente a superioridade de informação adquirida (conforme a **Figura 3**). Isso deve ser feito pela conjugação de informações relevantes, precisas e oportunas, pela "integração dos processos para a construção do conhecimento, o que promoverá a compreensão precisa e atualizada do ambiente operacional" (BRASIL, 2014a).

Ainda explorando o exposto na **Figura 3**, verifica-se que é necessário que o "competidor dominante" em um ambiente de informações relevantes, precisas e oportunas envolva o "competidor dominado", de modo que este fique circunscrito ao "dominante". Isso gerará a devida "*Superior Information Position*".[8]

Para o caso em análise, de acordo com a **Figura 3**, espera-se que o SISFRON permita ao Estado brasileiro desempenhar o papel de "competidor dominante", configurando a situação de superioridade de informação, e as organizações criminosas estejam na situação de "competidoras dominadas".

Somado ao exposto, outro aspecto relevante diz respeito ao processo de tomada de decisão. A superioridade de informação somente será evidenciada por decisões consistentes e oportunas.

Segundo Marcelo Paiva Fontenele (2008, p. 1),

> atualmente, vivenciamos uma genuína guerra de Informação, onde prevalece a assimetria e cujas batalhas são vencidas por aqueles que detêm a superioridade de informação em momentos decisivos. Entenda-se a superioridade de informação como: ter a capacidade de reagir de forma consistente a uma situação e **tomar decisões corretas mais rapidamente que o oponente com o objetivo de obter vantagem**. (grifo nosso)

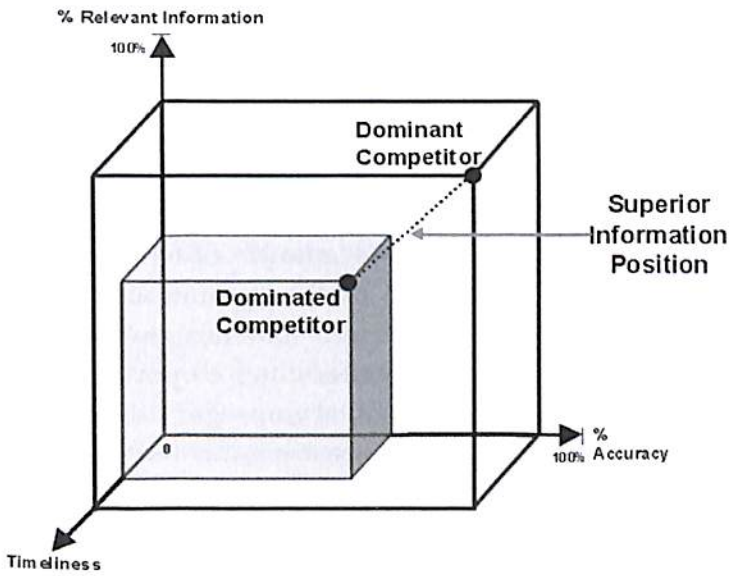

Figura 3 – Modelo conceitual de superioridade de informação
Fonte: Alberts, Garstka, & Stein, 1999, p. 34

Prosseguindo na ideia de superioridade de informação associada

ao processo decisório, pode-se afirmar que a primeira somente será efetivada se o segundo for coerente com a avaliação do impacto das informações recebidas. Esse pensamento não começou há pouco tempo. Como exemplo, temos o "Dilema Coventry" ocorrido com a Grã-Bretanha, durante a Segunda Guerra Mundial (1939-1945). A seguir, em linhas gerais, como ocorreu o fato:

> Durante a Segunda Guerra Mundial, os britânicos, usando a máquina Enigma, tiveram um acesso quase perfeito aos códigos operacionais alemães. Eles souberam, portanto, ao mesmo tempo que o comandante de campo alemão, que a Luftwaffe havia recebido ordem para destruir a cidade de Coventry, no interior da Inglaterra. Churchill enfrentou um dilema clássico. Se ele ordenasse a evacuação da cidade e os alemães descobrissem, eles saberiam que o código havia sido descoberto. Os alemães mudariam o código e os ingleses perderiam uma ferramenta de valor inestimável, talvez custando milhares de vida ou mesmo a guerra. Por outro lado, qual seria a finalidade da inteligência, se Churchill permitisse que uma cidade inglesa fosse devastada? Ele, apropriadamente, permitiu que a cidade fosse destruída sem evacuação, justificando que, se não o fizesse, muito mais vidas seriam perdidas no futuro. (FRIEDMAN; FRIEDMAN, 2009, p. 363)

Assim, ao refletirmos sobre a superioridade da informação associada ao armazenamento de informações em um cenário de grande volatilidade e quantidade de dados circulando nos meios de TI, é lícito destacar a importância do emprego de sistemas com a capacidade de contribuir para que a superioridade de informação seja assegurada.

Segundo George e Meredith Friedman (2009, p. 364),

> Imagens, o Programa norte-americano de apoio à Defesa, inteligência de sinais, inteligência eletrônica e quaisquer outros tipos de plataformas de reconhecimento, no espaço ou em outros lugares, **coletam vastas quantidades de dados; todos inúteis, em sua forma não processada. A torrente sem fim de material digital é incompreensível, a menos que algum sistema transforme os dados em informações, analise as informações e as distribuam às pessoas que tomem decisões ou estejam conduzindo guerras**. (grifo nosso)

Essa assertiva ressalta a importância do armazenamento eficiente e da análise, baseada em sistemas confiáveis, que irão contribuir para garantir a superioridade de informações.

Assim, observando o exposto até este momento, emergem novas premissas que sustentam a ideia chave do presente artigo. A primeira: a superioridade de informação é condição indispensável para adquirir e manter qualquer vantagem operativa; a segunda: é necessário possuir as capacidades técnicas e efetivamente empregar os meios tecnológicos para garantir a superioridade de informação.

Prosseguindo nessa linha de pensamento, a terceira premissa: a superioridade de informação somente será evidenciada por decisões consistentes e oportunas; e a quarta: é fundamental empregar sistemas com a capacidade de armazenamento de dados para que a supracitada superioridade seja assegurada.

Ao trazermos para a conjuntura brasileira, o SISFRON poderá ser o sistema com condições de prover, no contexto da Guerra de Informação, a necessária superioridade

de informação no atual cenário de grande tráfego de ilícitos transnacionais. Isso será tratado no tópico a seguir.

Os subsistemas do SISFRON e seu relacionamento com a superioridade de informação[9]

O SISFRON, como um "sistema de sistemas", funciona à semelhança de um organismo que tem a informação como o principal insumo que sustentará o processo de tomada de decisão.

Como já foi abordado, os subsistemas do SISFRON trabalham de forma integrada, cada um exercendo funções específicas. No que diz respeito à Guerra de Informação e, particularmente à superioridade de informação, serão detalhados alguns dos seus subsistemas.

O primeiro deles se refere ao Subsistema de Comunicações Táticas. Esse subsistema dispõe de meios de comunicações (fixos, portáteis e veiculares) que operam nas faixas de UHF, VHF e HF. De acordo com a concepção do SISFRON, esse subsistema irá reequipar as tropas de fronteira no que tange aos meios de comando e controle tático e será um dos principais eixos estruturantes para o trânsito das comunicações das tropas (MOTA, 2015, p. 24).

Dentro do assunto em tela, basicamente, a informação produzida nos menores escalões, como os Grupos de Combate e Pelotões, será transmitida (seja voz ou dados) até o escalão Brigada, por intermédio do Subsistema de Comunicações Táticas. Somado a isso, ele irá prover a integração dos demais subsistemas (MOTA, 2015, p. 35).

Ademais, em virtude de os equipamentos rádio estarem baseados em rede, tem sido necessária a implementação de um plano de treinamento[10] com o objetivo de capacitar tecnicamente os operadores dos rádios, no que concerne à instalação e operação de redes de computadores. Isso tem agregado novas competências aos militares da fronteira terrestre brasileira.

Esse subsistema está revestido de grande importância para garantir a superioridade das informações, uma vez que dispõe dos meios tecnológicos para o trânsito da informação no nível tático e está construindo, por ocasião do seu processo de implantação, uma massa crítica com o conhecimento técnico para operar com efetividade os referidos meios.

O segundo dos subsistemas é o de Comunicações Estratégicas. Esse subsistema vem extrapolando a expressão militar. Atualmente as expressões política e psicossocial vêm sendo agregadas a ele por sua capacidade de apoiar iniciativas nessas duas expressões.

Também em fase de implantação, esse subsistema disporá de um conjunto de torres (Infovia) com alturas variando entre 60 e 100m e com visada direta,[11] onde estarão instaladas antenas de micro-ondas que transmitirão os dados levantados pelos sensores postados na fronteira até os Centros de Comando e Controle de Dourados e Campo Grande, MS.

A sua capacidade de transmissão associada a outros subsistemas, como o de Centros de Comando e Controle e o de Sensores de Sinais Eletromagnéticos, contribuirá para prover o SISFRON de dados que certamente contribuirão para garantir a superioridade de informação sobre as organizações criminosas que estiverem atuando nas fronteiras terrestres do país.

O terceiro subsistema a ser detalhado é o de Comunicações Satelitais. Nele, serão estabelecidas, por intermédio de estações —

à semelhança da apresentada na **Figura 4** —, as comunicações do SISFRON em regiões onde não há cobertura de comunicações por outros meios. Esse subsistema impõe o lançamento de um satélite de produção nacional de curto a médio prazo, o que reforçará a dualidade do SISFRON (MOTA, 2015, p. 26).

Dessa forma, por ampliar a capacidade de tráfego do sistema, operando como elemento redundante do SISFRON, esse subsistema contribuirá para a aquisição e manutenção da superioridade de informação. Além disso, a capacitação[12] fornecida para operação dos terminais satelitais reforçará a referida superioridade pela ampliação dos efetivos com condições técnicas de operar o supracitado subsistema ou de outros congêneres que venham a surgir futuramente.

Ainda no Subsistema de Comunicações Satelitais, a empresa Visiona[14] está incumbida atualmente do supracitado lançamento do satélite militar brasileiro. Se considerarmos a inexistência de um satélite de defesa genuinamente nacional no Brasil e o envolvimento do SISFRON com essa empreitada, já seria um fator para considerá-lo como plenamente inserido na Guerra de Informação. Além disso, para fins práticos, o subsistema de comunicações satelitais contribuirá para o incremento de novas capacitações no emprego de meios que trabalhem na Banda X.[15]

O subsistema de Comunicações Satelitais será muito importante na busca pela superioridade de informações, em um contexto de ilícitos transnacionais, onde as organizações criminosas também empregam a comunicação satelital, por suas inúmeras facilidades, principalmente no que tange à segurança das comunicações.

Por fim, o quarto subsistema e não menos importante é o de Centros de Comando e Controle, tanto fixos quanto móveis (**Figura 5**). Esse subsistema está diretamente relacionado ao processo de tomada de decisão, uma das premissas estabelecidas para este artigo no que tange à superioridade de informação.

Figura 4 – Estações de Comunicação Satelital[13]
Fonte: Google®

Para tanto, o subsistema de Centros de Comando e Controle está estruturado em plataformas que fornecerão a informação coletada nos sensores em interfaces que auxiliarão o processo decisório, de modo que este ocorra de forma rápida e eficaz (MOTA, 2015, p. 27-28). Isso contribuirá para a construção de um cenário de superioridade de informação, no qual os envolvidos nos ilícitos transnacionais serão ainda mais cerceados em suas ações.

Pelo exposto até aqui, é lícito afirmar que o SISFRON é um sistema plenamente in-

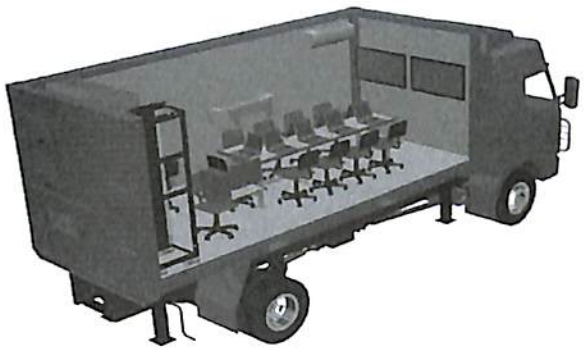

Figura 5 – Centro de comando e controle móvel
Fonte: MOTA, 2015, p. 27

serido na Guerra de Informação com condições de prover a necessária superioridade das Forças Armadas no combate aos ilícitos transnacionais.

Considerações finais

Dado o exposto neste trabalho, podemos afirmar que toda a análise apontou para o fato de a Guerra de Informação, particularmente na fronteira terrestre brasileira, se constituir em uma realidade com dois contendores importantes. De um lado, o Estado brasileiro, tendo o SISFRON, como uma ferramenta de vigilância das fronteiras terrestres; de outro, as organizações criminosas, relacionadas aos chamados ilícitos transnacionais. Ambos buscam garantir a superioridade de informação na consecução de seus objetivos.

Em síntese, e dentro desse escopo, podem ser apontados alguns aspectos importantes, que contribuirão para que o SISFRON siga sendo um vetor fundamental da Guerra de Informação no país. Tais aspectos merecem ser alvo de posteriores análises a fim de que sejam apontados futuros caminhos para o SISFRON.

O primeiro aspecto está relacionado à complexidade e envergadura tecnológica, além dos meios de TI associados aos seus subsistemas. Ao consideramos este aspecto associado à capilaridade e diversidade das fronteiras do país, surge a demanda de envolver, com profundidade, a Marinha do Brasil e a Força Aérea Brasileira na definição de requisitos e no acompanhamento das aquisições de equipamentos como embarcações e sistemas aéreos remotamente pilotados (SARP) a serem incluídos no SISFRON. O envolvimento das Forças irmãs com o Exército Brasileiro agregará maiores capacidades ao Sistema na Guerra de Informação contra as organizações criminosas.

O segundo aspecto está relacionado aos recursos financeiros envolvidos no SISFRON. Isso é muito importante, tendo em vista os altos custos envolvidos em um Sistema com grande integração de sensores, transmissão e armazenamento de dados. Nesse sentido, são indispensáveis todas as medidas para evitar a descontinuidade tecnológica do SISFRON em um cenário de avanço crescente dos ilícitos transnacionais alimentados pelas organizações criminosas. Considerando essa demanda, a superioridade de informação do SISFRON também depende da capacidade orçamentária do Estado, que deve considerar esse Sistema uma prioridade para o fortalecimento da estrutura de segurança pública do país.

O terceiro e último aspecto diz respeito à vigilância a ser provida pelo SISFRON na região da Tríplice Fronteira. É notório o estreito relacionamento entre o narcotráfi-

co e o terrorismo. Isso nos permite afirmar que será fundamental dirigir esforços para a vigilância das fronteiras comuns entre Brasil, Paraguai e Argentina, de modo a prover para o Estado as indispensáveis informações sobre prováveis movimentações de grupos terroristas naquela região.

Dado o exposto, pode-se concluir que o SISFRON é um importante vetor da Guerra de Informação na fronteira terrestre do Brasil. Isso se deve às capacidades agregadas em seus subsistemas, que lhe conferem alto valor tecnológico e a necessária superioridade de informação em face das organizações criminosas, principais responsáveis pelo trânsito dos chamados ilícitos transnacionais. Dessa forma, a manutenção e o aperfeiçoamento desse Sistema serão de importância vital para o Estado na garantia da segurança das fronteiras e da paz social, em um contexto da sempre presente Guerra de Informação.

Referências

ABBOT, Philip K. **A ameaça terrorista na Área da Tríplice Fronteira: Mito ou Realidade?**. Revista Military Review, 2005. Disponível em: <http://www.observatorioseguranca.org/pdf/abbot.pdf>. Acesso em: 13 Ago 16.

ALBERTS, D.. GARSTKA, J. STEIN, F. **Network Centric Warfare: Developing and Leveraging Information Superiority**. Washington DC: CCRP, 1999. Disponível em: <http://www.au.af.mil/au/awc/awcgate/ccrp/ncw.pdf>. Acesso em: 15 Ago 16.

BRASIL. Ministério da Defesa. **MD35-G-01 - Glossário das Forças Armadas**. 4ª Ed. [Brasília]: Ministério da Defesa, 2007.

_____. Estado-Maior do Exército. **O Processo de Transformação do Exército, 3ª Edição**. Brasília, 2010a.

_____. Secretaria-Geral do Exército. **Boletim do Exército nº 52/2010**. Brasília, 2010b.

_____. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, 2012. Disponível em: < http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf> Acesso em: 11 Ago 16.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2013. Disponível em:<http:// www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 05 Ago 16.

_____. Estado-Maior do Exército. **EB 20-MC-10.213, Operações de Informação**. 1ª Ed. Brasília, 2014a.

_____. Estado-Maior do Exército. **Doutrina Militar Terrestre em Revista**. 4ª Ed. Brasília, DF, 2014b.

CARVALHO, Rogério do Nascimento. **ILHAS MALVINAS: uma reflexão sobre a soberania argentina**. Disponível em:<http://www.esg.br/images/Monografias/2014/CARVALHO.pdf>. Acesso em: 18 Ago 16.

CASTELLS, Manuel. **A Sociedade em Rede. A Era da Informação: Economia, Sociedade e Cultura**. Vol. I, 4ª ed., Fundação Calouste Gulbenkian, 2011.

COSTA, Sérgio Miguel Correia. **A atividade de Inteligência na prevenção da ameaça terrorista no Brasil. Universidade Federal de Santa Catarina**. 2013. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/103858/Monografia%20do%20Sergio%20Miguel%20Correia%20Costa.pdf?sequence=1>. Acesso em: 16 Ago 16.

DANTAS, Leonardo Arêas. **O agravamento da problemática da Segurança Pública brasileira na faixa de fronteira e os seus reflexos para o preparo e emprego da Força Terrestre.** Rio de Janeiro. Escola de Comando e Estado-Maior do Exército. 2014.

FONTENELE, Marcelo Paiva. **Proposta de Taxionomia da Guerra de Informação e das Operações de Informação**. Centro de Instrução de Guerra Eletrônica, Brasília, DF, 2008. Disponível em: <http://www.ccomgex.eb.mil.br/cige/sent_colina/9_edicao_abr_10/index/Art_Maj_Fontenele.pdf>Acesso em: 02 Ago 16.

FRANÇA, Eriwelton Ferreira de. **O Sistema Integrado de Monitoramento de Fronteiras (SISFRON) no fortalecimento da soberania nacional**. Rio de Janeiro. Escola de Comando e Estado-Maior do Exército. 2014. Disponível em: <http://200.20.16.3/guardiao/controle.php?modulo=cadastro&tela=legislacao&acao=detalhar&menu=0&rodape=0&Id=11949&readonly=true>. Acesso em: 18 Ago 16.

FRIEDMAN, George; FRIEDMAN, Meredith. **Poder mundial: a tecnologia e o domínio dos Estados Unidos no Século XXI**. Tradução de Geraldo Alves Portilho Junior. Biblioteca do Exército. Rio de Janeiro, 2009.

HAENI, Reto E. **Information Warfare na Introduction**. The George Washington University, Cyberspace Policy Institute, 1997. Disponível em: <http://www.trinity.edu/rjensen/infowar.pdf> Acesso em: 18 Ago 16.

JOHNSON, Robert A. **Como prever a Guerra do Futuro**. Revista Military Review, Julho-Agosto, 2015. Disponível em: <https://www.joomag.com/magazine/military-review-edi%C3%A7%C3%A3o-brasileira-julho-agosto-2015/0483313001434382791>. Acesso em: 14 Ago 16.

MOTA, Dardano do Nascimento. **Uma Concepção e Estratégias de Aplicação do Método Desdobramento da Função Qualidade (QFD) para as Comunicações Táticas do SISFRON**. Rio de Janeiro. Escola de Comando e Estado-Maior do Exército. 2015.

NUNES, P. Viegas. **O Impacto da Aplicação do Conceito de Network Centric Warfare nas Forças Armadas Portuguesas**. "Subsídios para o levantamento de uma Capacidade Militar Centrada em Rede". Academia Militar, Ministério da Defesa Nacional, 2005.

RODER, Ariane. **A Agenda Externa Brasileira face aos ilícitos transnacionais: o contrabando na fronteira entre Brasil e Paraguai. Universidade de São Paulo**. 2007. Disponível em: <http://www.plataformademocratica.org/Publicacoes/21205_Cached.pdf>. Acesso em: 15 Ago 16.

TOFFLER, Alvin (2003). **A Terceira Onda**. A morte do industrialismo e o nascimento de uma nova civilização. São Paulo. Ed Record, 1980.

WERNER, Guilherme Cunha. **O crime organizado transnacional e as redes criminosas: presença e influência nas relações internacionais contemporâneas**. 2009. Disponível em: <www.teses.usp.br/teses/disponiveis/8/8131/.../GUILHERME_CUNHA_WERNER.pdf> Acesso em: 11 Set 16.

N. da R.: A adequação do texto e das referências às prescrições da Associação Brasileira de Normas Técnicas (ABNT) é de exclusiva responsabilidade dos articulistas.

[1] Consciência Situacional – Garante a decisão adequada e oportuna em qualquer situação de emprego, permitindo que os comandantes possam se antecipar aos oponentes e decidir pelo emprego de meios na medida certa, no momento e local decisivos, proporcionalmente à ameaça (BRASIL, 2014, p. 3-1).

[2] "Medidas tomadas para alcançar a superioridade de informação, afetando informações do adversário, processos baseados em informação, sistemas de informação e redes baseadas em computadores, enquanto protege a própria informação, informações baseadas em processos, sistemas de informação e redes baseadas em computadores" (tradução nossa).

[3] Mais informações sobre a obra de Manuel Castells no livro *A sociedade em rede* (*A era da informação: economia, sociedade e cultura* vol.1).

[4] Disponível em: <http://www.ssp.sc.gov.br/index.php?option=com_docman&task=doc_Download&gid=26&Itemid=174> . Acesso em: 15 Ago 16

[5] Disponível em: http://www.defesa.gov.br/projetosweb/cedn/arquivos/palestras-junho-2013/seguranca-das-areas-de-fronteira-brasileia-mj.pdf

[6] Informação em rede: é a integração entre sensores, armas e postos de comando e entre esses e sistemas similares — civis, militares, nacionais ou multinacionais — em todos os níveis de comando, do estratégico ao tático, apoiada em uma Infraestrutura de Informação e Comunicações comum. (BRASIL, 2014, p. 5-12).

[7] Um dos pilares do SISFRON, já abordado na introdução deste artigo.

[8] Posição de superioridade de informação (tradução nossa).

[9] Todas as informações específicas dos subsistemas do SISFRON apresentadas neste tópico foram retiradas do Trabalho de Conclusão de Curso *Uma Concepção e Estratégias de Aplicação do Método Desdobramento da Função Qualidade (QFD) para as Comunicações Táticas do SISFRON*, de minha autoria como aluno do Curso de Comando e Estado-Maior da ECEME no biênio 2015/2016.

[10] O Plano de Treinamento consiste na capacitação dos usuários de cada Subsistema do SISFRON, dada a complexidade tecnológica agregada em cada um deles. O autor, durante os anos de 2012 a 2014, participou da concepção e implantação do SISFRON na 4ª Brigada de Cavalaria Mecanizada, quando servia no Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEX), motivo pelo qual pôde acompanhar e fiscalizar o andamento dos treinamentos conduzidos pela Empresa Integradora do SISFRON (SAVIS TECNOLOGIA E DEFESA), particularmente no que se refere ao Subsistema de Comunicações Táticas.

[11] Em 2013, foram realizados reconhecimentos por este autor, juntamente com integrantes da SAVIS, na região da 4ª Brigada de Cavalaria Mecanizada para encontrar os locais mais apropriados que garantissem a inexistência de obstáculos entre as torres.

[12] Também incluída no Plano de Treinamento do SISFRON (à semelhança do que já foi abordado para o Subsistema de Comunicações Táticas).

[13] Disponível em: https://www.google.com.br/search?q=esta%C3%A7%C3%A3o+de+comunica%C3%A7%C3%A3o+satelital&biw=1138&bih=548&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj5-bO6kZDPAhVDUZAKHTVqBUYQ_AUIBygC&dpr=1.2#imgrc=nBFhRbMv9bO6yM%3A

[14] Empresa Resultado da associação entre os grupos Embraer e Telebrás, a Visiona atua como integradora de sistemas espaciais completos. Contratada para ser a *prime contractor* do sistema SGDC (Satélite Geoestacionário de Defesa e Comunicações), a Visiona está trabalhando para o lançamento desse sistema.

[15] Banda de emprego exclusivamente militar.