A Dependabilidade em um Sistema de Telecomunicações em Missão Crítica: A Percepção do Usuário como Instrumento de Poder Informacional para Segurança Pública

Luciano Castilho Assumpção
Polícia Federal – Curitiba/PR

RESUMO

Na sociedade da informação, o uso adequado de equipamentos de telecomunicações em missão crítica nas operações de segurança pública visa atender a requisitos de domínio da informação e de segurança de operadores. Desta forma, se exerce o poder informacional evidenciado nas ações policiais na medida em que tais requisitos são observados. A dependabilidade descreve a relação destes requisitos com a percepção dos usuários por meio de níveis aceitáveis de falhas em situações como quando os requisitos de disponibilidade dependem da infraestrutura da organização e de suas limitações. O objetivo desta pesquisa é descrever propostas de soluções a partir das experiências de uso baseada na dependabilidade. Trata-se de uma pesquisa exploratória e descritiva utilizando-se de estudo de casos, análise e observação direta de troca de mensagens em operações policiais e elaborando propostas de soluções a partir das experiências de uso baseada nos padrões encontrados. Os resultados propõe formas alternativas de uso dos equipamentos mesmo na presença de falhas de cobertura, assegurando o requisito da disponibilidade. Assim, pode-se proporcionar uma melhor percepção do usuário com relação ao sistema, propondo alternativas ao exercício do poder informacional em atividades ostensivas e considerando não apenas as questões tecnológicas, mas também as humanas e as organizacionais.

Palavras-Chave: Dependabilidade. Missão crítica. Telecomunicações. Segurança pública. Poder informacional.

1. Introdução

O bom uso dos recursos de telecomunicações nas atividades de segurança pública podem representar para o Estado o controle da informação e, assim, na visão de Braman (2006), reforçar o papel do Es-

Recebido em 20 de março de 2020.
Aceito em 16 de setembro de 2020.
Brasília, v. 12, n. 4 , p. 267-294 , jan/abr 2021. ISSN 2178-0013
ISSN Eletrônico 2318-6917

tado na manutenção do poder informacional. O papel das telecomunicações em uma operação policial é tão importante e decisivo quanto o armamento e as viaturas utilizadas (SILVA, 2006).

Assim, é fundamental que os recursos de comunicação ou telecomunicações estejam sempre em condições de pronto emprego, garantindo ainda a confidencialidade, a disponibilidade e a integralidade (MORAES, 2010) das informações que circulam e que são recursos para as tomadas de decisões em ações de segurança pública.

Os órgãos de Estado responsáveis pelas atividades policiais de segurança pública conhecidos como *Public Protection and Disaster Relief* – PPDR – necessitam, em suas atividades de comunicação durante situações operacionais, que se atenda a requisitos como rapidez, confiabilidade e não interrupção dos serviços em situações críticas como: atentados terroristas, desastres naturais e combate à criminalidade (ITU-R, 2015). Para tanto, um segmento de mercado para telecomunicações de órgãos oficiais surge chamado de missão crítica, visando aumentar a aderência a estes requisitos, tratando a informação digitalmente, com integrantes chamados de PMR[1]- *Professional Mobile Radio* (AMARAL, 2006). Os equipamentos de radiocomunicação[2] podem ser empregados em diferentes situações como ferramenta para o exercício do poder informacional no patrulhamento de fronteiras e fases ostensivas de operações policiais.

Abstrair tais diferenças torna os equipamentos menos usuais em muitas oportunidades pois não atendem as exigências da operação por completo, uma vez que a manutenção de uma configuração geral depõe em detrimento de uma condição específica. Um exemplo disso se revela nas atividades de escolta de presos ou dignitários. Ambas envolvem deslocamentos em uma célula de segurança e a necessidade de comunicação o tempo todo entre os policiais que estão nela e eventualmente para algum outro ponto fixo, ou uma outra equipe.

1 Voltado para Government Radio Network – GRN, conhecido como Mission Critical. Destinado a prover radiocomunicação crítica a órgãos oficiais, a tecnologia oferece recursos para requisitos de confidencialidade e integralidade em comunicações digitais criptografadas (AMARAL, 2006).

2 O rádio é um dos meios de comunicação à distância mais antigos, sendo eficiente e de baixo custo, utilizando-se de processos de tratamento da informação de modulação e codificação. Visando a adaptá-las ao meio de comunicação e a fenômenos como a propagação de ondas eletromagnéticas para transmitir mensagens, tem sido empregada em razão de sua eficiência em atividades militares e de segurança pública (SILVA, 2006).

Tais equipes, geralmente, adentram em edificações como palácios, hotéis, presídios, e outros eventos realizados em ambientes externos ou internos. Essa amplitude de ambientes em que a necessidade de comunicação se apresenta, exige dos recursos de telecomunicações em missão crítica requisitos de uma alta dependabilidade.

O objetivo desta pesquisa é descrever em forma de estudo de caso, uma proposta de soluções de uso de equipamentos de telecomunicações em missão e, a partir das experiências de uso da equipe técnica da organização, proporcionar uma melhor percepção do usuário com relação ao sistema baseada na dependabilidade, para exercício do poder informacional em atividades ostensivas. O estudo se desenvolve em um órgão de segurança pública, a Polícia Federal, conforme definido no art. 144 da Carta Magna (BRASIL, 1988).

2. Revisão de Literatura

Na segurança pública, o Estado exerce seu poder pela coibição de delitos e proteção interna de seus cidadãos. Na Sociedade do Conhecimento, a informação é uma forma de exercício de poder (BRAMAN, 2006). Portanto, em atividades de segurança pública, é necessário observar requisitos para o exercício do poder informacional por meio de equipamentos de telecomunicações em missão crítica, observando questões relacionadas à tolerância as falhas em condições adversas ao empregar o equipamento, usando-o de modo aceitável. A primeira parte da revisão de literatura aborda as relações entre o poder informacional e a segurança pública, em seguida os requisitos de dependabilidade por meio dos equipamentos de telecomunicações em missão crítica para o exercício de poder informacional.

2.1 O Poder Informacional e a Segurança Pública

O caráter sigiloso das operações, a restrição de informações no contexto policial se faz necessário (AMARAL, 2006) uma vez que em razão das transformações sociais, políticas e tecnológicas da sociedade fazem com que os sistemas de informação e de telecomunicações se tornem instrumentos de poder para o Estado (BRAMAN, 2006).

"O poder do exército é exercido pelo Estado externamente, defendendo suas fronteiras, o poder da polícia é exercido internamente aos domínios territoriais de um Estado" controlando a sociedade nas formas em que as leis apontam, compondo um sistema de segurança pública. (HABERMAS, 2002, p. 124).

Para Braman (2006) as formas tradicionais em que o Estado exerce seu poder são: de maneira instrumental, (utilizando de seus recursos que remetem a força); estrutural, (relacionados a regras e instituições); e simbólicas (ideias, palavras e imagens).

O desenvolvimento e o acesso cada vez maiores da população a estas tecnologias transformam a sociedade no que Castells (1999) descreve como sociedade em rede: interconectada que possui acesso imediato a grandes volumes de informação e capaz de interagir com ela. Assim surge uma nova forma de exercício do poder pelo Estado: o poder informacional. Capaz de amoldar o comportamento humano pela manipulação da base informacional do poder instrumental, estrutural e simbólico. Tais manipulações possibilitam novas ferramentas de exercício do poder, conforme descrito por Braman (2006, p. 1): "os governos contemporâneos utilizam a informação e as tecnologias de informação de nova maneira e tais práticas em seu objetivo irão mudar a natureza do poder e do seu exercício".

A afirmação de Braman (2006) sustenta a de Souza (2011) no contexto da segurança pública, que pela simples observação das rotinas operacionais, pode-se comprovar que a comunicação é uma ferramenta relevante na condução de missões de segurança. Braman (2006) cita armas inteligentes, como exemplo do efeito do poder da informação sobre o exercício do poder instrumental.

Por analogia, o mesmo conceito pode ser aplicado a sistemas de telecomunicações em missão crítica, uma vez que estas para o Estado são fatores que se relacionam a manipulação do mundo material, onde o fluxo da informação e o domínio desse fluxo informacional atua sobre o poder instrumental empregado pelos órgãos de segurança pública, como ilustra a Fig. 1.

Figura 1– Equipamento de telecomunicação em missão crítica empregado para o Exercício do poder informacional na segurança pública.
Fonte: *Secureland Communications.*[3]

O conceito de informação nesta pesquisa é empregado de modo que ela seja tratada como "recurso para tomada de decisões" (BRAMAN, 2006, p. 12), em nível operacional, tático e estratégico (LAUDON; LAUDON, 2010)[4].

Para Chiavenato (1994) as informações em nível operacional são mais detalhadas, de menor nível de relevância e empregadas para tomadas de decisão em curto prazo, em um ambiente mais hostil e de maior exposição a riscos eminentes, exigindo-se mais das comunicações em missão crítica. Enquanto as decisões de nível tático e estratégico tem impactos maiores, mas em médio e longo prazo, respectivamente, e são tomadas em ambientes mais controlados, e assim com menores exposições a riscos eminentes, se comparados ao nível operacional, conforme Fig. 2.

3 *Secureland Communica*tions. Disponível em: < https://www.securelandcommunications.com/customerstories/integrapol-brazilian-police-network >. Acesso em: 01 fev. 2020.

4 Classificação de sistemas de informação em nível operacional, relacionada aos processos detalhados de execução das tarefas, nível tático ou gerencial, para controle e gestão das execuções em nível operacional, alinhando com as informações estratégicas, estas de alto nível (LAUDON; LAUDON, 2010).

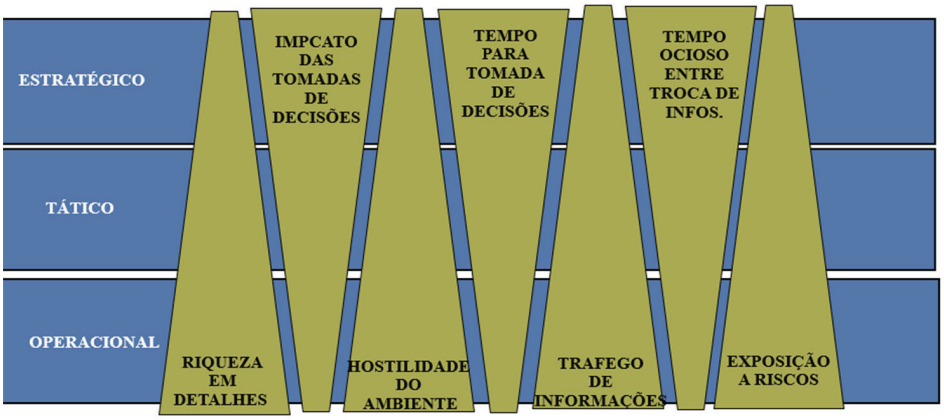

Figura 2– Os níveis de tomada de decisões com relação a seus detalhes, impactos, hostilidades dos ambientes, tempo para tomada de decisões, tráfego de informações e exposição a riscos. Fonte: O autor.

A informação, difundida em sistemas de comunicação deve ser empregada para tomada de decisões em ações de segurança pública, em atividades ostensivas de operações policiais nas atividades relacionadas a comando e controle (ORR, 1983), e seu domínio exercido na forma de poder informacional (BRAMAN, 2006).

Na atividade ostensiva de uma operação policial, segundo Goodman (1984), o domínio das informações e a difusão considerando sua cadeia de comando e controle de modo seguro, utilizando equipamentos apropriados com recursos que remetam a segurança da informação, onde deve ser desejável a fim de evitar a quebra do sigilo de informações, oferecendo possíveis vulnerabilidades ao oponente e que informações estratégicas das ações em campo, ou obtidas quando da investigação, efetivamente cheguem a todos os envolvidos na ação de modo rápido e de forma clara.

Orr (1983) compreendeu que as comunicações e as pessoas não são meros instrumentos de comando e controle, mas fazem parte do processo que chamou de C3I[5] juntamente com a informação advinda da inteligência.

O uso adequado à proteção a vários tipos de ameaças, a fim de minimizar os riscos, bem como a observação de requisitos de segurança da informação, da comunicação e dos operadores, constituem

5 Acrônimo para o processo de comando, controle, comunicação e inteligência (ORR, 1983).

em proteção a informação (ABNT, 2006), o que atribui valor à informação conforme Saracevic (1996) e por esta razão demandam ações relacionadas à segurança da informação e comunicação. Se relacionar a visão de Braman (2006), o valor que a informação tem para o Estado está relacionado ao exercício do poder informacional e a manutenção do domínio sobre ela.

De acordo com Moraes (2010) as proteções necessárias precisam estar relacionadas às seguintes propriedades: confidencialidade (limita o acesso à informação tão somente as áreas legítimas); integridade (garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação); e disponibilidade (a informação esteja sempre disponível para o uso legítimo). Há uma relação de interdependência entre elas, conforme a Fig. 3.

Figura 3 – Requisitos de proteção ao exercício do poder informacional. Fonte: Sêmola (2003)

No modelo de canal de comunicação para um fluxo de informação descrito por Shannon (1948) na Fig. 4, as fontes de ruído podem agir sobre o sinal transmitido, podendo causar alguma alteração no sinal recebido como, por exemplo, alterar ou impedir que a mensagem do emissor chegue corretamente ao destinatário.

Estes fenômenos podem prejudicar a sua inteligibilidade (quando não se possui sinais suficientes para que se possa compreender o conteúdo da informação), integridade (quando a informação recebida é diferente da que foi transmitida), ou disponibilidade (quando por algum motivo, não está disponível).

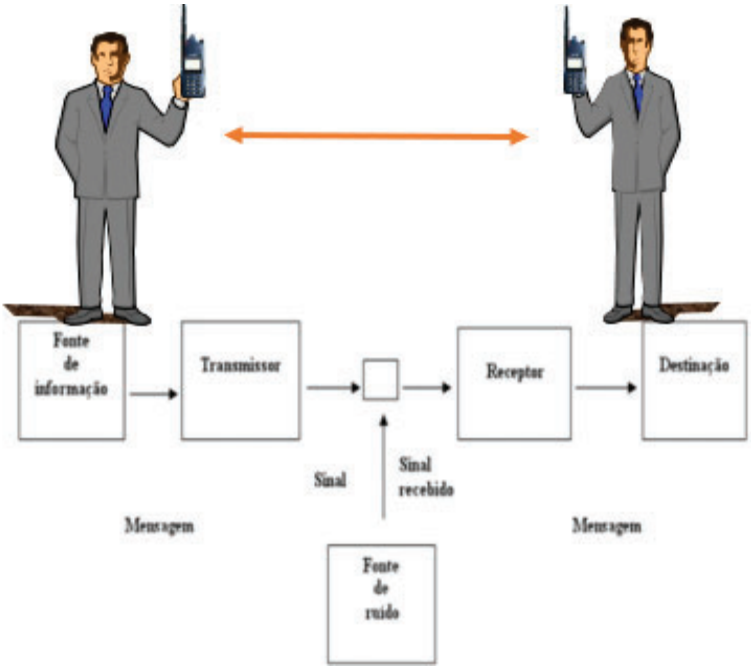

Figura 4 – Modelo de canal de comunicação (Shannon, 1948). Fonte: Adaptado de Shannon (1948, p. 4.)

O ruído no processo pode ser ocasionado por qualquer uma das dimensões envolvidas, seja tecnológica, organizacional ou humana como descrito na Fig. 5 (LAUDON; LAUDON, 2010).

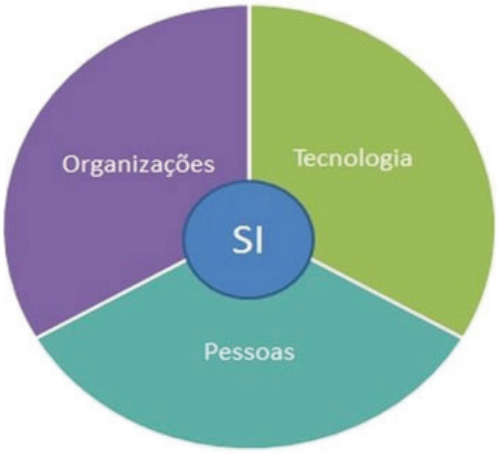

Figura 5 - As dimensões de um sistema de informação. Fonte: Laudon ; Laudon (2010)

As tecnologias envolvem as ferramentas de informação e comunicação propriamente ditas (hardwares e softwares); as dimensões organizacionais referem-se por sua vez a ações administrativas e de gestão que podem contribuir para os requisitos de segurança, já a dimen-

são humana envolve treinamento de usuários e técnicos para operar um sistema, ou seja, envolvem comportamentos que melhorem suas condições de segurança.

Dessa forma, pode-se analisar o processo sob uma visão sistêmica, como proposta para a Ciência da Informação por Araújo (2009), que descreve na corrente teórica que envolve a matemática que Shannon (1948) chama de ruído no fluxo de informação onde reconhece que as questões relativas à comunicação envolvem três níveis de problemas: o primeiro trata dos problemas técnicos, relativos ao transporte físico da materialidade que compõe a informação; o segundo nível se refere aos problemas semânticos (relacionado ao entendimento da mensagem) e o terceiro nível está relacionado com a eficácia da comunicação (relacionando a validade da informação).

Pinheiro (2007) conceitua as ameaças como possíveis violações de um sistema da informação e das comunicações, podendo ser acidental ou intencional, explorando vulnerabilidades que são falhas que se apresentem em uma das dimensões descritas por Laudon e Laudon (2010). Dessa forma, a incerteza causada pelo ruído pode ser associada com ameaças à segurança da informação em redes de telecomunicações em missão crítica, oferecendo riscos à manutenção do domínio da informação e, por consequência, à atividade policial.

Quando uma amaça intencional se coloca de forma premeditada em um sistema de informação, tem-se um ataque (PINHEIRO, 2007) que pode ser com objetivos desde uma simples curiosidade, busca de conhecimento em sistemas, espionagem e até mesmo ferir imagens de governos, o que claramente está relacionado ao poder informacional do Estado, na medida em que fere o exercício do poder simbólico, por meio da falta de domínio da informação.

Dessa mesma forma, relacionando os conceitos de poder informacional de Braman (2006), quando o Estado exerce seus poderes através de órgãos de segurança pública, as ameaças à segurança da informação em uma rede de telecomunicações podem comprometer o exercício do poder informacional pela exploração de falhas na manutenção sob o domínio da informação.

2.2 A Dependabilidade Aplicada a um Sistema de Telecomunicações em Missão Crítica

Fernandes e Rodrigues (2013) descrevem um sistema em missão crítica como aqueles que apoiam diretamente as organizações no cumprimento de sua missão. Um sistema de missão crítica é um sistema que, se interrompido, leva a organização a um estado de crise em um pequeno intervalo de tempo (AMARAL, 2006).

Logo, um sistema de telecomunicações em missão crítica, é um sistema que apoia a polícia no cumprimento de suas missões nas fases ostensivas de operações e de patrulhamento. Para Sommerville (2007) a criticidade de um sistema pode ser chamada de confiança, sendo em inglês empregado o termo *dependability*.

Para Avizienis *et al*. (2004, p. 5) "dependabilidade pode ser definida como a habilidade que um sistema tem de prover serviços que podem ser justificadamente confiáveis". Em outras palavras, pode-se admitir a falha em algumas circunstâncias, mas não a falta do recurso, como no caso de os de telecomunicações em missão crítica.

Pradhan (1996) e Alvizienis *et al*. (2004), defendem que para que um sistema possa apresentar elevada dependabilidade é necessário que se minimizem os impactos de eventuais falhas, através dos atributos: "confiabilidade, disponibilidade, segurança" (*Safety e Security*), como descrito por Weber (2003, p. 6) no Quadro 1.

Quadro 1 - Atributos da dependabilidade

Dependabilidade *(dependability)*	qualidade do serviço fornecido por um dado sistema
Confiabilidade *(reliability)*	capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período
Disponibilidade (*availability*)	probabilidade do sistema estar operacional num instante de tempo determinado; alternância de períodos de funcionamento e reparo
Segurança *(safety)*	probabilidade do sistema ou estar operacional e executar sua função corretamente ou descontinuar suas funções de forma a não provocar dano a outros sistema ou pessoas que dele dependam
Segurança (*security*)	proteção contra falhas maliciosas, visando privacidade, autenticidade, integridade e irrepudiabilidade dos dados

Fonte: Weber (2003, p. 6)

Assim, para que se possa dizer que o sistema possui alta de-

pendabilidade, um usuário deve receber ou desenvolver justificativas aceitáveis para confiar no serviço prestado por um sistema. Ocorre que na prática, nenhum sistema é isento de defeitos. Mas, em um sistema com dependabilidade, eles ocorrem dentro de um limite aceitável pelo usuário em termos de frequência e severidade.

A disponibilidade é a probabilidade de o sistema estar operacional num instante de tempo determinado, alternando períodos de funcionamento e reparo. Ainda conforme Pradhan (1996), com relação à disponibilidade, pode-se afirmar que os sistemas de missão crítica fornecem o serviço esperado para o usuário mesmo na possibilidade da presença de eventuais falhas.

Nesse sentido, ainda conforme Weber (2003), pode-se afirmar que a prevenção de falhas impede a ocorrência ou introdução de novas falhas, e a tolerância a falhas fornecem o serviço na percepção do usuário mesmo na presença de falhas, ainda que provida por outro meio.

Em um sistema de telecomunicações em missão crítica, a disponibilidade está relacionada a cobertura de sinal considerando três modos de operação (ITU-R, 2015):

- Cobertura rede fixa: relacionada à quantidade de estações PMR (ERBs) e canais de comunicação. Essencial na fronteira, em atividades ostensivas de operações policiais, vigilância e patrulhamento (quando são necessários contatos recorrentes com bases de apoio, comando e controle em extensos teatros operacionais) e em grandes eventos (necessárias às atividades integradas de comando e controle).
- Cobertura em rede tática: de uso eventual, onde não há cobertura por rede fixa, em meios urbanos ou rurais, sendo operada por equipe técnica especializada em comunicação e a cobertura é resultante das condições de planejamento[6] e viabilidade de

6 Os quatro T do planejamento tático de comunicação são: Terrain (terreno - a área de cobertura desejada para comunicação, considerando a distribuição dos alvos no teatro operacional, espaço geográfico onde se realiza a operação); Talk (hierarquia de comando e controle de comunicação, estrutura de comando e controle para a definição do Diagrama de Rede de Rádio -DRR (SILVA, 2006); Time: (tempo previsto para ação, para que se possa planejar adequadamente os suprimentos, baterias, homens, equipamentos e Terminals (tipos e quantitativos de terminais, estações, e acessórios necessários considerando as características da operação). Fonte: O autor, adaptado de Souza *et al*. (2015) e ITU-R (2015).

posicionamento (usual quando o comando e controle é realizado por técnica de apoio em profundidade).

- Cobertura no modo direto (ponto a ponto, para comunicação em células aproximadas).

A área de cobertura é definida como a porção geográfica onde é possível acessar o sistema de rádio e o alcance da rede é definido como a mais longa distância, onde um sinal tem a capacidade de conduzir a voz sem distorção ou perda de qualidade (SILVA, 2006).

Nesse cenário, confiabilidade é a capacidade de o sistema atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período.

Já a palavra "segurança" aparece em dois conceitos da dependabilidade: o *safety* que é a probabilidade do sistema ou estar operacional e executar sua função corretamente ou descontinuar suas funções de forma a não provocar um dano a outros sistemas ou pessoas que dele dependam, e o conceito de *security* está relacionado à proteção contra falhas maliciosas, visando privacidade, autenticidade, integridade dos dados. (WEBER, 2003).

Embora se configure uma ferramenta tecnológica a ser considerada na manutenção do poder informacional do Estado, quando em exercício nas atividades ostensivas de operações policiais, as telecomunicações em missão crítica contribuem para o processo, onde os recursos humanos e os organizacionais são tão relevantes quanto, como se descreve no Quadro 2.

Quadro 2 - Relações entre as dimensões de um sistema de telecomunicações em missão crítica e as diretrizes de segurança da informação

	Tecnológica	Organizacional	Humana
Confidencialidade	Criptografia	Gestão das chaves criptográficas	Disciplina do usuário
Integridade	Rádio digital (PMR)	Operação e manutenção da rede	Comprometimento do usuário.

Disponibilidade	Estações rádio base repetidoras; recursos extras (dados, imagens).	Quantitativos de terminais e acessórios adequados; área de cobertura; contratação de serviços/ aquisições.	Usabilidade; experiências de uso; customização; acessórios adequados.

Fonte: O autor (2019)

2.3 Telecomunicações em Missão Crítica na Organização em Análise

Na organização em estudo, a partir do ano de 2005, deu-se início ao uso de uma rede de telecomunicações digitais, considerando alguns requisitos, como por exemplo, a possibilidade de transmitir dados, o uso de protocolo aberto, criptografia ponta a ponta e comunicação digital. Dentre as possiblidades existentes a época (APCO 25, Tetra, e Tetrapol), a tecnologia escolhida para uso foi a Tetrapol[7].

Os requisitos de domínio da informação para o exercício do poder informacional são tratados em um sistema de telecomunicação em missão crítica como o PMR Tetrapol por meio de premissas considerando integralidade e confidencialidade, que são nativas das tecnologias empregadas no sistema, como modulação digital e criptografia.

A disponibilidade estará relacionada aos níveis de dependabilidade ideais e os possíveis, considerado as estruturas existentes na organização: quantidade de terminais, estações, gestão e manutenção do sistema.

Em 2005 estava previsto recursos para cerca de 100 Estações Rádio Base – ERB de telecomunicações em missão crítica com aproximadamente 9000 terminais ativos até o final de 2011 visando à manutenção do requisito de disponibilidade (SOUZA, 2011). No entanto, Cavallim (2007), já alertava para limitações em razão do número de estações previstas no projeto diante de uma área de atuação de 91.426 Km^2.

Para esta pesquisa, delimitou-se como universo de pesquisa a

7 Tetrapol é uma tecnologia de rádio móvel profissional (PMR) digital, troncalizada, para a comunicação de voz e dados com recursos de criptografia. (AMARAL, 2006).

Superintendência Regional de Polícia Federal no Paraná. Na organização, o uso de equipamentos de telecomunicações em missão crítica se dá na maioria das vezes, nas atividades ostensivas e de patrulhamento de fronteiras. Definidas questões relacionadas diretamente à operação policial, pode-se planejar os requisitos de comunicações para a fase ostensiva: quantitativos de terminais, de baterias e de cobertura necessária para que se possa conceber um diagrama de rede de rádio, descrevendo seu funcionamento para atendimento de demanda. O atendimento desta demanda se dá pela área responsável pelos recursos de telecomunicações em missão crítica (SOUZA *et al*., 2015).

Cabe ao Núcleo Regional de Tecnologia da Informação, executar as atividades relacionadas à implementação, ao controle e à fiscalização, garantindo o funcionamento e a manutenção (preventiva e corretiva) dos sistemas de telecomunicações e de informática. Além disso, prestar apoio técnico operacional na gestão e na manutenção em telecomunicações em missão crítica para o desenvolvimento da atividade fim do órgão na área de atuação da unidade regional do Paraná.

3. Procedimento Metodológico

Trata-se de pesquisa de natureza aplicada, caracterizada como exploratória e descritiva, a partir das experiências de uso da equipe técnica da organização em uma abordagem qualitativa sob uma perspectiva construtivista, que é empregada para buscar compreender relações (CRESWELL, 2007) entre a dependabilidade em sistemas de telecomunicações em missão crítica, a percepção do usuário e seus efeitos aplicados à segurança pública. Segundo Gil (2002), uma pesquisa exploratória, tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito, ou a constituir proposições.

Nesta pesquisa, seguindo o preconizado por Creswell (2007), foi empregada uma abordagem qualitativa por meio de técnica de pesquisa de estudo de caso por meio de procedimentos de coleta de dados e análise embasada na teoria.

Utilizando a técnica de revisão bibliográfica, o objetivo não é realizar apenas a repetição do que já foi escrito sobre o assunto, mas

por meio da relação proposta é proporcionar o exame dos conceitos sob uma nova abordagem (MARCONI, 1999), seguindo as etapas destacadas a seguir:

a) Abordagem qualitativa das questões envolvendo as formas de exercício de poder e segurança pública por meio de recursos de telecomunicações em missão crítica e dependabilidade;

b) Coleta de dados por meio de observação sistemática, direta e extensiva do emprego de equipamentos de telecomunicações em missão crítica em atividades ostensivas;

c) Estudo de um caso real prático e análise comparativa entre a teoria e a prática utilizada no caso de estudo;

d) Conclusões e considerações.

Para que se possam constatar as proposições alvo deste estudo, foram realizados uma observação e um levantamento quantitativo e qualitativo de trocas de mensagens por meio de equipamentos de telecomunicações em missão crítica, buscando verificar a dependabilidade do atributo da disponibilidade.

Em um segundo momento, as coletas de dados foram baseadas em informações dos próprios envolvidos nos processos, como gestores do sistema buscando formas de adequar à estrutura existente, com o objetivo de eliminar ou mitigar na medida do possível as vulnerabilidades do sistema causadas por eventual não disponibilidade do sistema. Na análise, empregando uma estratégia de teoria embasada (CRESWELL, 2007), busca-se estabelecer uma interação entre a disponibilidade da rede de telecomunicações em missão crítica e sua contribuição para a manutenção do poder informacional do Estado descrito por Braman (2006) e, por consequência, nas respostas à sociedade pelo combate ao crime, por meio do emprego de atributos de dependabilidade que reflitam na percepção do usuário.

4. Resultados e Análises

Durante a pesquisa, foram realizadas observações sistemáticas de atividades ostensivas recorrentes que empregam os equipamentos de

telecomunicações críticas para troca de mensagens em nível operacional e tático no âmbito da Superintendência Regional de Polícia Federal no Paraná: escolta de dignitário, ocorrida em 2018 no interior do Paraná; escoltas de presos da Operação Lava Jato em Curitiba, em dias e fases diversas ao longo do ano de 2017; no patrulhamento de fronteiras em dias diversos no ano de 2018 e deflagração de operações com mandados de busca e apreensão em Curitiba, ao longo de 2018.

Em observação sistemática de uma escolta de dignitário durante uma operação com três dias de duração e com uma agenda de cerca de sete horas diárias em média, foram contabilizadas uma média superior a oitenta mensagens utilizando equipamentos de telecomunicações críticas por dia de operação. Dessas mensagens, apenas seis em um dia e duas em outros dias envolveram equipes que estavam em posições distantes. Todas as demais mensagens foram trocadas entre os membros aproximados da equipe de segurança, conforme o Quadro 3.

Quadro 3 – Troca de mesagens em escolta de dignitário

OPERAÇÃO 1	DIA 1	DIA 2	DIA 3	Média	Percentual
MENSAGENS	82	84	81	82,3	100,0
LOCAIS	76	82	79	79,0	96,0
DISTANTES	6	2	2	3,3	4,0

Fonte: O autor (2019)

Cenários semelhantes se apresentaram em escoltas de presos. Por exemplo, durante cinco oportunidades foram realizados acompanhamento sistemático. Ainda que em um número bem menor se comparado com a segurança de autoridade, em média dez a cada evento, a maioria das mensagens foram trocadas entre os membros da célula de segurança aproximados, conforme o Quadro 4.

Quadro 4 – Troca de mensagens em escolta de presos

OPERAÇÃO 2	DIA 1	DIA 2	DIA 3	DIA 4	DIA 5	Média	Percentual
MENSAGENS	12	14	8	10	6	10	100
LOCAIS	12	12	8	8	6	9,2	92,0
DISTANTES	0	2	0	2	0	0,8	8,0

Fonte: O autor (2019)

Assim, considerando as duas atividades operacionais distintas nas oito oportunidades testadas, 94 % das mensagens envolviam as equipes aproximadas e apenas 6% mensagens trocadas entre pontos distantes, como ilustra a Fig. 6.

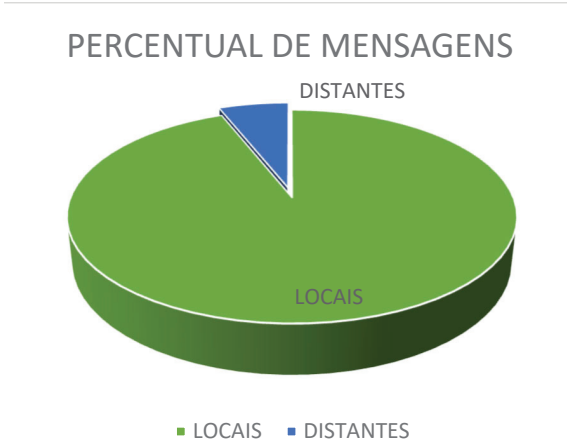

Figura 6 – Troca de mesagens em percentuais
Fonte: O autor (2019)

Já se considerar atividades de patrulhamento de fronteiras , observou-se que o contato das equipes ostensivas em campo e uma base fixa ou de comando e controle são relevantes e realizadas de forma contínua especialmente para troca de informações em nível tático, demandando uma rede de telecomunicações em missão crítica, operando com estações e repetidoras uma vez que as distâncias, geralmente, existem entre a base e as equipes de campo (muitas vezes mais de uma), bem como existe a necessidade de cobertura e abrangência em toda a área em que as operações ocorrem.

O mesmo pode-se aplicar a fases ostensivas de operações policiais, em que se observou grande mobilização de efetivo policial no cumprimento de mandados de prisão e de busca e apreensão em razão das investigações anteriores, com uma mescla de informações em nível tático e operacional, exigindo a tomadas de decisão em nível tático tempestivamente, assim como nas atividades de patrulhamento, demandando a disponibilidade de uma área de cobertura do tamanho do teatro operacional.

Considerando os requisitos de dependabilidade, os que envolvem a segurança do sistema são próprias dos equipamentos de telecomu-

nicações em missão crítica, residindo na dimensão tecnológica do sistema. A disponibilidade pode estar relacionada a outras dimensões como a organizacional, relacionada diretamente com a busca de uma área de cobertura ideal para as operações.

Da mesma forma, a confiabilidade estará relacionada à configuração correta dos equipamentos de telecomunicações em missão crítica, planejamento para uso nas fases ostensivas de operações policiais e no patrulhamento de fronteiras.

Circulando na área de abrangência das estações da rede, muitas vezes são percebidas a existência de áreas de sombra, (sem sinal da repetidora ou estação rádio base de um sistema PMR) o que pode levar o usuário a uma percepção de que o equipamento não funciona, em razão de uma eventual falha de disponibilidade do sistema em suas áreas de cobertura. Elas se apresentam por razões diversas, desde questões topográficas ou de edificações. De acordo com Silva (2006), os fatores que prejudicam as comunicações são os descritos no Quadro 5.

Quadro 5 – Fatores que prejudicam as comunicações

Topografia	Quando acidentada, as comunicações com esses equipamentos sofrem variações de frequência, ou seja, o alcance é limitado e pode não atingir o receptor.
Vegetação	A densidade da vegetação pode atenuar o sinal, limitando o alcance do equipamento.
Edificações	Comprometem a comunicação, limitando ou refletindo o sinal de rádio.
Linhas de transmissão elétrica	Seu campo eletromagnético causa interferência nas emissões de rádio.

Fonte: O autor (2019)

Dessa forma, utilizando-se das redes PMR e repetidoras, os usuários do sistema de telecomunicações em missão crítica em escoltas, frequentemente entram em edificações, passam por elevadores, hotéis, casas de custódia, etc., que são edificações que constantemente apresentam dificuldades para a disponibilidade dos recursos de telecomunicações, o que nessas situações pode comprometer o exercício do poder informacional.

A fim de minimizar os problemas de disponibilidade considerando estas situações, e considerando ainda que a maior parte das comunicações nas atividades de escolta está relacionada aos trabalhos aproximados das equipes em campo, e a necessidade de tomadas de decisão em tempo real no nível operacional, usuários sugerem inovações no processo.

Nesse sentido, a equipe técnica, que faz a gestão do sistema sugere que ao invés de utilizar os terminais de telecomunicações em missão crítica na rede PMR ou repetidoras, dependendo de sinais que venham delas até os terminais, necessitando assim de uma alta disponibilidade e área de abrangência de sinal, o que dificilmente se pode garantir mesmo em condições adversas, é que se empreguem os terminais no modo direto de operação, ou seja, cada terminal transmitindo diretamente para os outros terminais no mesmo canal sem que se tenha a necessidade de conexão com uma repetidora ou estação da rede PMR.

Nesse modo de operação, se exclui a necessidade de que os terminais estejam na área de cobertura de uma repetidora ou estação da rede, mas se mantem a disponibilidade dos recursos de telecomunicações para a maioria das mensagens, visto que a maior parte delas se apresenta entre os membros da equipe aproximada, que mantém as condições de comunicação no modo direto, justamente em razão da proximidade dos terminais.

Segundo o fornecedor (EADS, 2008), no modo direto, os terminais são capazes de manter comunicações no modo direto em distâncias de até 2 km.

Esse modelo privilegia a disponibilidade dos recursos para a maioria das mensagens que no modelo anterior poderia estar sujeitada a falta de disponibilidade mesmo quando os terminais estão próximos entre si, o que para o usuário trazia a percepção de que a dependabilidade ficasse prejudicada, ou que o sistema não funcionasse.

Se a grande maioria aferida em condições reais de trabalho das comunicações em situações de escolta de presos e de dignitários são trocadas entre membros da equipe que estão próximos, a proposta pode ser validada. A comunicação com postos fixos, que representaram uma

minoria das situações não é totalmente prejudicada, pois ainda podem ser realizadas dentro de um raio de 2 km.

Dessa forma, se privilegia a tomada de decisões em nível operacional em tempo real, enquanto as decisões táticas podem ser tomadas tempestivamente em um prazo maior (CHIAVENATO, 1994), podendo aguardar o momento de maior proximidade ou emprego de recurso de comunicação alternativo, se for o caso.

Isso atende à demanda das escoltas, que normalmente avisam os postos fixos que estão próximos e recebem informações dos postos fixos sobre as condições locais para receber a equipe de segurança, e exercendo o poder informacional nessas fases de operações policiais, podendo aguardar o momento de maior proximidade ou emprego de recurso de comunicação alternativo, se for o caso, ou ainda empregar o uso combinado quando a situação requerer contato com bases mais distantes. Tais possibilidades devem ser debatidas conforme planejamento operacional de comunicações definido entre a coordenação de operação e a equipe de comunicações. (SOUZA *et al*., 2015).

Para tanto, é necessário capacitar os policiais envolvidos nas ações para que possam ter esta percepção, enfatizando a necessidade de comunicação rápida e eficaz na célula de segurança prioritariamente, podendo admitir, nos termos da dependabilidade, a falta pontual da cobertura em condições específicas, mas usufruindo da disponibilidade do recurso de telecomunicações em missão crítica na maior parte das situações.

Nas fases ostensivas de operações policiais em que são necessários grande mobilização de efetivo, para compor um grande número de equipes para cumprir mandados, buscas ou apreensões em diversos endereços dentro de uma área geográfica ou no patrulhamento de fronteiras, em que atividades de vigilância são realizadas, o uso dos recursos de telecomunicações em missão crítica em rede por estações ou repetidoras é necessário em razão das necessidades de disponibilidade em grandes áreas de coberturas e constante contatos com bases fixas para apoio nas atividades em campo, em tarefas típicas de comando e de controle.

Nesses casos, o exercício do poder informacional pelas equipes de campo também pode ser exercido pela disponibilidade e confiabili-

dade do sistema, nas dimensões humanas e organizacionais, visto que os requisitos nas dimensões tecnológicas já são próprios dos sistemas PMR.

No entanto, é recorrente a necessidade de contato com uma base em situações extremas, inclusive para solicitar reforços, o que remete a necessidade de comunicações em rede. Dessa forma, os insights de aprendizagem de uso sugerem uma inovação no processo de comunicação, onde ao invés de todos os terminais estejam na rede, sujeitos aos problemas de disponibilidade já relatados, os terminais de mão, chamados de hand-transceptor (HT), estejam com os usuários aproximados da equipe em modo direto, garantindo a comunicação entre eles, e um dos rádios, normalmente embarcado em uma viatura, esteja em conexão com as bases para comunicação tática e estratégica, para emprego de comando e de controle.

Considerando tais demandas das atividades ostensivas e de patrulhamento de fronteiras, a área responsável pelos recursos de telecomunicações em missão crítica sugeriu como forma de melhorar a dependabilidade do sistema, considerando o requisito da disponibilidade refletindo na percepção do usuário, as propostas descritas no Quadro 6.

Quadro 6 – Propostas de uso para mitigar problemas com a disponibilidade

Instalação de terminais veiculares nas viaturas ostensivas e embarcações	A utilização de antenas de ganho e rádios veiculares com potência maior, resultando em menores áreas de sombra em rede fixa (ERBs)e rede tática (repetidora)
Incentivo de uso do modo direto (ponto a ponto) nos terminais de mão	Privilegiando as comunicações entre os membros da célula aproximada, mesmo em áreas de sombra.
Uso combinado	Terminais veiculares das viaturas e embarcações no modo rede fixa, ou modo tático e, adicionalmente, terminais de mão no modo direto.

Fonte: O autor (2019)

O mesmo processo pode ser utilizado em atividades semelhantes, como as que envolvem o patrulhamento de fronteiras e vigilância, bem como em grandes eventos. Os rádios embarcados apresentam maiores potências de transmissão, e antenas com maiores ganhos em potência se comparados aos terminais de mão (EADS, 2008).

5. Conclusão

Pode-se compreender que as questões organizacionais, tecnológicas, ocupacionais, espaciais e culturais expostas por Capurro e Hjorland (2007), em um contexto de um sistema de telecomunicações podem se relacionar a segurança da informação na medida em que se expõem as ameaças ocasionadas por vulnerabilidades em um sistema de telecomunicações em missão crítica, como os ruídos descritos por Shannon (1948) interferindo no fluxo de informação.

Nesse sentido, a manutenção do poder informacional do Estado apresentado por Braman (2006) relaciona-se com o domínio sobre o fluxo da informação por parte dos órgãos de segurança pública nas atividades ostensivas.

Para tanto, devem atentar aos requisitos de segurança da informação, não apenas nas dimensões tecnológicas, mas também nas dimensões humanas e organizacionais, para que eventuais ameaças ofereçam riscos controlados para que mantenha o domínio sob a informação necessário para que exerçam o poder informacional, contribuindo assim para o sucesso de operações policiais em razão da condição estratégica que os sistemas de informação representam para estes órgãos.

Dessa forma, os conceitos de dependabilidade podem fornecer alternativas baseadas na percepção dos usuários e nas experiências de uso da equipe técnica, de modo a oferecer o emprego efetivo do equipamento mesmo em áreas de sombra ou falhas de cobertura, podendo-se admitir uma maior área de abrangência.

Assim, o emprego dos equipamentos no modo direto ou ainda combinado com equipamentos veiculares proporciona a percepção de disponibilidade do sistema para seu uso efetivo, de modo que em locais que poderiam ser considerados áreas de sombra para um terminal de mão de telecomunicações em missão crítica, para um terminal embarcado, é uma área com cobertura de sinal, que contribui para a manutenção do poder informacional pelo requisito da disponibilidade para tomada de decisões em nível operacional em tempo real, possibilitando a troca de mensagens em nível tático e estratégico de modo tempestivo.

Para tanto, é necessário na dimensão humana que um usuário esteja atento aos dois terminais sintonizados nos diferentes modos de operação, afim de formar o fluxo de informação, quando necessário.

Nesse sentido, é necessário também a capacitação e treinamento continuado com abordagens específicas para estes casos, como as empregadas nas experiências da Superintendência Regional de Polícia Federal no Paraná, de modo especial, nas escoltas de presos da Operação Lava Jato, ou nas atividades de patrulhamento de fronteiras, visando a manutenção do poder informacional nas atividades ostensivas de polícia.

Dessa forma, em um ambiente colaborativo, mais uma vez se tem uma demanda que se apresenta a área responsável pelas telecomunicações em missão crítica, proporcionando uma oportunidade de aprendizagem pelo uso, em que a solução se demostre na dimensão organizacional pelo planejamento dos recursos em níveis de tomada de decisão na perspectiva humana, pela capacidade de operar em condições adversas.

Luciano Castilho Assumpção

Polícia Federal

Agente de Telecomunicações da Polícia Federal, Mestre em Ciência da Informação pela UFSC. Especialista em Gestão da Segurança da Tecnologia da Informação e Comunicações pela UnB/DF e em Telecomunicações pela ESAB/ES. Professor Universitário e da Academia Nacional de Polícia, na disciplina de Técnicas Operacionais-Comunicação no CFP 2019.

Dependability in a Mission-Critical Telecommunications System: The User Perception as an Instrument of Informational Power for Public Security

ABSTRACT

In the information society, the proper use of mission-critical telecommunications equipment in public security operations aims to meet the requirements of information domain and operator security. Therefore, the informational power evidenced in the Police actions is exercised as such requirements are met. Dependability describes the relationship between these requirements and the perception of users through acceptable levels of flaws in situations such as when the availability requirements depend on the organization's infrastructure and its limitations. The aim of this research is to describe proposed solutions based on use experiences based on dependability. It is an exploratory and descriptive research using case studies, analysis, and direct observation of exchange of messages in police operations, and developing proposals for solutions from the experiences of use based on the patterns found. The results propose alternative ways of using the equipment even in the presence of coverage flaws, ensuring availability requirement. Thus, it is possible to provide a better perception of the user with respect to the system, proposing alternatives to the exercise of informational power in ostensive activities and considering not only technological issues, but also human and organizational ones.

Keywords: Dependability. Mission-critical. Telecommunications. Public Security. Informational power.

Dependabilidad en un Sistema de Telecomunicaciones en una Misión Crítica: la Percepción del Usuario Como Instrumento del Poder Informativo para la Seguridad Pública

RESUMEN

En la sociedad de la información, el uso adecuado de equipos de telecomunicaciones en misión crítica en operaciones de seguridad pública tiene como objetivo anticipar

los requisitos para el dominio de la seguridad de la información y los operadores. De esta forma, el poder informativo evidenciado en la actuación de la Policía se ejerce en la medida en que se cumplan dichos requisitos. La confiabilidad describe la relación entre estos requisitos y la percepción de los usuarios a través de niveles aceptables de fallas en situaciones como cuando los requisitos de disponibilidad dependen de la infraestructura de la organización y sus limitaciones. El objetivo de esta investigación es describir las soluciones propuestas centradas en experiencias de uso basadas en la confiabilidad. Se trata de una investigación exploratoria y descriptiva que utiliza estudios de caso, análisis y observación directa del intercambio de mensajes en operativos policiales y desarrollo de propuestas de soluciones a partir de las experiencias de uso a partir de los patrones encontrados. Los resultados proponen formas alternativas de uso del equipo incluso en presencia de fallas de cobertura, asegurando el requisito de disponibilidad. Así, es posible brindar una mejor percepción del usuario en relación al sistema, proponiendo alternativas al ejercicio del poder informativo en actividades ostensivas y considerando no solo aspectos tecnológicos, sino también humanos y organizacionales.

Palabras clave: Fiabilidad. Misión crítica. Telecomunicaciones. Seguridad pública. Poder informativo.

Referências

AMARAL, C. T. Interoperabilidade nos Padrões de Rádio Troncalizado Digital. Rio de Janeiro. 2006. 55 p. Monografia (Sistemas de Telecomunicações) — Universidade Federal Fluminense/ Centro de Estudos de Pessoal - Exército Brasileiro. Disponível em: https://pt.scribd.com/document/45732639/Interoperabilidade-em-Sistemas-de-Radio-Digital-de-Seguranca-Publica-P25-Tetra-Tetrapol-Monografia- Acesso em: 18 nov. 2019.

ARAÚJO, C. A. A. Correntes teóricas da ciência da informação. Ciência da Informação, Brasília, v. 38, n. 3, p. 192-204, dez. 2009. FapUNIFESP (SciELO). DOI: http://dx.doi.org/10.1590/s0100-19652009000300013. Disponível em: http://www.scielo.br/scielo.php?pid=S010019652009000300013&script=sci_abstract&tlng=pt Acesso em: 9 dez. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2006.

AVIZIENIS, A.; LAPRIE, J. C.; RANDELL, B; LANDWEHR,

C. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE transactions on dependable and secure computing. v.1, n.1, p. 1-23. Jan/mar. 2004. Disponível em: https://www.nasa.gov/pdf/636745main_day_3-algirdas_avizienis.pdf. Acesso em: 12 set. 2019.

BRAMAN, S. Change of State. Cha Information, Policy, and Power. Ca The MIT Press. Cambridge Mand London, 2006.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. 40. ed. São Paulo: Saraiva, 2007.

CAPURRO, R.; HJORLAND, B. O conceito de informação. Perspectivas em Ciência da Informação, [s.l.], v. 12, n. 1, p. 148-207, abr. 2007. FapUNIFESP (SciELO). DOI: http://dx.doi.org/10.1590/s1413-99362007000100012. Disponível em: http://www.scielo.br/scielo.php?pid=S1413-99362007000100012&script=sci_arttext. Acesso em: 2 jan. 2020.

CASTELLS, M. A Sociedade em rede. Vol. 1. São Paulo: Paz e Terra, 1999.

CAVALLIM, N. L. A Implantação do Sistema Digital de Radiocomunicação TETRAPOL na Polícia Federal. 2007. Monografia (Curso Especial de Polícia) - Academia Nacional de Polícia, Brasília, DF, 2007.

CHIAVENATO, I. Introdução à teoria geral da administração. Rio de Janeiro: Elsevier, 2003.

CRESWELL, J. W. Projeto de pesquisa: métodos qualitativo, quantitativo e misto. 2. ed. - Porto Alegre: Artmed, 2007.

EADS. Workshop de radiocomunicação TETRAPOL. Brasília, 2008.

FERNANDES, J.; H. C.; RODRIGUES, G. Fundamentos Da Gestão Da Segurança da Informação. Notas de Aula (Especialização) - Curso de Especialização em Gestão da Segurança da Informação e Comunicações - CEGSIC / Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília. 2013.

GIL, A. C. Como Elaborar Projetos de Pesquisa. 4. ed. São Paulo: Atlas, 2002.

GOODMAN, I.R. Toward a General Theory of C3 Processes. San

Diego, Jan.

84. Disponível em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a216154.pdf. Acesso em: 8 jan. 2020.

HABERMAS, J. A Inclusão do outro: estudos de teoria política. São Paulo: Loyola, 2002.

ITU-R – International Telecommunicacion Union-Radiocommunication. Radiocommunication objectives and requirements for Public Protection and Disaster Relief (PPDR): Report ITU-R M.2377-0. ITU: Geneva, 2015. Disponível em: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2377-2015-PDF-E.pdf Acesso em: 30 set. 2019.

LAUDON, K; LAUDON, J. Sistemas de informação gerenciais. 9. ed. São Paulo: Pearson Prentice Hall, 2010.

MARCONI; M. de A.; LAKATOS, E. M. Técnicas de pesquisa. 4. ed. São Paulo: Atlas, 1999.

MORAES, A. F. Redes de Computadores Fundamentos. 7. ed. São Paulo: Érica, 2010.

ORR, G. E. Combat Operations C3I: Fundamentals and Interactions. Maxwell Air Force Base: Air University Press, 1983.

PINHEIRO, J. M. dos S. Ameaças e Ataques a Sistemas de Informação: prevenir e antecipar. Cadernos UniFOA, v. 2, n. 5, p. 11-21, Dez. 2007. Disponível em: http://revistas.unifoa.edu.br/index.php/cadernos/article/view/885/790. Acesso em: 7 nov. 2018.

PRADHAN, D. K., Fault-Tolerant System Design. Prentice Hall: New Jersey, 1996.

SARACEVIC, T. Ciência da Informação: origem evolução e relações. Perspectivas em Ciência da Informação, v. 1, n. 1, p. 41-62, Jan./jun. 1996. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235. Acesso em: 28 out. 2018.

SÊMOLA, M. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

SHANNON, C. A. Mathematical Theory of Communications. The Bell System Technical Journal, v. 27, p. 379-423, Jul./out. 1948.

Disponível em: http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf. Acesso em: 28 dez. 2019.

SILVA, E. N. Manual de Radiocomunicação. Brasília: Academia Nacional de Polícia, 2006.

SOMMERVILLE, I. Engenharia de Software. 8. ed. São Paulo: Persson, 2007.

SOUZA, C. L. et. al. Manual de Planejamento Operacional. Brasília: Academia Nacional de Polícia, 2015.

SOUZA, J. L. P. de. Rede Brasileira de Radiodifusão Segura: uma opção nacional.

2011. Monografia (Curso de Altos Estudos de Política e Estratégia)-Departamento de Estudos da Escola Superior de Guerra. Disponível em: http://livrozilla.com/doc/1005444/souza--jos%C3%A9-luiz-povill-de.-rede-brasileira-de-radiodifus. Acesso em: 17 out. 2018.

WEBER, T.S. Tolerância a falhas: conceitos e exemplos. Apostila do Programa de Pós-Graduação–Instituto de Informática-UFRGS. Porto Alegre. 2003. Disponível em: http://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF Acesso em: 12 out. 2019.