O ASPECTO INFORMACIONAL NO LEVANTAMENTO DE CENÁRIOS PARA COMUNICAÇÕES CRÍTICAS EM SEGURANÇA PÚBLICA NO BRASIL[1]

THE INFORMATIONAL ASPECTS IN THE SURVEY OF SCENARIOS FOR CRITICAL COMMUNICATIONS FOR PUBLIC SAFETY IN BRAZILAL UNIVERSITY OF PARAÍBA

Débora Vanessa Campos Freire
ORCID: https://orcid.org/0000-0002-6580-6377
Doutoranda no Programa Doutoral em Avaliação de Tecnologia – Universidade Nova de Lisboa." que seja substituído por: "Doutoranda no Programa Doutoral em Avaliação de Tecnologia – Universidade Nova de Lisboa, pesquisadora no Centro Interdisciplinar de Ciências Sociais CICS.NOVA
deborafreire@gmail.com

Ana Clara Cândido
ORCID: http://orcid.org/0000-0003-1897-3946
Doutora em Avaliação de Tecnologia – Universidade Nova de Lisboa. Docente no Departamento de Ciência da Informação da Universidade Federal de Santa Catarina.
acc.anaclara@gmail.com

RESUMO: As redes de radiocomunicação são uma das principais ferramentas de apoio das entidades que desenvolvem ações em Segurança Pública, sendo necessária constante modernização e atualização destas tecnologias para que estas possuam uma ação efetiva perante a sociedade. Entendendo que este problema engloba, além dos aspectos técnicos, os aspectos relacionados ao contexto social ao qual estes sistemas estão inseridos, este estudo tem como objetivo: realizar um levantamento de possíveis cenários, através da aplicação de entrevistas a especialistas na área com questões baseadas na Teoria da Atividade, objetivando auxiliar na realização de um exercício de Avaliação Tecnológica dos sistemas empregados para radiocomunicação digital na Segurança Pública no Brasil, visando auxiliar os gestores destes órgãos no processo de Tomada de Decisão. Trata-se de uma pesquisa exploratória do ponto de vista dos procedimentos metodológicos, e aplicada através do uso de dados primários e secundários. É assim caracterizada tendo em vista que aproxima temáticas de áreas distintas para a realização de um exercício de Avaliação Tecnológica. O resultado esperado ao final da pesquisa é o suporte para a realização da Avaliação Tecnológica, através de análise dos possíveis cenários que deverão ser avaliados durante o exercício, além do fortalecimento da potencialidade da Ciência da Informação para solução de problemas reais advindos de áreas técnicas.

PALAVRAS-CHAVE: Avaliação Tecnológica. Ciência da Informação. Land Mobile Radio (LMR). Long Term Evolution (LTE). Segurança Pública.

ABSTRACT: Radiocommunication networks are one of the main support tools of agencies that carry out actions in public safety field, and it is necessary to update these technologies in order to have an effective action before society. Understanding that this problem encompasses, besides the technical aspects, the aspects related to the social context to which these systems are inserted, this study aims to carry out a survey of possible scenarios, through the application of interviews with specialists in the area, with questions based on the Theory of Activity, aiming to assist in the accomplishment of a Technological Assessment exercise of the systems for digital radiocommunication in Public Safety, to assist the managers in the decision-making process. It is an exploratory research, from the point of view of methodological procedures, and it is applied through the use of primary and secondary data. It is characterized in view that it approximates different thematic areas to carry out a Technological Assessment exercise. The expected result is the support for the Technological Assessment, through analysis of the possible scenarios that should be evaluated during the exercise, besides strengthening the potential of Information Science to solve real problems coming from technical areas.

KEYWORDS: Technological Assessment. Information Science. Land Mobile Radio (LMR). Long Term Evolution (LTE). Public Safety.

1 Introdução

As tecnologias de comunicação sem fio desempenham papel central nas operações de Segurança Pública. Diante disso, uma comunicação não eficiente, ou até mesmo uma ausência de estrutura de radiocomunicação, pode acarretar situações perigosas que colocariam em risco os profissionais que atuam nesse segmento e até mesmo a sociedade.

Portanto, atuações em Segurança Pública exigem que o sistema de rádio apresente uma robustez e diversidade de aplicações e situações que forneçam soluções rápidas, confiáveis, seguras e escalonáveis, para atender as mais diversas situações que se apresentam no dia-a-dia.

Por estas e outras questões relativas à estratégia de atuação dos órgãos de Segurança Pública, os sistemas de radiocomunicação utilizados são denominados Comunicações Críticas e possuem características específicas, descritas em protocolos internacionais para esses tipos de sistemas [2].

[2] Os órgãos responsáveis por este assunto são: European Radiocommunications Committee (ERC), Federal Communications Commission (FCC), Tetra & Critical Communications Association (TCCA), 3rd Generation Partnership Project (3GPP), European Telecommunication Standards Institute (ETSI), Telecommunications Industries Association (TIA) e TETRAPOL Forum.

A utilização de redes digitais seguras por meio de implantação, operação e gestão pelos próprios órgãos de segurança representou um importante marco para a modernização das forças de Segurança Pública no Brasil.

Contudo, diversos problemas também surgiram devido à forma como estes sistemas vêm sendo implantados e geridos, como por exemplo a falta de corpo técnico suficiente para manter e gerir a rede, e também a falta de planejamento para atualização e modernização dos sistemas.

Além disso, cada um dos órgãos de segurança de atuação nacional, bem como as Secretarias de Defesa Social (SDS) dos estados, investem em redes próprias, o que implica em multiplicidade de esforços e investimentos, assim como uma maior dificuldade na integração e interoperabilidade de sistemas entre as diferentes agências (FREIRE; CÂNDIDO, 2018).

As tecnologias utilizadas atualmente pelos órgãos de Segurança Pública no

Brasil, sendo estas a APCO 25, TETRA e TETRAPOL, apesar do bom atendimento e comunicação de voz, possuem baixa eficiência espectral, capacidades limitadas de transmissão de dados e altos custos devido à falta de economia de escala dos equipamentos e acessórios. Com transmissão variando de 7,2kbps a 50kbps, dependendo da tecnologia, esses sistemas oferecem taxas insuficientes para abarcar as aplicações de dados atuais, com ampla gama de serviços centrados em dados.

Por conseguinte, é comum que as agências de segurança contratem serviços para provimento de banda larga móvel, providos a partir de redes comerciais destinadas a atender a população (GSMA, 2018), sem prioridade de uso para Comunicações Críticas. Além disso, a construção e manutenção de uma rede dedicada para cada agência é complexa, demorada e com alto custo.

Dessa forma, os órgãos estão buscando inovações tecnológicas para modernização de suas redes. As organizações, por diversos fatores, buscam gerar e adotar inovações tecnológicas, sendo "adoção" quando a inovação é desenvolvida em outros lugares e é nova para a organização que adota. Esses fatores podem ser, por exemplo, para operar de forma eficiente e eficaz, ganhar vantagem competitiva sobre a concorrência ou até mesmo se adaptar ao ambiente em que está inserida (DAMANPOUR, 2017).

Em empresas com fins lucrativos, o objetivo para buscar inovação tecnológica provavelmente envolve aumento na receita e maior participação no mercado. Já em entidades governamentais, inovar tem o objetivo de melhorar os serviços prestados aos cidadãos, para melhor atuação perante a sociedade.

Contudo, antes da escolha de uma tecnologia, deve-se analisar diversas perspectivas de informações em diversas áreas e fontes, buscando consolidá-las através de um método científico que possibilite verificar o impacto que a implantação da tecnologia irá representar dentro do contexto pesquisado.

Nesse sentido, os investimentos em tecnologias para melhorar a segurança pública devem focar em melhorias que tenham resultados efetivos, realizando uma projeção do impacto desta tecnologia na sociedade antes do seu desenvolvimento

ou adoção, atendendo ao requisito de eficiência no gasto público através da escolha adequada de uma tecnologia que trará resultados positivos para a comunidade.

Nestes termos, a abordagem da Avaliação Tecnológica (AT) ou Technology Assessment, pretende ser um apoio para a Tomada de Decisão, podendo ser realizada a partir do levantamento do cenário atual existente e projeções de cenários futuros, incluindo, nestas projeções, a realização de provas de conceito, proof of concept (POC), para novas tecnologias.

Através de comparações das principais vantagens e desvantagens das tecnologias empregadas, procura-se fornecer embasamento para o processo decisório dos gestores com relação ao futuro dessas tecnologias.

Durante os anos 1980, a AT tornou-se um instrumento de política pública, utilizada para apoiar vários atores envolvidos na tomada de decisões em inovação. Observa-se que, já no final dos anos 80, a noção de Avaliação de Tecnologia Construtiva (ATC) consolidou-se na Europa, existindo tipos diferentes de ATC, contudo, com o mesmo princípio: antecipar os aspectos sociais em um estágio inicial do desenvolvimento para obter uma melhor tecnologia para a sociedade (MERKERK; SMITS, 2008).

Torna-se importante mencionar que, para uma aprofundada avaliação, é necessária uma análise detalhada do projeto com a previsão de resultados e cenários a partir das condições iniciais consideradas, com o intuito de comparar sistemas distintos considerando os mesmos parâmetros de referência.

Dessa forma, este trabalho pretende realizar o levantamento de possíveis cenários a partir do tratamento informacional da percepção dos especialistas no assunto. O objetivo geral do estudo é apresentar contribuições a partir do levantamento e análise de cenários para Comunicações Críticas em Segurança Pública no Brasil, como suporte para exercícios de AT.

2 O Suporte da Ciência da Informação para a aplicação prática

A comunicação está presente em todas as ações policiais. Neste estudo é analisada a comunicação utilizada em sistemas de radiocomunicação digital pelos órgãos de Segurança Pública. Portanto, a informação considerada neste processo possui um contexto social abrangente, sendo este toda a comunidade onde o órgão atua.

Justifica-se, assim, a importância em aproximar este estudo da Ciência da Informação (CI), para além das ciências exatas. Nas palavras de Wersig e Neveling (1975, p.173), "[...] transmitir o conhecimento para aqueles que dele necessitam é uma responsabilidade social, e essa responsabilidade social parece ser o verdadeiro fundamento da CI".

Indo mais além, a transmissão do conhecimento precisa ser otimizada para que essa responsabilidade social da CI possa ser atingida. A realização de exercícios de AT busca consolidar as informações estratégicas no intuito de auxiliar os gestores dos órgãos de segurança no processo decisório.

O objeto de estudo permeia um problema informacional; portanto, a CI apresenta potencialidades de contribuição, dada a interdisciplinaridade e a natureza de ciência social aplicada.

De acordo com Borko (1968), A CI tem tanto um componente de ciência pura, que se dá através da pesquisa dos fundamentos, sem se preocupar com sua aplicação, quanto um componente de ciência aplicada, ao desenvolver produtos e serviços.

Dessa forma, a transmissão, transformação e uso de informação estão na área de estudos da CI, buscando, através do caráter interdisciplinar dessa ciência, agregar conceitos de outras áreas do conhecimento para auxiliar no processo informacional em análise.

Essa característica interdisciplinar, de acordo com Saracevic (1996), constitui até mesmo um dos motivos da existência da CI, além do imperativo tecnológico imposto à atual sociedade da informação, que vincula inexoravelmente a CI à tecnologia da informação. Nesse sentido, a AT, tendo que trazer conceitos de diversas

áreas que circundam a tecnologia que será avaliada, pode ser considerada parte da CI, ligada à área de ciência social aplicada.

A noção de informação como a que reduz a incerteza pode ser vista como um caso especial de informação como conhecimento. Às vezes, a informação aumenta a incerteza ao invés de diminui-la (BUCKLAND, 1991).

Através de uma AT, considerando diversos fatores, como usuários, especialistas, tecnologia, sociedade, governo e empresas privadas, busca-se verificar as informações necessárias para o auxílio no processo de tomada de decisão, analisando de forma ampla os contextos envolvidos, sendo a gestão da informação, nesse quesito, utilizada para a redução de incertezas.

Nesse sentido, a compatibilização de mecanismos e padrões de tratamento da informação podem minimizar conflitos na ecologia informacional.

> Até que a tecnologia tenha capacidade para permitir a interação direta entre os vários manipuladores da informação, tal incompatibilidade não constitui problema sério. Mas, com o aumento das novas capacidades tecnológicas e do número de novos atores no processo, além das crescentes demandas de informação orientada para o usuário, o alto grau de incompatibilidade torna-se crítico (SARACEVIC, 1996, p. 59).

Os problemas tratados por AT são amplos; portanto, as tentativas de solução não podem ser desenvolvidas isoladamente dos demais atores e mecanismos da cadeia ecológica, exigindo, como regra, a consideração dos vários outros atores e mecanismos no conjunto maior da ecologia informacional.

Segundo Saracevic (1996), considerando que a ciência e a tecnologia são críticas para a sociedade da informação, prover meios para que os indivíduos sejam fornecidos de informações relevantes também se faz crítico. Nesse sentido, a AT, através da consolidação de informações estratégicas no intuito de auxiliar no processo decisório, executa um papel considerado crítico.

3 Procedimentos metodológicos

A presente pesquisa é de natureza aplicada, com abordagem quantitativa e qualitativa, e caracteriza-se como exploratória e descritiva do ponto de vista da natureza do objetivo. São utilizados dados primários e secundários, visando aproximar temáticas de áreas distintas para a realização de um exercício de AT.

Os dados secundários foram obtidos através de Revisão Sistemática de Literatura (RSL) e revisão bibliográfica, através de livros e documentações técnicas disponibilizadas por órgãos que regulamentam e definem Comunicações Críticas.

Como levantamento de dados primários, foram realizadas entrevistas com dez especialistas na área de pesquisa, sendo estes pertencentes ao quadro funcional de diferentes órgãos de Segurança Pública no Brasil, e diferentes fabricantes de equipamentos para Comunicação Crítica, além de especialistas vinculados ao Ministério de Ciência, Tecnologia e Inovação (MCTIC).

Foi seguida a metodologia de Mwanza (2001) com as contribuições de Mello (2018), o que possibilitou a construção do questionário aplicado aos especialistas, além de diversas análises a partir dos dados obtidos, como por exemplo levantamento de cenários, necessidades dos usuários, dificuldades dos atuais sistemas, aspirações para uma rede ideal e comparações entre sistemas já adotados. Este artigo demonstrará os dados levantados com relação ao levantamento de possíveis cenários.

Para a realização das entrevistas, utilizou-se como base a análise da atividade a partir da Teoria da Atividade (TA), que constitui um modelo teórico-conceitual com sua unidade básica, a atividade, analisando as práticas humanas em níveis individuais e sociais.

Dentre os métodos que operacionalizam a aplicação da TA para contextos de Interação Humano-Computador (IHC), Mwanza (2001) propôs uma metodologia que guia o processo de coleta e interpretação de dados para levantamento de requisitos através da aplicação de estágios para levantamento de dados, sendo que a

coleta de dados através das entrevistas, denominada por Mwanza (2001) de estágio 1, tem a sugestão de aplicação de oito perguntas.

Os tópicos abordados nas questões foram: 1. Atividade de interesse; 2. Objeto ou objetivo da atividade; 3. Sujeitos da atividade; 4. Ferramentas de mediação da atividade; 5. Regras e regulações de mediação da atividade; 6. Divisão de trabalho de mediação da atividade; 7. Comunidade em que a atividade é conduzida; 8. Qual é o resultado desejado ao realizar esta atividade? (MWANZA, 2001). 9. Aspirações para resolução de problemas relacionados à atividade (MELLO, 2018); 10. Dificuldades para a realização da atividade; 11. Oportunidades para realização da atividade; 12. Governança para realização da atividade; 13. Nível de transferência e aproveitamento da tecnologia existente e identificação de dificuldades para implantação de tecnologias futuras, para a realização da atividade; 14. Aspirações para governança.

4 Identificação de cenários para comunicações críticas: O olhar informacional para as inovações tecnológicas

A partir da análise das entrevistas com especialistas, alguns possíveis cenários foram considerados para este estudo, citados e descritos a seguir. As descrições para cada cenário também foram realizadas a partir dos dados coletados.

1) Cenário 1 – Melhoria dos atuais sistemas em Land Mobile Radio (LMR), sendo estes: APCO 25, TETRA e TETRAPOL;

2) Cenário 2 – Implantação de sistema híbrido LMR e Long Term Evolution (LTE);

3) Cenário 3 – Implantação de uma rede única para os órgãos de Segurança Pública e defesa em LTE.

4.1 Cenário 1: Melhoria dos atuais sistemas em LMR

Trata-se de inovação tecnológica incremental, pois as melhorias apresentadas pelos sistemas são referentes às atualizações de versões de software e hardware, além

de manutenção da rede existente, oferecendo melhor desempenho do sistema, com provável menor quantidade de manutenções corretivas.

Contudo, este cenário não viabiliza o atendimento das aspirações por parte dos especialistas. Segundo estes, apesar de uma possível melhoria na eficiência do sistema, o usuário continuaria insatisfeito com as funcionalidades disponíveis atualmente.

Seria uma solução mais adequada, considerando fatores de imediatismo, não englobando todo o contexto necessário para uma decisão abrangente, contudo, reduzindo o impacto de um problema atual, relacionado à falta de manutenção e atualização adequadas.

Quanto às necessidades para implantação, os sistemas já estão implantados nos órgãos. Dessa forma, as ações de melhoria não precisam de adoção de novas políticas públicas, processos ou sistemas, necessitando apenas de contrato de manutenção com os fabricantes para fornecimento de peças e serviços necessários, assim como planejamento de expansão da cobertura para locais que atualmente possuem falhas.

4.2 Cenário 2: Sistema híbrido LTE e LMR

Trata-se de inovação tecnológica incremental, pois as melhorias apresentadas pelos sistemas seriam referentes às atualizações de versões de software e hardware, oferecendo melhor desempenho do sistema, com provável menor quantidade de manutenções corretivas, além da inserção de novas funcionalidades viabilizadas através da junção do LTE aos sistemas LMR.

Quanto às necessidades para implantação, este cenário considera os órgãos de segurança utilizando as atuais redes LMR atualizadas e disponíveis, com a viabilidade de integração com o LTE através de plataforma que realize integração entre o atual sistema LMR e a rede LTE comercial das operadoras de telefonia celular.

Dessa forma, os usuários poderiam utilizar smartphones com voz integrada ao atual sistema LMR, possibilitando integração de grupos de comunicação e apli-

cações especificas para Segurança Pública através de aplicativo.

Há, entre os smartphones com licença para uso do aplicativo LTE, viabilidade de envio e recebimento de dados, imagens e vídeos em tempo real, além de aplicações especificas para Segurança Pública, utilizando a rede das operadoras de telefonia celular.

Os sistemas em LMR já estão implantados nos órgãos. Dessa forma, a ação de melhoria na rede LMR não precisaria de implantação de novas políticas públicas, processos ou sisadro 2temas, necessitando apenas de contrato de manutenção com os fabricantes para fornecimento de peças, serviços e atualização das redes.

A diferença para com o Cenário 1 deve-se à necessidade de aplicação de processos específicos que viabilizem a operação da rede híbrida, processos estes que podem ser adotados de outros países que já estão em fase adiantada de implantação da rede híbrida, bem como a criação de um modelo de governança específico para o Brasil.

O México é um exemplo de país que está em fase de implantação da rede TETRAPOL – LTE, com a utilização da rede de banda larga através de operadoras, denominada "Red Compartida".

Essa é uma solução mista, atendendo em parte o imediatismo do Cenário 1 e em parte as necessidades mapeadas, atendidas totalmente pelo Cenário 3.

4.3 Cenário 3: Implantação de uma rede única LTE

Trata-se de inovação de ruptura. As ações desejadas são atendidas pela nova tecnologia, bem como pela aplicação de processos específicos que viabilizem a implantação da rede única.

Este cenário possibilita uma solução ampla, englobando todas as necessidades mapeadas. De acordo com Freire, Jorge & Cândido (2019), tal rede poderia ser capaz de disponibilizar mais informações para os agentes que estão em campo através de:

- Consultas a banco de dados;
- Transmissão de imagens em tempo real com alta resolução;

- Uso de tablets e smartphones com sistemas embarcados;
- Pesquisas em base de dados de indivíduos, veículos, mandados de prisão e qualquer outro sistema que agilize a atuação policial;
- Reconhecimento de placas veiculares através de câmeras, com envio da leitura dessas placas para a base de dados da polícia para verificação;
- Integração de drones;
- Utilização de video inteligence;
- Utilização de aplicações através de multimídia IP, personalizada para usuários e capazes de prover agilidade e eficiência na atuação policial.

Quanto às necessidades para implantação, os processos que viabilizam a adoção da tecnologia podem ser baseados em processos já utilizados em outros países que estão em fase adiantada de implantação da rede única LTE, bem como através da criação de um modelo de governança específico para o Brasil.

Os Estados Unidos (EUA) e o Reino Unido podem ser utilizados como referência de processos para adoção devido ao grau de adiantamento da implantação da rede, além de, segundo a 3GPP (2018), esses projetos estarem sempre apresentando contribuições que auxiliam na padronização do LTE para Comunicação Crítica.

Para o caso de criação de uma rede única LTE, algumas questões precisam ser consideradas, como por exemplo:

- Suportar o número de acessos simultâneos das várias agências, com planejamento de tráfego adequado.
- A taxa mínima de dados deve ser capaz de transmitir pacotes em banda larga, visando suportar aplicações em segurança pública para combate ao crime. Essas soluções devem ser atuais e atualizáveis, já que os criminosos também utilizam recursos tecnológicos atuais para cometer crimes.
- A eficiência das comunicações em situações de movimento também é um requisito relevante.

• A latência nas comunicações em LTE deve ser tão baixa quanto a obtida pelas atuais redes LMR, uma vez que o tempo é um recurso crítico nas operações em Segurança Pública.

• Segurança nas comunicações, com uso de criptografia fim a fim e através de dispositivos seguros. Também é interessante que se possa estabelecer diferentes níveis de segurança em função da aplicação utilizada e do agente que está utilizando o terminal.

• Existência de uma central de atendimentos disponível durante 24h, os sete dias da semana, dedicada à rede. O atendimento, identificação e resolução dos problemas técnicos deve ser rápido o suficiente para não prejudicar o andamento das operações policiais.

• Definição de requisitos para dispositivos de usuário, que devem possuir requisitos mínimos de duração de bateria, facilidade de uso e aplicativos.

• Além dos smartphones disponíveis no mercado, são necessários diferentes modelos de aparelhos e acessórios, possibilitando a utilização do equipamento em diversas situações, desde equipamento a prova d'água, para uso pela polícia marítima; equipamentos robustos, para uso pelos grupos táticos; e equipamentos velados, para utilização em locais públicos que necessitem discrição na atuação policial. Também são necessários acessórios auriculares de diferentes modelos e com diferentes tipos de acionamento do Push to Talk (PTT).

5 Limitações atuais no Brasil para comunicações críticas na visão dos especialistas entrevistados

Atualmente, com relação à integração das redes, um dos grandes problemas para utilização de um mesmo sistema entre os diferentes órgãos é a falta de conhecimento em sistemas de Comunicação Crítica. Esse tipo de sistema permite que se tenha controle da rede e separação dos órgãos, inclusive separação da gerência da

rede, com criação de redes separadas e integração, caso necessário, em grupos de comunicação previamente designados para isso.

Atualmente, existem no Brasil mais de 30 redes de Comunicação Crítica, cada órgão com sua própria rede e sistemas distintos, com coberturas por vezes até na mesma região, mas sem integração e interoperabilidade.

Portanto, não é possível fazer a interoperabilidade de forma eficiente, pois cada órgão compra sistemas diferentes e a forma de se fazer interoperabilidade é através do uso de gateways, que integram apenas voz.

Quando cada órgão compra uma tecnologia diferente, posteriormente, para que os órgãos se falem em um grupo integrado, como necessário em uma situação de crise, por exemplo, precisa-se comprar mais equipamentos, deixando os sistemas ainda mais complexos.

Aparentemente, o melhor caminho seria, desde a concepção do projeto, ainda na fase de planejamento, pensar no investimento em uma mesma tecnologia, de preferência com o maior número possível de fabricantes, para viabilizar a economicidade para aquisição.

Essa falta de padronização e interoperabilidade implica em dificuldades para uma atuação integrada entre as forças. Atualmente, caso o país tenha uma situação crítica, grande parte dessas redes não possui interoperabilidade, como também protocolos de ações para a comunicação entre órgãos são ausentes.

Ou seja, em uma situação de crise, os órgãos de segurança teriam dificuldades para se comunicar entre si; situação similar ao que ocorreu durante o atentado de 11 de setembro nos EUA, em que houveram problemas de comunicação entre órgãos, o que ocasionou na demora para tomada de decisões e execução de ações.

Como exemplo de falta de padronização, hoje, no Brasil, tem-se: exército utilizando APCO 25, na faixa de 800Mhz; a Polícia Militar (PM) de Minas Gerais, utilizando APCO 25, na faixa de 170Mhz; em São Paulo, a PM utiliza o APCO 25, na faixa de 800Mhz; a Polícia Federal (PF) utiliza o sistema TETRAPOL, na faixa de 450Mhz; a Polícia Rodoviária Federal (PRF) utiliza o sistema TETRA, na faixa

de 380Mhz.

Tomando como exemplo apenas o Governo Federal, as três principais agências de segurança pública e defesa, PF, PRF e Exército, utilizam redes LMR, com as tecnologias, respectivamente, TETRAPOL, TETRA e APCO 25, tendo cada um desses órgãos já investido cerca de 300 milhões de reais para a implantação de três redes distintas com a mesma finalidade, comunicação crítica, e com coberturas coincidentes em diversas localidades, totalizando algo em torno de 900 milhões de reais em três redes sem interligação ou interoperabilidade entre elas.

Portanto, no cenário atual, é muito difícil ter interoperabilidade. A solução mais simples seria criar centros integrados de comando e controle (CICCR), onde os órgãos teriam cadeiras. Em Belo Horizonte, por exemplo, existem 42 agências no CICCR, incluindo companhia de energia, polícia, entre outros. Grande parte dessas agências possui seu próprio sistema de rádio, com interlocutores atuando como operadores.

Dessa forma, as agências não se comunicam diretamente, mas através de um interlocutor. Essa é a interoperabilidade mais viável atualmente no Brasil, diante de tantas redes distintas. O operador da rede de rádio do órgão solicita algum dado ou informação, ou até mesmo a transmissão de uma comunicação, para o operador de rádio dos outros órgãos.

Tecnicamente, é viável a integração apenas de voz, porém é complicado fazer a integração de vários sistemas distintos dessa forma.

Para o Cenário 2, além do problema de falta de interoperabilidade a ser enfrentado, devem ser avaliadas questões referentes à proteção dos dados em virtude da utilização de redes públicas de telefonia celular e à verificação da disponibilidade de utilização de aplicativo com criptografia robusta acima da criptografia das operadoras de telefonia. Na rede LMR, a criptografia já é inerente ao sistema de comunicação crítica.

O Cenário 2 viabiliza, em parte, o atendimento das aspirações, pois apenas a funcionalidade de voz estaria integrada aos atuais sistemas LMR. A rede LTE uti-

lizada seria a das operadoras de telefonia celular, sem prioridade para os usuários advindos dos órgãos de Segurança Pública, portanto enfrentando possíveis problemas de congestionamento de tráfego em situações críticas, onde as comunicações dessas forças devem funcionar de qualquer forma.

6 Proposição de soluções para comunicações críticas na visão dos especialistas entrevistados

Com relação à integração, para que esta ocorra, o primeiro passo é existir nos órgãos a vontade de utilizar a mesma infraestrutura, não precisando utilizar o mesmo sistema, bastaria um compartilhamento de infraestrutura, através de um investimento único, como por exemplo a mesma torre para todos os órgãos.

Com relação à opção de utilização de uma única rede, os recursos financeiros são destinados para o mesmo sistema, tornando mais barato ampliar a rede. Sistemas diferentes para diferentes forças implicam em desperdício de recursos.

No Brasil, não existe padronização de uso para sistemas de Comunicação Crítica. Inclusive dentro do mesmo Estado existem polícias estaduais (civil e militar) utilizando sistemas distintos, como ocorre, por exemplo, no estado de Minas Gerais. Ou seja, há falta de planejamento e diretrizes de investimentos nessa área por parte dos órgãos centrais.

No Brasil também falta um órgão que seja responsável pela gestão de um sistema unificado de Comunicações Críticas. Em vários países europeus foi definido previamente pelo governo federal qual sistema LMR seria utilizado, de forma que o país inteiro utilize a mesma rede, tendo prevalência pelo sistema TETRA.

Com relação ao Cenário 2, como proposição de redução da vulnerabilidade em virtude de possível indisponibilidade do sistema de telefonia celular em situações de alto tráfego, os especialistas sugerem a adoção de políticas públicas que priorizem o uso dos equipamentos advindos das forças de segurança com relação aos demais usuários da rede LTE.

Com relação ao Cenário 3, segundo os especialistas, um modelo ideal seria parecido com a rede dos EUA, através da Firstnet, onde criou-se uma rede LTE para segurança pública e o governo federal demonstrou para as agências os benefícios de aderir a esta rede, como por exemplo ter acesso a informações de outras agências quando necessário.

A rede única LTE, por ser uma plataforma IP, é uma ferramenta de integração para distintas tecnologias, não apenas sistemas de voz, mas sistemas de vídeo monitoramento e sistemas de dados.

Essa rede única deve possuir uma gerência central, responsável pela manutenção e gestão de forma macro, e de preferência que não seja um órgão de Segurança Pública e sim um órgão em que sua expertise seja comunicação e tecnologia. A despeito de uma gerência central, todos os órgãos públicos teriam participação na gestão da rede, com poderes e responsabilidades sobre sua gestão, manutenção, operação e planejamento da expansão e atualização.

Com isso, criar-se-ia uma plataforma comum com possibilidade de integração de comunicação entre os órgãos, em caso de necessidade e em situações previamente definidas, através de protocolos de atuação. As frequências poderiam ser designadas para um órgão federal e este faria o gerenciamento da rede, entrando em contato com todos os órgãos dos estados e municípios que necessitem de Comunicação Crítica, mostrando o benefício da rede e oferecendo permissão para que o órgão faça adesão diante de alguns critérios e contrapartidas. A adesão a essa rede única seria facultativa.

Algum órgão ligado ao MCTIC, como por exemplo a TELEBRÁS, poderia ser o órgão gestor, tendo o direito de uso da frequência e propriedade dos ativos, e sendo subsidiada por recursos vindos de fundos, como por exemplo o Sistema Único de Segurança Pública (SUSP), com um percentual de cada telefone celular vendido no país, viabilizando, dessa forma, a implantação do sistema.

Para terem acesso ao sistema, os estados e municípios teriam que disponibilizar locais para a instalação das Estações Rádio Base (ERBs). Portanto, a TELEBRÁS,

nosso exemplo, realizaria a instalação, gerência e manutenção da rede. O estado ou município, em contrapartida, forneceria o espaço físico da torre, ficando também a cargo da compra dos rádios ou smartphones compatíveis com a rede. Esse seria um exemplo viável para se aplicar o conceito da rede única.

O órgão gestor poderia terceirizar a manutenção da rede; contudo, cada órgão teria gerência sobre sua rede, com, por exemplo: criação de grupos de comunicação; habilitação de usuários com funcionalidades e prioridades determinadas pelo operador da rede; fusão de grupos; controle sobre o compartilhamento de voz, dados e vídeo; planejamento técnico operacional para operações policiais e grandes eventos, entre outros.

Portanto, o órgão de segurança necessita de corpo técnico para a gerência técnica da rede; controle; configuração; manutenção dos terminais; entre outras funções.

O corpo técnico do órgão também deve ser responsável por gerenciar, configurar, operar e instalar a rede tática em situações de operações em locais sem cobertura da rede única, ou até mesmo situações táticas e operacionais, como por exemplo em alto mar, floresta, caatinga, túneis, locais internos de edifícios, equipes em deslocamento com equipamento tático instalado dentro da viatura, dentre outros. Situações como essas exigem especificidades técnicas e operacionais inerentes ao corpo técnico do órgão de Segurança Pública.

Deve existir também um conselho para a rede única, formado por representantes dos órgãos. Uma sugestão dada pelos especialistas seria: um representante de cada Estado da SDS responderia pelos órgãos que utilizam a rede única de Comunicação Crítica daquele Estado, e os órgãos federais teriam seus próprios representantes.

Portanto seriam então: um representante para a PF, um para a PRF, um para a marinha, um para o exército e um para a aeronáutica. Dentro dos estados existiria também um conselho que elegeria o representante da SDS, que responderia no conselho nacional sobre os órgãos daquele Estado com relação à rede única

de Comunicação Crítica. No final das contas, o conselho nacional seria formado por 32 representantes, sendo estes um por Estado e cinco dos órgãos federais de segurança e defesa.

A partir do momento que algum órgão aderisse à rede, este passaria a ter direito a um representante no conselho nacional, que teria reuniões algumas vezes por ano, com pautas abordando aspectos da rede.

A rede seria apenas para Segurança Pública e, a partir disso, criar-se-ia diretrizes, como por exemplo: todo aeroporto terá que compartilhar as imagens das câmeras com o SUSP; todo concessionário de serviço público que possua videomonitoramento deverá disponibilizar este recurso para SUSP, etc.

6.1 Vantagens e desvantagens para a implantação de uma rede única LTE

A implantação do LTE é uma oportunidade, para os órgãos, de ter uma única rede com grande capacidade de transmissão de dados, sendo que, quanto maior a quantidade de órgãos participando da rede, melhor será para compensar os investimentos iniciais.

Os recursos físicos da rede podem ser compartilhados e mesmo assim haver separação de organizações, com comunicação e gerência de grupos e terminais controlados pelos órgãos. Ou seja, um órgão não teria acesso à rede de outro órgão e, em situações previamente definidas, poderia haver troca de dados, informações e até mesmo comunicações em um mesmo grupo.

Uma importante questão a considerar é a economia de escala proporcionada pela utilização de ERB, sistemas irradiantes e terminais, similares aos utilizados pelas operadoras de telefonia celular, além da facilidade em desenvolver aplicativos para plataforma Android e iOS que atendam uma demanda específica de determinada delegacia ou grupo operacional.

Essa rede em banda larga pode prover integração de inteligência artificial ao sistema, possibilitando análise de vídeos com reconhecimento facial e de placas de veículos integrados à base de dados, identificando, por exemplo, pessoas procuradas

e veículos roubados, entre outras aplicações.

Poderá haver também visualização de imagens de câmeras conectadas ao sistema através de rádio e/ou smartphone, como por exemplo uma câmera instalada no aeroporto, ou até mesmo no uniforme do agente, provendo transparência na atuação policial e maior segurança para o próprio agente.

Além da possibilidade de utilização de rádios com smartphones integrados, adaptados para os diversos cenários de utilização em Comunicação Crítica, haveria, desde equipamentos à prova d'água, até smartphones com botão de acionamento do PTT de fácil acesso, além dos já disponíveis no mercado.

A possibilidade de trafegar dados, voz e vídeo numa única base de dados em banda larga viabiliza também que as agências compartilhem informações em uma única base de dados de Segurança Pública, ou pelo menos uma base de dados integrada, compartilhada através de uma rede protegida.

Outros exemplos de aplicação em banda larga são: gerenciamento de sistemas inteligentes via rádio, como por exemplo controle de semáforos e movimentação do posicionamento de câmeras; possibilidade de monitoramento de localidades através da comunicação crítica; por exemplo, as câmeras detectariam uma situação de perigo e, através do processamento da informação, o próprio sistema dispara um alerta para o policial mais próximo ao local.

Aumentar-se-ia a disponibilidade de banda para fazer controles à distância de máquinas que utilizem inteligência artificial, em situações onde o volume de informações para ser processado é muito grande, com interoperabilidade de sistemas e elementos da cidade. Isso implica a modernização da atuação da segurança pública para o cenário de Smart City, com interoperabilidade aos diversos meios, como por exemplo energia e trânsito.

Contudo, a possibilidade de interação entre equipamentos através da inteligência artificial deve levar em consideração a questão ética, como por exemplo através de câmeras apenas em locais públicos.

Há, porém, limitações. A identificação de criminosos e suspeitos poderá ser

feita apenas entre os que estiverem em uma base de dados prévia de procurados; a investigação seria preditiva, apenas situacional, identificando, por exemplo, alguém que pula a cerca de um local onde é proibido fazer isso, um carro que trafega em alta velocidade na contramão, entre outras situações.

Ou seja, a inteligência artificial não realizaria a Tomada de Decisão sobre um possível criminoso, apenas identificaria criminosos pelo reconhecimento facial através de uma base de procurados, e os parâmetros de situações que possam representar riscos seriam definidos previamente pelos programadores, de forma ética e isenta, a Tomada de Decisão devendo sempre ser de um ser-humano.

Com relação à governança, no Brasil, faltam leis e regulamentos que especifiquem para que órgão será atribuída a frequência designada para o LTE em Comunicação Crítica e como serão a regras de utilização. Por exemplo, quem será o gestor da rede; como será a manutenção; como os órgãos de segurança poderão aderir à rede; como será a operação, entre outros.

Atualmente, no entanto, diversos países estão em fase de implantação da rede LTE para Comunicação Crítica, seja através de dedicada em LTE ou por meio da rede híbrida. Dessa forma, como estratégia para resolução da falta de políticas públicas, pode-se adotar processos já existentes em países de referência, como também aproveitar parte dos modelos adotados por outros países e desenvolver algo específico para o Brasil.

7 Considerações Finais

A partir dos possíveis cenários para utilização em Comunicação Crítica no Brasil abordados neste estudo, pretende-se auxiliar a realização de um exercício de AT de forma ampla, considerando as funcionalidades já oferecidas pelas redes atuais, como também pelas redes que surgem como tendências para o futuro.

Além disso, a partir do levantamento de dados das aspirações por parte dos especialistas, consegue-se confrontar informações entre o cenário desejado e os ce-

nários possíveis, auxiliando, dessa forma, a busca de uma tecnologia que se adeque às necessidades atuais dos órgãos de Segurança Pública.

Os especialistas também apontaram dificuldades atuais e possibilidades de aplicação de modelos que minimizem esses problemas, contribuindo, dessa maneira, para ampliar as discussões com relação à governança no Brasil para esses sistemas.

Referências:

3GPP. 3GPP Global Initiative LTE. The mobile broadband standard. Disponível em: http://www.3gpp.org/technologies/keywords-acronyms/98-lte. Acesso em 25 mar. 2020.

Borko, H. Information science: what is it?. American Documentation, v. 19, n. 1, p. 3– 5, 1968.

BUCKLAND, M. K. Information as thing. Journal of the American Society for Information Science, v. 42, n. 5, p. 351 – 360, jun. 1991.

DAMANPOUR, F. Organizational Innovation. Oxford Research Encyclopedia of Business and Management. Disponível em: http://negocios.udd.cl/files/2017/10/Fariborz-Damanpour-2017-Organizational-Innovation.pdf. Acesso em: 25 mar. 2020.

FREIRE, Débora Vanessa Campos; CÂNDIDO, Ana Clara. Avaliação Tecnológica em Comunicações Críticas: análise para decisão. In: XIX Encontro Nacional de Pesquisa em Ciência da Informação – ENANCIB, 2018, Londrina. Anais. Londrina: ANCIB (Ed.), 2018. p. 5388 - 5396.

FREIRE, Débora Vanessa Campos; JORGE, Juliana Müller Reis; CÂNDIDO, Ana Clara. Avaliação tecnológica para comunicações críticas: contexto social. In: PINTO, Adilson Luiz (org.). Aproximação entre a Ciência da Informação com a Ciência Policial. Florianópolis, SC: Senac SC, 2019. p. 105 – 133. ISBN – 978-85-67932-08-8.

GSMA. Network 2020. Mission Critical Communications. Disponível em: https://www.gsma.com/future-networks/wp-content/uploads/2017/02/767-Mission-critical-communications-low-res.pdf. Acesso em 25 mar. 2020.

MELLO, A. C. B. de. (2018). Levantamento de requisitos por meio da análise da atividade e da tarefa para sistemas digitais. Dissertação (Mestrado em Design) – Curso de Pós-Graduação em Design, Universidade Federal de Pernambuco, Recife, 2018.

Merkerk, R. O. V.; smits, R. Tailoring. CTA for emerging technologies. Technological Forecasting and Social Change, v. 75, n. 3, p. 312 – 333. Março 2008.

Mwanza, D. Where Theory meets Practice: A Case for an Activity Theory based Methodology to guide Computer System Design. In: Eighth ifip tc 13 international conference on human-computer interaction, 2001, Tokyo, Japan. Proceedings of INTERACT'2001. Tokyo, Japan: HIROSE, M. (Ed.). Oxford, UK: IOS Press, 2001.

SARACEVIC, T. Ciência da informação: origem, evolução e relações. Perspec. Ci. Inf., Belo Horizonte, v. 1, n. 1, p. 41 – 62, jan./jun. 1996.
WERSIG, G.; NEVELING, U. The phenomena of interest to information science. Information Scientist, v. 9, p. 127 – 140, 1975.