



UEPB

**UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS CAMPINA GRANDE**

**Coordenação da Pós-Graduação do Curso de Especialização em Inteligência Policial e
Análise Criminal**

PAULO SÉRGIO LOPES ANGELIM

**CONTRAINTELIGÊNCIA DE SEGURANÇA PÚBLICA: TÉCNICAS DE FALSA
INFORMAÇÃO, DESINFORMAÇÃO E DECEPÇÃO**

JOÃO PESSOA - PB

2017

PAULO SÉRGIO LOPES ANGELIM

CONTRAINTELIGÊNCIA DE SEGURANÇA PÚBLICA: TÉCNICAS DE FALSA
INFORMAÇÃO, DESINFORMAÇÃO E DECEPÇÃO

Trabalho de conclusão de curso apresentado à
Coordenação do Curso de Especialização em
Inteligência Policial e Análise Criminal como
requisito parcial para conclusão do Curso de
Especialização em Inteligência Policial e
Análise Criminal.

Orientador: Vinícius Lúcio de Andrade

JOÃO PESSOA - PB

2017

É expressamente proibida a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano da dissertação.

A582c Angelim, Paulo Sérgio Lopes
Contrainteligência de segurança pública [manuscrito] :
técnicas de falsa informação, desinformação e decepção / Paulo
Sérgio Lopes Angelim. - 2016.
39 p.

Digitado.

Monografia (Especialização em Inteligência Policial e Análise
Criminal) - Universidade Estadual da Paraíba, Centro de Ciências
Jurídicas, 2016.

"Orientação: Prof. Me. Vinícius Lúcio de Andrade,
Departamento de Ciências Jurídicas".

1. Contrainteligência. 2. Técnicas de falsa informação. 3.
Desinformação. 4. Decepção. I. Título.

21. ed. CDD 323.44

PAULO SÉRGIO LOPES ANGELIM

**CONTRA INTELIGÊNCIA DE SEGURANÇA PÚBLICA: TÉCNICAS DE FALSA
INFORMAÇÃO, DESINFORMAÇÃO E DECEPÇÃO**

Trabalho de conclusão de Curso apresentado ao Programa de Pós-Graduação em Inteligência Policial e Análise Criminal da Universidade Estadual da Paraíba, como requisito para à obtenção do título de especialista.

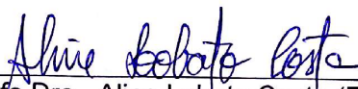
Área de Concentração: _____

Aprovado em: 27 / 01 / 2017

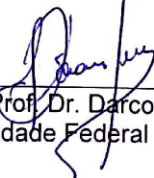
BANCA EXAMINADORA



Prof. Ms Vinícius Lúcio de Andrade (Orientador)
Faculdade de Ciências Sociais Aplicadas (FACISA)



Prof.ª Dra. Aline Lobato Costa (Examinadora)
Universidade Estadual da Paraíba (UEPB)



Prof. Dr. Darcon Sousa (Examinador)
Universidade Federal de Campina Grande (UFCG)

À minha mãe(in memóriam), à minha esposa e
aos meus
filhos. As minhas maiores fontes de
estímulo, determinação e amor.
Dedico.

AGRADECIMENTOS

Ao Grande Arquiteto do Universo, pelo dom da vida.

À minha família, especialmente minha mãe, Maria José Angelim, por sua abnegação em educar os filhos.

À minha esposa, Rita Braz do Nascimento Angelim, por entender a minha ausência.

Aos meus filhos, fontes de inspiração para uma vida melhor.

Aos meus professores do curso, pela atenção dispensada.

Aos vários amigos que fiz durante o curso.

“Previsão era a razão pela qual o príncipe esclarecido
e o general prudente venciam o inimigo,
quaisquer que fossem os seus movimentos.”

(SunTzu)

RESUMO

A violência urbana é, no campo da Segurança Pública, um dos desafios mais difíceis de ser combatido. O tráfico de drogas, os crimes patrimoniais, a lavagem de dinheiro e o crime organizado são exemplos de ameaças que circundam as Instituições de Segurança Pública. O crime organizado se infiltra e corrompe os servidores públicos destas instituições, que se desviam de suas funções, quando deveriam combatê-las. A adoção dos sistemas de informações integrados cria novas possibilidades de ferramentas para fazer frente ao assédio desse tipo de atuação criminosa, e garantindo o funcionamento das agências de informação dos órgãos de segurança pública. É nessa atmosfera que se insere este trabalho que discutirá Contrainteligência de Segurança Pública e trará à baila conceitos como: Técnicas de Falsa Informação, Desinformação e Decepção. Para apoiar nossa discussão, autores como Braga (2005), Gleghorn (2003) entre outros, prestarão o suporte teórico.

Palavras-chave: Contrainteligência. Técnicas de Falsa Informação. Desinformação. Decepção.

ABSTRACT

Urban violence is, in the field of Public Security, one of the most difficult challenges to be tackled. Drug trafficking, property crimes, money laundering and organized crime are all examples of threats that surround the Public Security Institutions. Organized crime infiltrates and corrupts the public servants of these institutions, who deviate from their functions when they should fight them. The adoption of integrated information systems creates new possibilities for tools to deal with harassment of this type of criminal activity, and ensures the functioning of information agencies of public security agencies. It is in this atmosphere that this work is inserted that will discuss Public Security Counterintelligence and bring to light concepts like: False Information Techniques, Disinformation and Deception. To support our discussion, authors such as Braga (2005), Gleghorn (2003) among others, will provide theoretical support.

Keywords: Counterintelligence. Techniques of False Information. Disinformation. Disappointment.

SUMÁRIO

1. INTRODUÇÃO	11
2. INTELIGÊNCIA DE SEGURANÇA PÚBLICA	14
2.1 A Inteligência de Segurança Pública:	14
2.2 Por sua vez a Inteligência Policial:	14
2.3 Contrainteligência:	15
3. INTELIGÊNCIA POLICIAL	17
4. ATIVIDADE DE CONTRAINTELIGÊNCIA	18
4.1 SEGURANÇA EM OPERAÇÕES NA CONTRAINTELIGÊNCIA	20
4.2 Técnica de Contrainteligência	21
4.3 Falsa Informação	21
4.4 Desinformação	22
4.5 Decepção	25
5. RESOLUÇÃO Nº 1, DE 15 DE JULHO DE 2009	26
6. COMENTÁRIOS	39
7. CONSIDERAÇÕES FINAIS	41
8. REFERÊNCIAS BIBLIOGRÁFICAS	42

1. INTRODUÇÃO

A violência urbana é, no campo da Segurança Pública, um dos desafios mais difíceis de ser combatido. O tráfico de drogas, os crimes patrimoniais, a lavagem de dinheiro e o crime organizado são exemplos de ameaças que rodeiam as instituições de Segurança Pública. O crime organizado se infiltra e corrompe os servidores públicos destas instituições, que se desviam de suas funções, quando deveriam combatê-las.

A adoção dos sistemas de informações integrados cria novas possibilidades de ferramentas para fazer frente ao assédio desse tipo de atuação criminosa, e garantindo o funcionamento das agências de informação dos órgãos de segurança pública. Ainda no tocante ao crime organizado, podemos observar a existência de organizações ou empresas que se estabelecem com aparência de legalidade, apresentando preparo e destreza que em muito dos casos se infiltram nas instituições de Segurança Pública, inclusive, patrocinando a aprovação de pessoas comprometidas com o crime organizado, em concurso público para ingressarem nas instituições, e dessa forma atingirem seus objetivos e interesses escusos. Desses, o exemplo mais evidente, quando nos referimos ao crime organizado, é o tráfico de drogas, todavia, atividades como o contrabando, o jogo ilegal e roubos em larga escala são todas atividades criminosas que requerem preparação e cooperação das pessoas envolvidas para que possam lograr êxito.

Essa estratégia não é nova, a famosa família da máfia italiana que atuaram entre 1930 e 1960 era formada por famílias de imigrantes italianos, vinham para Estados Unidos da América, se juntavam com a ideia de grupo “família”. A mais famosa denomina-se “cosa nostra”, que ainda existe no mundo criminoso dos Estados Unidos.

No caso de nossa realidade, é fato o grande número de pessoas cooptadas com a finalidade de obstruir ações de Segurança pública no combate à criminalidade.

A violência é a forma utilizada pelo crime organizado para manutenção de sua existência. O apoio de órgãos institucionais, seja pela omissão ou pela corrupção, também é um fator determinante.

Dentre os problemas sociais mais graves dos dias atuais, destaca-se a insegurança associada à violência, à ocorrência de roubos e furtos, o tráfico de drogas, os homicídios e a criminalidade, que têm vitimado pessoas e organizações, que passaram a procurar meios de protegerem-se sem esperar pela ação do Estado. Para Costa (1997), a perda da eficiência e a diminuição das funções dos governos originaram a busca por proteção particular por parte de

empresas e cidadãos, o que fomentou o desenvolvimento de sistemas de segurança que, em muitos casos, atuam à margem da lei. O uso da violência tornou-se um recurso decorrente de uma sociedade que alimenta o individualismo e a ambição, recrudescendo a agressividade.

A criminalidade organizada representa uma força significativa, principalmente pela instabilidade que proporciona na segurança pública. Há algumas décadas, quando os valores sociais ainda eram rigorosamente definidos e controlados, tornava-se mais fácil prever as reações e posicionamento das pessoas nas mais variadas situações, sendo possível o controle da criminalidade. Diferente do que ocorre atualmente.

As políticas públicas de segurança falham. A lei tem mostrado pouco ou nenhum efeito, e a polícia desaparelhada e com baixos salários torna-se ineficaz no combate à criminalidade. A reformulação da Segurança Pública no País tem que ser imediata. A mudança deve começar pela maneira como a violência é encarada pelas autoridades, que não observam as particularidades de cada lugarejo. Planos gerais de segurança devem ser apenas norteadores e não reguladores da atividade, figurando o modelo descentralizado, o melhor a ser adotado nessa situação.

Já existe uma literatura extensa e diversificada que estuda sobre o tema da violência, as causas, as consequências, as formas de extirpá-la da sociedade ou meios de controle mais eficazes. É consenso mundial o pensamento de que as desigualdades sociais potencializam a violência, porém tanto nas nações socialmente desenvolvidas, assim como nas nações em desenvolvimento, onde as desigualdades são gritantes, encontram-se crimes, atentados, e todo tipo de violência. Da mesma forma que os aspectos econômicos, políticos e tecnológicos são importantes, as instituições de Segurança Pública deve também estar atenta aos processos e mudanças sociais, analisando os valores, crenças e comportamentos de uma sociedade. Mudanças no ambiente social podem apresentar grandes desafios às instituições públicas, principalmente em um mundo globalizado como o de hoje.

A análise de um único fator de ameaça pode levar o gestor de Segurança Pública a tomar decisões equivocadas, mas considerar todo o conjunto de fatores que pode influenciar o ambiente social minimiza o efeito da criminalidade no local. Por exemplo: não é suficiente saber apenas quantas pessoas se mudaram do centro para um bairro da periferia num determinado ano, você terá uma visão muito maior se identificar e atender necessidades básicas se souber quantas destas pessoas são aposentadas, quantas são solteiras, com ou sem filhos, ou se estas possuem situação financeira estável o suficiente para comprar os serviços disponíveis no local ou em outra localidade, ou se vão ficar à margem do mercado consumidor fomentando a violência.

Qual seria então a importância da contrainteligência na produção de informações para assessoramento dos gestores públicos, especialmente dos órgãos policiais, para esse enfrentamento?

A Contrainteligência tem como atribuições a produção de conhecimentos e a realização de ações voltadas para a proteção de dados, conhecimentos, infraestruturas críticas – comunicações, transportes, tecnologias de informação – e outros ativos sensíveis e sigilosos de interesse do Estado e da sociedade.

Sendo a Contrainteligência o ramo da atividade de Inteligência que se destina a proteger a própria atividade de Inteligência e a instituição ou órgão a que pertence, de modo a salvaguardar seus dados e conhecimentos sigilosos, e identificar e neutralizar ações adversas realizadas por organismos ou por pessoas, esta se programa através da adoção de ações, normas, medidas e procedimentos voltados para estes fins, denominados Política de Segurança Institucional.

A atividade de Contrainteligência de Segurança Pública deve trabalhar para a salvaguarda de conhecimentos decisórios, do planejamento e da execução de políticas de Segurança Pública e das ações. A Inteligência de Segurança Pública, doravante ISP, compreende a produção de conhecimentos, dados e a proteção destes, cabendo ao Estado preservar as informações que lhe seja de seu interesse.

Para o correto exercício da atividade de inteligência é imperativo o uso de metodologias e de técnicas voltadas para a produção do conhecimento que permitam afastar a prática de ações meramente intuitivas e procedimentos sem orientação racional. A atividade de Inteligência de Segurança Pública é um exercício permanente e sistemático de ações especializadas em nível estratégico, direcionadas para obtenção de dados e a avaliação de situações externas que impliquem ameaças, veladas ou dissimuladas, capazes de dificultar ou impedir a consecução dos interesses estratégicos da Organização; Identificação, avaliação e neutralização da espionagem promovida por serviços de Inteligência ou outros organismos, vinculados ou não a governos; Proteção dos conhecimentos científicos e tecnológicos que, no interesse da segurança da Organização e do Estado, sejam considerados sigilosos e, conhecimentos necessários para prevenir e reprimir atos delituosos de qualquer natureza ou relativos a outros temas de interesse da Segurança Pública e da Defesa Social.

A produção e a proteção de conhecimentos é o cerne da atividade de ISP, principalmente no que tange à tomada de decisões ou apoio às Instituições de Segurança Pública. O acesso indevido a registros de informações sensíveis – aquelas que, pela importância e necessidade de proteção, exigem medidas especiais de segurança – sempre

foram grande fonte de atenção das Instituições de Segurança Pública, tendo sido suas técnicas de obtenção, por um lado, e neutralização, por outro, compiladas, organizadas e transformadas, respectivamente, nas atividades de medidas e contramedidas. É notório que uma medida preventiva adequada pode neutralizar o ato de infração antes que ele venha a ocorrer.

Os conceitos e métodos de medidas e contramedidas vêm sendo utilizados por diversas instituições de segurança pública, visando a proteger contra o crime organizado que de alguma forma busca o vazamento ou fuga de informações em defesa de seus interesses, seja tangível, físico, eletrônico ou composto por valores intangíveis tais como o capital intelectual ou a credibilidade junto à opinião pública, por exemplo.

2. INTELIGÊNCIA DE SEGURANÇA PÚBLICA

2.1 Inteligência de Segurança Pública: é formada por um conjunto de órgãos, interagindo de forma transversal, estruturada nos moldes do Estado Democrático de Direito, organizada administrativamente na forma centralizada, com processos bem definidos e únicos, com ampla capacidade de agregar conhecimentos das mais diversas fontes, garantindo a proteção do que for produzido e tem por finalidade executar a atividade de inteligência.

é a atividade permanente e sistemática, via ações especializadas, que visa identificar, acompanhar e avaliar ameaças, reais ou potenciais, sobre a segurança pública e produzir conhecimentos e informações que subsidiem o planejamento e a execução de políticas de Segurança Pública, bem como ações para prevenir, neutralizar e reprimir atos criminosos de qualquer natureza, de forma integrada e em subsídio à investigação e à produção de conhecimentos.(FERREIRA, Romeu Antonio).

2.2 Por sua vez a Inteligência Policial: È uma investigação voltada para a Segurança Pública, Por outro lado, é uma investigação policial que tem por objetivo, numa primeira instância, produzir conhecimento e, após, conseguir provas para um processo judiciário. "Conhecimento é poder". (Thomas Hobbes,1588-1679) no seu livro "Leviatã".

é o conjunto de ações que empregam técnicas especiais de investigação, visando a confirmar evidências, indícios e a obter conhecimentos sobre a atuação criminosa dissimulada e complexa, bem como a identificação de redes e organizações que atuem no crime, de forma a proporcionar um perfeito entendimento sobre a maneira de agir e operar, ramificações, tendências e alcance de condutas criminosas.(Ibid).

2.3 Contrainteligência: É o seguimento que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações de qualquer natureza que ameacem à salvaguarda de dados, conhecimentos, áreas, pessoas e meios de interesse da segurança, da sociedade e do Estado.

é a atividade que objetiva salvaguardar dados e conhecimentos sigilosos e identificar e neutralizar ações adversas de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem.(BRASIL. Resolução Nº 1, de 15 de julho de 2009, regulamenta o Subsistema de Inteligência de Segurança Pública – SISP).

Existe uma origem mitológica da Inteligência segundo a qual Argus, príncipe de Argólida, por volta de 690 a.C, que suplantou a hegemonia de Micenas, protegeu de diversas maneiras suas mensagens enquanto vivo e criou uma rede eficaz de espiões, tornou-se o pai da Inteligência. Após seu falecimento, tornou-se um semideus, e há diversas versões para sua “pós-morte”. Alguns vocábulos vindos de Argus são comuns à Inteligência: arguto, argúcia, argumento, arguir, etc. (BRAGA, 2005).

Ao identificar as origens da atividade de inteligência, tem-se como um dos primeiros registros históricos quando da jornada dos hebreus no deserto em busca de Canaã, a terra prometida, quando “Disse o Senhor a Moisés: Envia homens que espieem a terra de Canaã, que eu ei de dar aos filhos de Israel” (BIBLIA, Números 12,13).

Por esta passagem bíblica se percebe que a necessidade de conhecer o adverso é inerente às atividades governamentais, no caso em questão a conquista da terra sagrada pelo povo hebreu.

Outro registro histórico do emprego de informação para a tomada de decisão ocorre com Sun Tzu (2002, p.134), grande estadista e general chinês, que viveu há cerca de quinhentos anos antes de Cristo que afirmava:

O meio pelo qual, governantes sábios e generais sagazes se moveram e conquistaram outros, pelo qual suas realizações ultrapassaram as massas, foi o conhecimento acurado. O conhecimento acurado não pode ser obtido de fantasmas e espíritos, inferido dos fenômenos ou projetado a partir das medidas do Céu, mas deve ser obtido dos homens, porque é o conhecimento da verdadeira situação do inimigo.

O conceito da atividade de inteligência no Brasil está previsto no art. 1º, § 2º, do Decreto n. 4.376/2002:

Inteligência é a atividade de obtenção e análise de dados e informações e de produção e difusão de conhecimentos, dentro e fora do território nacional, relativos a fatos e situações de imediata ou potencial influência sobre o processo decisório, ação governamental, a salvaguarda e a segurança da sociedade e do Estado.

O Estado Democrático de Direito preconiza que todo ato decisório deve estar, lastreado em fundamentos amplos, legais e seguros.

De acordo com Kent (1967) na linguagem do ofício, a palavra informação (aqui no sentido de Inteligência) não é apenas utilizada para designar os tipos de conhecimentos que discutimos e o tipo de organização que as produz, é usada como sinônimo da atividade que a organização desempenha.

Prossegue o autor dizendo que é a informação como processo, e a preocupação primordial é com o grande número de problemas metodológicos, de diversas naturezas, características do processo de produção de informações.

O conhecimento que deriva do processo de produção de informações tem duas utilizações:

- i) serve para o uso preventivo ou defensivo, uma vez que alerta com antecipação dos problemas e dos desígnios do adversário que pode estar agindo contra a organização;
- ii) serve também para o uso positivo e antecipado da própria política ativa externa ou da estratégia administrativa da organização.

Mas, o que há de importante perceber é que, qualquer que seja a diversidade de sua utilização, o conhecimento é produzido por um processo de pesquisa.

Às vezes a pesquisa é formal, altamente técnica e trabalhosa; outras vezes é informal, sem técnica e rapidamente feita ou obtida. Na maioria das vezes um plano de produção de conhecimento requer diversos analistas trabalhando coletando e buscando informações de diversas fontes, outras vezes é executado em um minuto ou menos dependendo da oportunidade.

Os processos de pesquisas, particularmente os de produção de conhecimento em organizações policiais, são iniciados de duas maneiras principais.

Primeiro, quando os dirigentes e elaboradores da política começam a formular algo novo para tornar eficiente a missão institucional, e nesse caso devem pedir as informações antecedentes (devia ser feito com mais frequência). Isto significa estimular o pessoal da inteligência a lançar-se sobre uma pesquisa e a um processo de levantamentos com objetivos específicos. Segundo, quando os agentes do processo de inteligência são levados por seu próprio trabalho sistemático e contínuo de levantamentos sobre determinados temas considerados relevantes para a política de segurança.

Levantamento tem um significado de observação do que acontece dentro e fora da organização e a tentativa deliberada de descobrir o sentido dos acontecimentos. O processo real de observação tem lugar no ambiente organização e pode ser feito de forma ostensiva, velada, virtual ou de todas as maneiras associadas.

Em alguns países estrangeiros, as organizações de aplicação da lei fazem isso de forma massiva (principalmente em fontes abertas) com departamentos e uma multidão de funcionários ostensivos e outros credenciados, cujo dever é monitorar os acontecimentos e manter-se atento e relatar o que apreenderem. Cada um deles tem seu campo especial de interesse e competência e mantém seus chefes a par das novidades em tempo real e com antecipação. O trabalho deve ser suplementado com atividades de operações de inteligência por meio de agentes em campo ou recrutadores encobertos para descobrir e relatar os assuntos que são mais difíceis de verificar abertamente.

3. INTELIGÊNCIA POLICIAL

O conceito e a abrangência da Inteligência Policial visam sua aplicação no âmbito da investigação criminal (polícia judiciária) e no emprego do policiamento ostensivo (polícia militar). No primeiro caso, é procurada a produção de provas; no segundo, se busca uma otimização dos meios e a análise do fenômeno criminal.

Também é necessário desfazer a confusão conceitual na aplicação dos termos “Inteligência Policial” e “Inteligência de Segurança Pública”. Esta tem por conteúdos a Inteligência Policial e a Análise Criminal. Diante dos níveis de decisão (estratégico, tático e operacional), a Inteligência de Segurança Pública se materializa no nível tático/operacional através da Inteligência Policial e da análise criminal.

Para Ferro Junior (2004) um dos pressupostos em estratégia de uma organização policial é ter a possibilidade de uma visão ampla de uma situação externa (fenômeno criminal) com a capacidade interna da organização em desenvolver ações que propiciem eficiência e eficácia nas atividades contra o crime. Assim, no momento de formulação de diretrizes, devem ser considerados todos os fatores que influenciam na atual deficiência da organização, perante a complexidade do crime, identificando os pontos fortes e pontos fracos e desenvolvendo as medidas para a solução.

Inteligência e Investigação são conceitos que, apesar de terem muitas vezes similaridades, não se confundem. Inteligência seria uma atividade *pro-ativa*, caracterizada pela busca incessante de informações, para fins de possibilitar ao gestor público um supedâneo mínimo para seu poder decisório. Com base em informações contextualizadas, o destinatário final da atividade de inteligência poderá propor e comandar ações concretas em termos de segurança pública. O conhecimento teria o potencial para “equacionar o poder”, sendo necessário possuir a informação mais atualizada possível, para conseguir posição de vantagem sobre o adversário (no caso, a criminalidade em geral e organizada).

4. ATIVIDADE DE CONTRAINTELIGÊNCIA

As atividades de Contrainteligência foram desenvolvidas e adaptadas a partir das técnicas aplicadas nos contextos militar e de estado e, no seu sentido mais amplo, tais técnicas são entendidas como sendo as que objetivam neutralizar as ações de espionagem.

A Contrainteligência, pela perspectiva militar, é definida como um esforço multidisciplinar que contempla a Contrainteligência Humana (C-HUMINT), a Contrainteligência de Sinais (C-SIGINT) e a Contrainteligência de Imagens (C-IMINT) desenvolvidas contra todo processo de coleta de origem externa. A força da Contrainteligência, em conjunto com outros ativos de inteligência, deve possuir a capacidade em detectar todos os aspectos da coleta de inteligência e atividades relacionadas que se propõe a ameaçar a Segurança em Operações, de Pessoal e de Material (Equipamentos). Através de sua capacidade analítica, a Contrainteligência provê recomendações, as quais, se implementadas, irão resultar em negação de informação às eventuais ameaças.

O manual da Marine Corps dos USA, conceitua a contrainteligência como sendo a coleta de informações e a condução de atividades que visa proteger contra espionagem ou

outras atividades de inteligência, sabotagem ou assassinatos conduzidos por ou em nome de governos ou elementos estrangeiros, assim como organizações estrangeiras, ou atividades de terrorismo internacional.

Gleghorn (2003,) se apoia nos referenciais da Marine Corps para afirmar que existem, essencialmente, quatro funções nas quais a contrainteligência se fundamenta e opera: coleta, investigação, análise e operações. Enquanto estas quatro funções são derivadas especificamente desse manual, os demais organismos de força nacional e o Departamento de Defesa Americano reconhecem que as diretivas de contrainteligência possuem como princípio estas mesmas funções.

Pela perspectiva civil, as ações de contrainteligência buscam detectar o invasor, neutralizar sua atuação, recuperar, ou mesmo contra-atacar por meio da produção de desinformação (PASSOS, 2005).

Quando o processo de decisão envolve as necessidades de segurança e proteção nas organizações, somos impelidos a imaginar somente as perspectivas da tecnologia da informação (TI) como sendo as principais. Todavia, existem outros aspectos que precisam ser considerados, e que se imaginam haver tantas vulnerabilidades quanto possíveis.

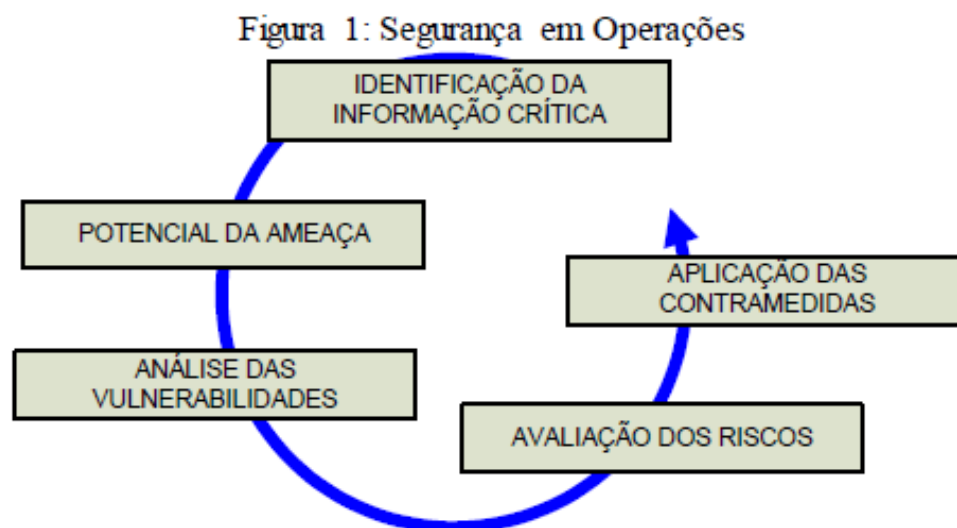
Segundo a Portaria Nr11 do Exército Brasileiro (BRASIL, 2001), com o fim de abranger todas as eventuais vulnerabilidades, as medidas de proteção de Contrainteligência devem contemplar ações nos mais variados segmentos das instituições. Os domínios de informação sensível relativos à Segurança de Pessoal, da Documentação, do Material, de Áreas e Instalações, da Comunicação e da Informática necessitam de análise e atenção quanto às necessidades de controles e mecanismos de proteção. Esta maior abrangência torna-se fundamental para permitir a redução das vulnerabilidades e ameaças em um ambiente organizacional.

Starry e Arnenson (2008), afirmam que à medida que a tecnologia permite um maior número de indivíduos, grupos, organizações e nações-estados conectarem-se com o mundo por meio do ambiente de informação global. Assim, pode-se esperar que esses usuários prossigam seus interesses, tentando manipular e controlar o conteúdo e o fluxo das informações dentro do ambiente de informação militar.

4.1 SEGURANÇA EM OPERAÇÕES NA CONTRAINTELIGÊNCIA

O processo de Segurança em Operações é um contraponto ao modelo de Inteligência por se configurar na defesa de ações de inteligência. Este processo representa uma abordagem de contrainteligência em termos práticos. Esta abordagem trata-se de um processo sistemático que propicia proteção a informações e segredos fundamentais de contrainteligência (Quinn, 2002, p.245). Conforme apresentado na Figura 1, o objetivo é implantar ações concretas em matéria de capacidades, limitações, atividades e intenções, evitando ou controlando, assim, a exploração por forças contrárias.

Figura 1: Segurança em Operações



Fonte: Anton et all, 2003 e Miller, 2002

Este processo contempla uma estrutura de fluxo contínuo de atividades, onde o resultado de cada uma é a saída para as atividades seguintes. O referido autor apresenta o modelo tendo como principal objetivo considerar o valor do tempo da informação. Corresponde ao entendimento de que se qualquer organização tiver algum tipo de invasão, qual seria a capacidade da função Segurança em identificar e quantificar o potencial da perda. Tal postura é fundamental para amenizar os eventuais resultados negativos.

Como metodologia, a Segurança em Operações, também denominado de OPSEC originou-se durante a guerra do Vietnam como um meio de descobrir como o inimigo estava obtendo informações avançadas em certas operações de combate no Sudeste da Ásia. OPSEC é um programa de contramedidas voltado para a proteção de informações críticas (ANTÓN *et al*, 2003, p.21).

Conforme Miller (2002, p.249), George Lean, o ex-diretor de Segurança em Operações da NSA, comenta que cada uma das fases do Modelo de Proteção é importante para a integridade e eficácia do processo em seu todo. Embora cada uma delas possua valores, isoladamente nessa condição, é só quando se consegue empregá-las em conjunto que se faz possível avaliar o valor sinérgico do processo de segurança em operações.

4.2 Técnica de Contrainteligência

Para alguns profissionais, os termos falsa informação, desinformação e decepção são sinônimos. Para o profissional de Inteligência são consideravelmente diferentes. A falsa informação estaria fundamentada em erro ou ignorância. Desinformação já mostra uma conotação de malícia e é tipicamente encontrada na área ofensiva da inteligência. A decepção, encontrada mais frequentemente na área defensiva da inteligência, embora tenha também uma clara conotação ofensiva, especialmente quando usada em âmbito internacional, é comumente referida numa maneira mais politicamente correta como gerência da percepção.

4.3 Falsa Informação

A falsa informação são os falsos entendimentos, aqueles elementos confusos que os infiltrados obtêm em suas pesquisas, através de seus próprios erros, ou através de falsos passos. Por exemplo, se o infiltrado descobre alguma coisa através de um artigo de jornal que está total e completamente errado, e que o órgão de Segurança Pública não tem nada a fazer com a inexatidão do repórter, o infiltrado será a vítima de uma falsa informação. Se este repórter se baseou em respostas de servidores que não sabiam a coisa certa ou mesmo exageraram nos seus relatos, é erro dele e das fontes e o Analista de Contrainteligência não fez nada propositadamente para criar esse falso entendimento (COELHO, Paulo Cesar).

Por extensão, se um agente de inteligência cometer um erro ou segue um caminho que parece ter sido ditado por algum informe que sabe que pode ser errado, você não está obrigado por nenhuma regra ou ética a corrigi-lo. Simplesmente é responsabilidade do

Agente, verificar a validade do informe que recebe, bem como a sua exatidão antes de tomar qualquer tipo de decisão ou atitude (BRASILIANO, Antonio Celso Ribeiro).

Mesmo que o termo “contraineligência” não existisse até o século XIX, ele foi sempre empregado no intuito de neutralizar ações ilícitas, fazendo com que informações falsas fossem passadas aos inimigos, para que caíssem no erro e pudessem acreditar e assimilar tais informações.

4.4 Desinformação

Para Walter Féliz, a desinformação é o nome técnico que se dá à “arte” de enganar alvos para alcançar um efeito determinado, seja ocultando ou distorcendo fatos e induzindo os adversários a erro de julgamento. Já Sun-Tzu, toda a arte da guerra está baseada no engodo.

Toda campanha militar repousa na dissimulação. Finge desordem. Jamais deixes de oferecer um engodo ao inimigo, para ludibriá-lo. Simula inferioridade para encorajar sua arrogância. Atiça sua raiva para melhor mergulhá-lo na confusão. Sua cobiça o arremeterá contra ti e, então, ele se estilhaçará. (TZU, 2009, p. 23-24).

As ações de contraineligência buscam detectar o invasor, neutralizar sua atuação, recuperar, ou mesmo contra-atacar por meio da produção de desinformação entende que especificamente na segurança pública, não basta focar somente ações e medidas operacionais. Torna-se fundamental, também, a aplicação de técnicas e ferramentas para a manutenção desse conhecimento.

Desinformação é o resultado de uma atitude ativa de alguém que pensou num caminho e num objetivo para ser alcançado através da cessão de informações que deliberadamente são falsas. A informação é inserida no sistema de comunicação do alvo, em algum ponto, seja através da mídia, seja através das fontes em que se sabe que o alvo é levado a confiar e é projetada para desorientar o público alvo. Muito frequentemente a desinformação é idealizada no sentido de aproveitar estereótipos existentes, particularmente no que se refere à cultura de um povo — ou de um grupo específico. Os principais alvos da desinformação são as pessoas que estão nos extremos do espectro político ou social, que geralmente possuem apenas o menor grau de tolerância e cepticismo e que sempre permitem que relatos de fontes menos confiáveis influenciem seu julgamento. A operação mais conhecida nos manuais de contraineligência de quem milita nesse meio ficou conhecida como a mais bem sucedida

Operação de Desinformação da Segunda Guerra Mundial, surge a Operação “*Mincemeat – Recheio*”.

Após o sucesso da invasão da África do Norte, os Estrategistas aliados queriam definir o próximo passo: avançar da África para a Europa através da Sicília, pelo estreito de Messina. É claro que os alemães, por certo, esperavam por isso e iriam concentrar suas forças na região. Como convencê-los do contrário, induzindo-os a dispersar suas tropas para outros pontos do continente europeu? A partir daí é que entra em ação o Intelligence Service britânico, quando um de seus membros pensa numa *Operação de Desinformação*.

Na noite de 30/04/1943 um submarino britânico lançou no local previamente planejado uma cápsula que se abriria no mar. Quase ninguém a bordo sabia o que havia dentro. Um pescador espanhol encontrou o corpo trazido pela maré e avisou as autoridades navais que, de imediato, comunicaram o evento aos nazistas. De fato o serviço de espionagem alemão verificou a exatidão das informações que o corpo trazia e, após uma semana de contrainformações, o Alto Comando Aliado recebeu notícias de que grande contingente de tropas alemães estava sendo transferido para a Grécia, Córsega e Sardenha.

A Operação foi planejada nos mínimos detalhes desde a escolha do cadáver que deveria ter como causa mórtis as características de um afogamento para confundir os alemães, pois fatalmente isso seria verificado pelo Serviço de Inteligência Alemão, bem como todo o resto da Estória de Cobertura. Foi criado um passado para o major William Martin, que na verdade era um súdito inglês que morrera de pneumonia e a família havia cedido seu corpo ao Estado desde que sua identidade jamais fosse revelada. A farda que ele usava trazia seu nome bordado, colocaram em seus bolsos bilhete de sua noiva, tickets de teatro da véspera do desastre e até nota de lavadeira. Tudo poderia ser checado que haveriam de dar crédito ao achado, várias ligações fizeram para o major William inclusive lhe arrumaram uma namorada para dar mais realidade a história e a ela criar maior poder de convencimento aos alemães. Cartas e documentos foram dobrados e desdobrados várias vezes para parecer que tinham sido lidos diversas vezes.

O major Martin conduzia ainda chapas de identificação, um relógio de pulso, cigarros, bilhetes antigos de ônibus e chaves. Em sua última noite na Inglaterra, teria levado a noiva ao teatro e tinha no bolso a metade de dois ingressos para uma peça no dia 22 de abril de 1942.

Em suma, o plano de certa forma simples, baseava-se nos seguintes pontos:

Martin levaria numa pasta uma carta do general Sir Archibald Nye, subchefe do Estado-Maior Imperial, ao general Alexander, comandante do Grupo de Exércitos da África,

com uma explicação, entre amigos, dos motivos pelos quais Alexander não estava recebendo do chefe do Estado-Maior, tudo o que queria. Por inferência, chegava-se a conclusão que se planejava atacar o Mediterrâneo Ocidental. Os possíveis pontos seriam um na Grécia e o outro, não muito bem identificado, mas não era a Sicília.

O major levava ainda um comunicado do Lorde Louis Mountbatten ao almirante de Esquadra, Sir Andrew Cunningham, comandante-e-chefe no Mediterrâneo, explicando sua missão e concluindo: “Creio que Martin é o homem que lhe serve. Queira mandá-lo de volta logo que termine o assalto. E não se esqueça de dar-lhe mais sardinhas. Elas estão aqui racionadas”.

A palavra “sardinhas” servia apenas para indicar aos alemães a Sardenha como objetivo do ataque. Estava assim em grosso modo preparada, a Operação Recheio.

O cadáver de Martin seria transportado pelo submarino Seraph, sob o comando do tenente Jewell, e lançado ao mar próximo a Huelva.

O próprio Churchill deu sua aprovação e ordenou para que o general americano Eisenhower, no comando da invasão da Sicília, fosse informado.

A operação foi desencadeada e na manhã do dia 30 de abril de 1943, um pescador espanhol avistou o corpo perto da praia e avisou as autoridades. Após autópsia, constatou-se asfixia por imersão no mar.

Como os britânicos imaginavam, os documentos caíram nas mãos de um conhecido espião nazista operando na Espanha, que depois de fotografá-los enviou as fotos para a Alemanha. Nesse ínterim, um agente alemão estava na Inglaterra verificando o passado de Martin, investigando os dados relativos a sua vida. Tudo que procurou achou e se convenceu que tudo era verdadeiro, informando a seus superiores na Alemanha, sem saber que a Contra-Inteligência havia seguido seus passos.

Como resultado o Alto Comando Alemão transferiu uma Divisão Blindada da França para o Peloponeso (região da Grécia) e também foram colocadas minas ao longo do litoral grego.

No oeste, o marechal-de-campo Wilhelm Keitel assinou uma ordem determinando o reforço da Sardenha.

Mesmo depois de iniciado o ataque principal à Sicília, os alemães continuavam pensando tratar-se apenas de uma manobra secundária. O êxito da missão pode ser avaliado nas palavras do marechal-de-campo, Erwin Rommel, cujos documentos pessoais revelam que,

quando os aliados invadiram a Sicília, as defesas alemãs achavam-se dispersas em consequência do encontro do cadáver de um mensageiro diplomático na costa da Espanha.

É certo que a Operação tinha muito mais detalhes do que os aqui mencionados, porém, nosso intuito é mostrar a importância do Serviço de Inteligência e ContraInteligência para a Segurança Pública, em particular a atividade de ContraInteligência que se utiliza de meios técnicos para garantir o sucesso das operações de segurança pública, utilizando um recurso indispensável a DESINFORMAÇÃO.

4.5 Decepção:

Sun Tzu (2013) bem definiu quando sugeriu que toda arte de guerra é baseada no engodo(decepção).

“Qualquer operação militar tem na dissimulação sua qualidade básica. Um chefe que é capaz deve fingir ser incapaz; se estiver pronto, deve fingir-se despreparado; se estiver perto do inimigo deve parecer estar longe. Um bom chefe deve: Oferecer uma isca para fascinar o inimigo que procura alguma vantagem; Capturar o inimigo quando ele está em desordem”

(Sun Tzun)

Assim, quando capaz, finja incapacidade; quando ativo, finja inatividade. Quando próximo, faça parecer que você está muito longe; quando longe, que você está muito perto. Ofereça ao inimigo uma isca para atraí-lo; finja desordem e derrube-o. Quando ele se concentrar, prepare contra ele; onde ele for forte, evite. Irrite-o e confunda-o. Finja inferioridade e encoraje sua arrogância. Este são os elementos que defini a técnica de Decepção, é a forma de induzir o oponente quando você está começando a proteger a si mesmo e quer permitir que ele obtenha impressões errôneas através de suas ações controladas e orientadas ao induzimento. Essas impressões freqüentemente gerenciam de tal forma a opinião do adversário que se torna difícil ele acreditar que sejam erradas e sobrepujam muitas vezes as análises mais rigorosas.

A essência da decepção é saber — ou acreditar que você saiba — quem está obtendo o quê de quem e através quem. E então, com esses pensamentos em mente, colocar dentro desses canais — e apenas estes canais — a informação que você quer que eles acreditem e sobre a qual possivelmente irão trabalhar. Desorientem-os até que encontrem um

caminho que não mostre o que você está realmente investigando. Propositadamente permita-lhes confusão e falsos entendimentos sobre suas capacidades, situação e limitações.

O ramo de contrainteligência não deve ser visto como algo apartado do ramo de inteligência, posto que ambos são parte da atividade de inteligência enquanto todo. Enquanto uma age de forma “ofensiva”, a outra atua no campo “defensivo”, visando proteger as metodologias, atividades operacionais, documentos, comunicações, áreas, instalações, e, mais importante, os próprios integrantes da força policial da atuação perniciosa de organizações criminosas ou de qualquer outra potencial ameaça à integridade dos referidos elementos constituintes da Polícia. Não poderíamos encerrar este trabalho sem que trouxéssemos a baila a resolução de regulamentação, da atividade de inteligência e contrainteligência de Segurança pública.

5. RESOLUÇÃO Nº 1, DE 15 DE JULHO DE 2009

Regulamenta o Subsistema de Inteligência de Segurança Pública - SISP, e dá outras providências.

O SECRETÁRIO NACIONAL DE SEGURANÇA PÚBLICA, no uso das atribuições que lhe conferem o art. 3º, I, "a", do Decreto nº 3.695, de 21 de dezembro de 2000,

Considerando a manifestação favorável do Conselho Especial do Subsistema de Inteligência de Segurança Pública, resolve:

Art. 1º O Subsistema de Inteligência de Segurança Pública -SISP, que compõe o Sistema Brasileiro de Inteligência - SISBIN, constituído de rede própria e responsável pelo processo de coordenação e integração das atividades de inteligência de segurança pública no âmbito do território nacional, tem por objetivo fornecersubsídios informacionais aos respectivos governos para a tomada de decisões no campo da segurança pública, mediante a obtenção, análise e disseminação da informação útil, e salvaguarda da informação contra acessos não autorizados.

§ 1º O SISP tem como fundamentos a preservação e a defesa da sociedade e do Estado, das instituições, a responsabilidade social e ambiental, a dignidade da pessoa humana, a promoção dos direitos e garantias individuais e do Estado de Democrático de Direito.

§ 2º A Agência Central do SISP é a Coordenação-Geral de Inteligência - CGI, da Secretaria Nacional de Segurança Pública - SENASP, recipiendária direta dos dados, informações e conhecimentos decorrentes das atividades de Inteligência de Segurança Pública.

§ 3º São elementos constituintes do SISP, originariamente:

I - Conselho Especial do Subsistema de Inteligência de Segurança Pública;

II - a Rede Nacional de Inteligência de Segurança Pública -RENISP;

III - a Rede de Integração Nacional de Informações de Segurança Pública, Justiça e Fiscalização - INFOSEG;

IV - o Sistema Nacional de Identificação de Veículos em Movimento - SINIVEM;

V - os Organismos de Inteligência de Segurança Pública e suas agências, o respectivo pessoal e estrutura material;

VI - a Doutrina Nacional de Inteligência de Segurança Pública - DNISP; e

VII - os sistemas de informações, os bancos de dados de propriedade e ou cedidos à SENASP;

VIII - Conselho Nacional de Chefes de Organismos de Inteligência de Segurança Pública - CNCOI.

IX - as Agências de Inteligência - AI - a ele vinculadas, respectivo pessoal e material.

§ 4º Para os efeitos desta Resolução deverão ser considerados os seguintes conceitos:

I - Inteligência: é a atividade que objetiva a obtenção, análise e disseminação de conhecimentos, dentro e fora do território nacional, sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado;

II - Contra-Inteligência: é a atividade que objetiva salvaguardar dados e conhecimentos sigilosos e identificar e neutralizar ações adversas de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem;

III - Inteligência de Segurança Pública: é a atividade permanente e sistemática via ações especializadas que visa identificar, acompanhar e avaliar ameaças reais ou potenciais sobre a segurança pública e produzir conhecimentos e informações que subsidiem planejamento e execução de políticas de Segurança Pública, bem como ações para prevenir, neutralizar e reprimir atos criminosos de qualquer natureza, de forma integrada e em subsídio à investigação e à produção de conhecimentos;

IV - Inteligência Policial: é o conjunto de ações que empregam técnicas especiais de investigação, visando a confirmar evidências, indícios e a obter conhecimentos sobre a atuação criminosa dissimulada e complexa, bem como a identificação de redes e organizações que atuem no crime, de forma a proporcionar um perfeito entendimento sobre a maneira de agir e operar, ramificações, tendências e alcance de condutas criminosas;

V - Análise Criminal: é um conjunto de processos sistemáticos direcionados para o provimento de informação oportuna e pertinente sobre os padrões do crime e suas correlações de tendências, de forma a apoiar a área operacional e administrativa no planejamento e distribuição de recursos para a prevenção e supressão de atividades criminosas;

VI - Dado: é qualquer representação de um fato ou de uma situação, passível de estruturação, obtenção, quantificação e transferência, sem exame e processamento pelo profissional de inteligência de segurança pública;

VII - Informação: é o conjunto de dados que possui relevância e aplicação útil, exige unidade de análise e consenso em relação ao seu conteúdo;

VIII - Conhecimento: é a representação de um fato ou de uma situação, real ou hipotético, de interesse para a atividade de inteligência de segurança pública, com exame e processamento pelo profissional de inteligência;

IX - Atividade de Informação: é a que tem por finalidade a produção de conhecimento que habilite as autoridades governamentais, nos respectivos níveis e áreas de atribuição, à oportuna tomada de decisões ou elaboração de planos, fornecendo subsídios à administração institucional para a formulação, execução e acompanhamento de políticas próprias; e

X - Atividade de Inteligência de Segurança Pública: é a atividade técnico-especializada, permanentemente exercida e orientada para a produção e salvaguarda de conhecimentos de interesse da segurança pública que, por seu sentido velado e alcance estratégico, configurem segredos de interesse do Estado e das instituições, objetivando assessorar as respectivas chefias em qualquer nível hierárquico.

Art. 2º Ficam reconhecidas as AI existentes e a serem criadas na estrutura dos Organismos de Inteligência integrantes do SISP, conforme as diretrizes contidas nesta Resolução.

§ 1º As AI funcionarão na sede da unidade correspondente e terão a conformação nominal, estrutural e orgânica das unidades a que estejam vinculadas.

§ 2º As AI comporão a Rede Nacional de Inteligência de Segurança Pública - RENISP, sob a gestão, responsabilidade e controle direto da Coordenação-Geral de Inteligência da SENASP, para fins táticos, estratégicos e normatização.

§ 3º Integrarão ainda a RENISP os gabinetes e as unidades de inteligência desconcentrados, adidos e avançados que contem com a participação da SENASP, ainda que em caráter temporário.

Art. 3º As AI são unidades integrantes da RENISP e funcionarão como sistemas de captação, tratamento e difusão de dados, informações e conhecimentos em torno da atividade de inteligência de segurança pública, nos moldes da doutrina apropriada e na área da circunscrição ou de competência da instituição, observados os aspectos geográfico, competitivo, político-social, tecnológico, temporal, dentre outros, sob a orientação, coordenação e supervisão da CGI / SENASP.

Art. 4º As AI tem por objetivo viabilizar a interoperacionalidade entre a CGI e todas as unidades que compõe a estrutura do SISP.

Art. 5º Constitui finalidade das AI desenvolver, de forma rápida, eficaz, eficiente e conjunta, a execução de serviços compreendidos na atividade de inteligência de segurança pública em âmbito de cada instituição, para atendimento das demandas emergentes e do planejamento de ações que impliquem na realização de serviços denatureza correlata, além de prover informações, observado o princípio da oportunidade, dentre outros, com vistas a subsidiar a adoção de providências adequadas em cada esfera de atuação.

Art. 6º As AI subordinam-se à chefia da unidade organizacional respectiva e a sua atuação sempre deverá obedecer as diretrizes contidas na DNISP e nas deliberações do Conselho Especial do Subsistema de Inteligência de Segurança Pública.

Art. 7º É atribuição prioritária das AI, a execução das atividades de informações e inteligência de segurança pública na área da circunscrição correspondente, cabendo-lhes, ainda, planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência de segurança pública da área respectiva, obedecidas a política e as diretrizes superiores, e:

I - captar e difundir as informações de interesse à atividade de inteligência de segurança pública, observando-se o seguinte:

a) foco principal - Segurança Pública:

a.1. crime organizado, tráfico de drogas, armas e explosivos, terrorismo, tráfico de seres humanos e de órgãos, homicídios, quando envolver ações de grupos de extermínio, encontro de cadáver, furto e roubo de veículos, roubo e furto de cargas, seqüestros, crimes contra os meios de comunicação e transportes, fluxo migratório de infratores, movimentação

em unidades prisionais, rebelião em unidades prisionais; roubo a banco, lavagem de dinheiro, corrupção, desvio de conduta policial e as ações criminosas que envolvam a participação de quadrilhas e bando, grupos, facções, seitas ou similares, seja no nível local ou em amplo espectro, além de outros assuntos de interesse da Atividade de Inteligência de Segurança Pública considerados úteis.

b) foco secundário - Segurança Interna - fatos relativos à dinâmica social que possam atentar contra a segurança interna.

c) foco político e administrativo - fatos relativos à demanda social

II - catalogar as modalidades criminosas, procedendo, inclusive, à fotografia de infratores;

III - coletar, gravar, transcrever e retransmitir, quando for o caso, as notícias locais relevantes à segurança pública, detalhando a fonte;

IV - registrar a memória da AI no que concerne à atividade de informações e inteligência de segurança pública em nível local;

V - realizar estudos e estatísticas de interesse da segurança pública, relacionadas com a atividade de inteligência;

VI - acompanhar fatos de fatos de interesse da segurança pública;

VII - manter atualizado o protocolo de informações essenciais e dados básicos proposto pelo CNCOI e estabelecido pela CGI;

VIII - proceder ao recebimento, na qualidade de recipiendário imediato, de notícia oriunda de serviço institucionalizado de captação de delação anônima, dar o tratamento adequado em face do sigilo a ela inerente, efetuando a triagem e encaminhamento segundo a área de competência e/ou interesse envolvido, buscando as respectivas respostas e difusão adequada, ainda que demandem seqüência de trabalho, desde que não haja instrução expressa em contrário;

IX - exercer o papel de multiplicador da Atividade de Inteligência de Segurança Pública, observadas as diretrizes da CGI e a doutrina aplicável, na área de sua competência, ;

X - valer-se dos recursos disponíveis na AI para o exercício de suas atribuições;

XI - executar, quando lhe forem atribuídas, obedecidas as disposições legais, as atividades de interceptação de comunicações de informática e de telemática;

XII - colher informes e dados, validá-los, interpretá-los e, se for o caso, reavaliá-los, bem como gerar informações ou conhecimentos, procedendo à gestão da informação;

XIII - elaborar os relatórios de apoio auxiliar às atividades diárias de informações e inteligência de segurança pública;

XIV - prestar assessoramento para auxiliar na análise criminal, administrativa, tático-operacional e estratégica da AI;

XV - elaborar os documentos de inteligência de segurança pública segundo a DNISP;

XVI - criar, interpretar, compreender, analisar, transformar, difundir, compartilhar, gerir e arquivar dados, informações e conhecimentos relacionados com a Atividade de Inteligência de Segurança Pública;

XVII - recrutar e aproveitar potenciais colaboradores da sociedade civil com capacidade técnica para apoiar a execução da Atividade de Inteligência de Segurança Pública, resguardando o sigilo das operações e atividades;

XVIII - manter a memória física ou digital das atividades de inteligência de segurança pública na AI;

XIX - definir, em conjunto com a autoridade competente, a estratégia informacional local e atender às demandas e necessidades da Agência Central e demais AI da Comunidade de Inteligência - CI;

XX - catalogar os diversos tipos de crimes, técnicas utilizadas para a sua prática, informantes, autores, vítimas, testemunhas e notícias relacionadas às ações que sejam ou que se pressupõe de interesse para a atividade de inteligência de segurança pública, objetivando antecipar possíveis ações a serem desenvolvidas e a subsidiar outras formas de contenção ou acompanhamento de suas ocorrências;

XXI - requalificar permanentemente os respectivos agentes em habilidades específicas, visando aperfeiçoar métodos e técnicas de tratamento da informação e aprimoramento da Atividade de Inteligência de Segurança Pública;

XXIII - produzir informações sobre a criminalidade violenta, estruturando os seus padrões e tendências;

XXIV - acompanhar permanentemente a evolução da legislação relacionada à matéria de inteligência de segurança pública;

XV - coletar, quando necessário, informações sobre qualquer investigação criminal, correcional e administrativa que estiver sendo executada no respectivo âmbito, ressalvados os impedimentos legais;

XVI - gerir documentos e arquivos visando a salvaguardar assuntos de interesse do Estado e da atividade de inteligência de segurança pública;

XVII - atuar em conformidade com o Plano Nacional de Inteligência de Segurança Pública, por iniciativa e ou estímulo externo;

XVIII - propor medidas de segurança orgânica na AI respectiva, cadastrando os profissionais de inteligência de segurança pública da área para os fins de difusão de documentos de inteligência;

XIX - participar do planejamento de operações e supervisionar a arrecadação, digitalização e organização de fotos do banco de dados em apoio à investigação, produção de conhecimentos e análise sobre a conjuntura e a estrutura criminal na respectiva área.

XX - apresentar sugestões e boas práticas para a área em questão, bem como sugerir mudanças para o aperfeiçoamento da ISP e do SISP.

Parágrafo único. A CGI, oferecerá o suporte necessário para o treinamento, adaptação, estágio, qualificação, requalificação e aperfeiçoamento dos profissionais de inteligência de segurança pública integrantes do SISP, para que exerçam com eficiência, eficácia e efetividade as atribuições que lhes competem segundo as regras aplicáveis à ISP.

Art. 8º Fica atribuída aos chefes dos Organismos de Inteligência de Segurança Pública integrantes do SISP a função de gestores da ISP na respectiva esfera de competência, incumbindo-lhes fazer cumprir, em sua área de competência, o disposto nesta Resolução.

Art. 9º Cada AI manterá arquivo mínimo para guarda de documentos afetos à ISP, devendo observar as normas relativas à salvaguarda de assuntos sigilosos e proteção do conhecimento, classificando-os de acordo com a sua natureza.

Art. 10. Os profissionais que atuarão na ISP serão selecionados de acordo com o preconizado na DNISP, códigos de ética e regulamentos de cada órgão integrante do SISP, observados os seguintes requisitos mínimos:

I - ser, preferencialmente, servidor público da ativa;

II - estar no exercício de suas funções;

III - não ter sofrido pena disciplinar de suspensão por mais de dez dias, nos doze meses anteriores à data da seleção, salvo se reabilitado;

IV - ter concluído com aproveitamento o treinamento básico acerca da ISP a ser ministrado pela instituição a que pertencer ou de qualquer outra, integrante do SISP, de qualquer nível ou esfera de poder; e

V - assumir o compromisso, mediante declaração expressa e sob as penas da lei, de estar ciente de que a utilização indevida, bem como a divulgação não autorizada, dentro ou fora do ambiente de trabalho, de dados, informações, conhecimentos, documentos, materiais e meios sigilosos, de que tiver conhecimento em razão do exercício do cargo ou função, acerca de fatos de interesse do SISP, de suas AI e unidades organizacionais, de seus meios operacionais, da sociedade e do Estado, implica em sanções administrativas, civis e criminais.

Art. 11. Os profissionais integrantes das AI possuem atribuições e vantagens próprias decorrentes do exercício da Atividade de Inteligência de Segurança Pública.

§ 1º São atribuições:

I - incumbir-se das atividades afetas à AI, sob a orientação, coordenação e supervisão da CGI;

II - observar os procedimentos e normas relativos à salvaguarda de informações e proteção de conhecimentos sensíveis;

III - participar do treinamento básico para integrar a AI e freqüentar cursos correlatos quando convidado pela CGI;

IV - observar o disposto na respectiva lei de organização da carreira e regime jurídico, bem como os princípios e valores elencados no Código de Ética do Servidor Público;

V - respeitar os direitos e garantias fundamentais previstos na Constituição Federal e promover a efetividade dos direitos humanos e o Estado Democrático de Direito;

VI - obedecer os princípios e pressupostos filosóficos da doutrina de inteligência de segurança pública; e

VII - desenvolver suas atividades segundo a necessidade de informações de âmbito local e da Agência Central, tendo como parâmetros, além dos princípios e valores previstos na doutrina de inteligência de segurança pública, a impessoalidade, o apartidarismo, lealdade à nação e fidelidade à respectiva instituição.

§ 2º São vantagens:

I - consignação do exercício da função nos assentamentos funcionais, por se constituir em serviço de relevante interesse público;

II - prioridade em situação de transferência, por interesse do servidor, para prestar serviços nos Órgãos integrantes do SISP; e

III - prioridade na participação em cursos ministrados pela CGI e demais integrantes do SISP ou fora dela, de interesse para a atividade de inteligência de segurança pública, inclusive em outros Estados ou países.

Art. 12. O profissional de ISP será excluído das funções a pedido ou de ofício, nas seguintes hipóteses:

I - a pedido:

a) mediante requerimento contendo as razões, motivos e fundamentação para a sua exclusão ao seu chefe imediato que despachará expondo seu posicionamento, remetendo o expediente, com a observância do canal de comunicação estabelecido na doutrina de inteligência, ao superior hierárquico para deliberação;

b) até que ocorra a decisão pela exclusão, o profissional de ISP deverá afastar-se da função na AI, apresentando o inventário do acervo e bens, sob sua responsabilidade;

c) quando houver interesse do servidor em transferir-se para outra localidade.

II - de ofício:

a) por interesse da AI, com motivação expressa;

b) quando ocorrer transferência do servidor ex-officio para outra unidade organizacional;

c) quando houver condenação do servidor por transgressão disciplinar de natureza grave, em conformidade com o disposto na legislação que lhe for aplicável.

§ 1º Na hipótese da alínea c do inciso I, o servidor deverá encaminhar requerimento com pedido de exclusão, devidamente fundamentado, com o "de acordo" da chefia imediata, para deliberação da chefia imediata.

§ 2º Na hipótese da alínea c do inciso II, o servidor somente será excluído após o trânsito em julgado da decisão, sendo-lhe aplicado o disposto no inciso b do mesmo artigo.

§ 3º Os casos de exclusão de servidores não abrangidos nesta Resolução serão estabelecidos em deliberação do Conselho Especial do Subsistema de Inteligência de Segurança Pública.

Art. 13. No caso de afastamento temporário ou definitivo do servidor, a chefia imediata se encarregará de substituí-lo imediatamente, observados os requisitos previstos no art. 10, evitando-se prejuízos para as atividades de que trata esta Resolução.

Art. 14. Na hipótese de exoneração do cargo ocupado pelo servidor, de forma a desvincular-se da atividade de ISP, por qualquer meio, deverá a chefia imediata notificar o SISISP, mediante a observância do canal de comunicação apropriado.

Parágrafo único. Para os efeitos desta Resolução, chefia imediata, é o titular da unidade a que o servidor estiver diretamente subordinado.

Art. 15. O treinamento dos profissionais para integrarem as AI ficará a cargo da instituição à qual pertence o servidor, sob coordenação técnica da CGI, obedecidas as disposições e deliberações do Conselho Especial do Subsistema de Inteligência de Segurança Pública.

Art. 16. Fica instituído e implantado, a partir da publicação desta Resolução, o Conselho Nacional de Chefes de Organismos de Inteligência de Segurança Pública - CNCOI, órgão de caráter consultivo para os fins do SISISP.

§ 1º O CNCOI será presidido pelo Coordenador-Geral de Inteligência da SENASP e composto, de forma permanente, pelos Coordenadores de Inteligência - COINT, de Redes e

Sistemas - CORESI, da SENASP e pelos titulares dos Órgãos de Inteligência componentes do SISP, nos termos do Decreto 3.695, de 21 de dezembro de 2000.

§ 2º Cabe ao CNCOI propor a inclusão de novos membros ao SISP, mediante deliberação de seus membros.

§ 3º Compete ao CNCOI auxiliar a CGI na definição das políticas, das normatizações e das estratégias do SISP a serem submetidas ao Conselho Especial do Subsistema de Inteligência de Segurança Pública.

§ 4º O CNCOI se reunirá ordinariamente, a cada três meses e, extraordinariamente, por convocação de seu presidente, lavrando-se ata da reunião que será classificada segundo o sigilo aplicável nos termos da legislação.

§ 5º O CNCOI procederá à elaboração de seu regimento interno.

Art. 17. Compete à Coordenação-Geral de Inteligência da SENASP - CGI, integrar e coordenar as atividades de inteligência de segurança pública no âmbito nacional, obedecidas a política, as diretrizes e as normatizações definidas pelo Conselho Especial do Subsistema de Inteligência de Segurança Pública.

Art. 18. À CGI compete, privativamente:

I - propor, para deliberação do Conselho Especial do Subsistema de Inteligência de Segurança Pública, a política de inteligência de segurança pública, especialmente a sua doutrina, a forma de gestão, o uso dos recursos e as metas de trabalho, bem como coordenar, orientar e supervisionar as atividades de ISP no âmbito nacional;

II - representar, quando designado, o titular do SISP perante as Comunidades Internacional, Nacional e Estaduais de Inteligência e aos demais órgãos e entidades que se dediquem às atividades compreendidas em sua área de competência;

III - articular, de forma permanente, perante os órgãos responsáveis, o provimento contínuo de recursos orçamentários e financeiros necessários à execução das atividades de inteligência de segurança pública;

IV - identificar a necessidade e propor aquisição e distribuição de bens permanentes, de consumo e prestação de serviços destinados às atividades de inteligência de segurança pública, inclusive para as centrais de inteligência de segurança pública e seus centros de monitoramento e análise;

V - oferecer suporte técnico às AI interessadas, para que possam produzir, preservar e recuperar informações por meio das técnicas próprias;

VI - propor e colaborar na elaboração de convênios relacionados às atividades de inteligência de segurança pública;

VII - acompanhar a instalação das centrais de inteligência de segurança pública dos Estados e supervisionar suas atividades;

VIII - propor, para deliberação do Conselho Especial do Subsistema de Inteligência de Segurança Pública, políticas e projetos objetivando:

a) a interceptação de dados, vídeo, telefone e imagem, com o escopo de mantê-las atualizadas para os objetivos da atividade de inteligência de segurança pública;

b) o desenvolvimento, customização, adaptação ou contratação de terceiros para criação de software destinado à concentração das informações de inteligência de segurança pública;

c) o acompanhamento da microfilmagem e ou digitalização de documentos que compõem seu acervo ou legado, atendendo aos requisitos legais e técnicos relacionados à preservação de documentos oficiais sigilosos e manutenção do meio ambiente;

IX - propor a execução de cursos para o treinamento de pessoal no que se refere à execução de atividades de inteligência de segurança pública;

X - controlar, guardar, armazenar, distribuir e zelar pelos dados, informes, informações e conhecimentos relacionados às atividades de inteligência de segurança pública;

XI - acessar de forma irrestrita:

a) dados, informações e conhecimentos, produzidos diretamente ou obtidos por meio de acordos e convênios;

b) procedimentos, observadas as normas legais.

XII - acompanhar e avaliar o desempenho da atividade de inteligência de segurança pública no âmbito nacional;

XIII - planejar, supervisionar, executar e orientar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados ao assessoramento institucional;

XIV - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses da instituição, do Estado e da Sociedade;

XVI - participar da análise das informações de segurança pública a serem divulgadas nos meios de comunicação, visando avaliar as suas conseqüências;

XVII - realizar estudos e pesquisas para o aprimoramento da atividade de inteligência de segurança pública; e

XVIII - atender às demandas do SISBIN, do SISP, da Comunidade de Inteligência e suas agências, observado o canal técnico, e ainda, quando possível, outras de origem externa;

XIX - gerir os bancos de dados e índices nacionais integrantes do SISP;

XX - exercer as atividades que lhe sejam inerentes e correlatas, focando esforços para o compartilhamento de informações, para a geração de conhecimento e a integração no âmbito do SISP, servindo como indutora e fomentadora da atividade de ISP.

XXI - propor políticas e aprovar projetos objetivando:

a) - estruturação das diversas redes de transmissão, comunicação e interceptação de dados, vídeo, telefone e imagem, com o escopo de mantê-las atualizadas na arte existente no mercado;

b) - desenvolvimento, customização, adaptação ou contratação de terceiros para criação de software corporativo ou local destinado à concentração das informações de inteligência de segurança pública, além de proceder diretamente ou pôr meio de terceiros a sua manutenção;

XXII - manter a Escola Nacional de Inteligência de Segurança Pública; bem como executar diretamente ou em parceria, no Brasil ou no exterior, cursos de treinamento, aperfeiçoamento, e especialização de pessoal necessário ao desenvolvimento e execução de atividades e serviços de inteligência de segurança pública, instalação e implantação e operação de redes e sistemas de ISP;

XXIII - atuar, em conjunto com as demais diretorias da SENASP, para o desenvolvimento de sistemas informatizados destinados à identificação, avaliação e acompanhamento do nível de satisfação dos usuários dos recursos informatizados disponibilizados pela SENASP visando atingir os objetivos relacionados à atividade de inteligência de segurança pública;

XIX - controlar, guardar, armazenar, distribuir e zelar pelo patrimônio no que diz respeito à equipamentos, dados, informes, informações e conhecimentos relacionados às atividades de inteligência de segurança pública;

XX - proceder à atualização preventiva e corretiva dos sistemas destinados à atividade de ISP, atualizando os equipamentos e procedendo a qualificação e requalificação de seus agentes;

XXI - solicitar a adoção dos procedimentos licitatórios para compras, em todas as modalidades de licitação, de dispensa, inexigibilidade ou cotação eletrônica de preços para a aquisição de bens permanentes, de consumo ou prestação de serviços relacionados à atividade de inteligência de segurança pública, estabelecendo e manifestando acerca da especificação técnica e emitindo pareceres, quando necessário, podendo, ainda:

a) - acompanhar, sugerir mudanças e controlar o recebimento das faturas relativas à aquisição de software, hardware, rede de transmissão de dados, microfilmagem, digitalização,

certificação digital de documentos e serviços de processamento eletrônico de dados, relacionados à atividades de ISP;

b) - proceder o acompanhamento dos contratos cujo objeto seja bens ou serviços de inteligência de segurança pública;

XV - gerenciar os bancos de dados pertencentes à SENASP ou aqueles em que ela participa em convênio ou em parceria que se relacione com a atividade de ISP;

§ 1º - Competirá, ainda, à CGI, acompanhar e fiscalizar, credenciar e certificar, na forma da regulamentação, as instituições e entidades externas ao SISP que se dediquem a atividades de ISP ou que a esta se relacionem.

Art. 19. A Atividade de Inteligência de Segurança Pública se desenvolverá pelos membros do SISP observando-se os princípios básicos da Atividade de Inteligência, sendo responsabilidade recíproca das instituições integrantes a observância de relações de cooperação mútua, inclusive com a cessão de servidores e ou colaboradores.

6. DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 20. As AI integrantes do SISP, além de produzirem os conhecimentos de que trata esta Resolução e as respectivas doutrinas, em atenção aos respectivos planos de inteligência de segurança pública, se encarregarão de enviar sistematicamente à agência central do SISP um sumário de inteligência, via RENISP.

Parágrafo único - A CGI se encarregará de providenciar os meios para a integração das AI à RENISP e definirá as formas e padrões de utilização da rede.

Art. 21. Os documentos de inteligência de segurança pública, respeitado o canal técnico, tramitarão em conformidade com o procedimento doutrinário e metodologias apropriadas.

Art. 22. As informações destinadas ou prestadas à imprensa possuem natureza diversa das informações de que trata esta Resolução e não se substituem mutuamente, ainda que com igualdade de conteúdo.

Art. 23. As AI poderão constituir ou aderir a redes locais ou regionais de informação e inteligência de segurança pública, devendo informar o que produzirem ou recepcionarem à Agência Central.

Art. 24. Fica vedado o exercício de qualquer atividade de informação e inteligência de segurança pública no âmbito do SISP, diversa da estabelecida nesta Resolução, caso em que, se executadas, serão consideradas irregulares, sujeitando-se os responsáveis às conseqüências legais.

§ 1º A regularidade do exercício de qualquer atividade de informação e inteligência de segurança pública no âmbito do SISP fica sujeita ao cumprimento das normas previstas na legislação aplicável e nesta Resolução.

§ 2º A execução de atividade de informação e inteligência de segurança pública que esteja ocorrendo no âmbito do SISP, no prazo de cento e oitenta dias, deverá se adequar às normas de que trata esta Resolução.

Art. 25. Compete ao Coordenador-Geral de Inteligência/SENASP acompanhar o cumprimento das normas estabelecidas nesta Resolução e na DNISP e apurar, diretamente ou por meio de delegação, a ocorrência de irregularidade, adotando providências para a responsabilização cabível.

§ 1º As deliberações do Conselho Especial do Subsistema de Inteligência de Segurança Pública serão difundidas de acordo com a legislação que rege a matéria e deverão ser cumpridas por todas as AI integrantes do SISP.

Art. 26. Fica proibida, sob pena de responsabilização administrativa, civil e criminal, a difusão das formas e métodos operacionais das ações de inteligência de segurança pública fora do SISP.

Art. 27. A Coordenação-Geral de Inteligência/SENASP é a gestora dos sistemas informatizados integrantes do SISP, devendo definir, a política de acesso aos dados neles contidos.

Art. 28. A unidade de Orçamento e Finanças da SENASP promoverá ações para assegurar a provisão no orçamento anual do Ministério de Justiça, em rubrica específica, dos recursos necessários à execução das atividades a cargo da CGI.

Art. 29. Esta Resolução entrará em vigor na data de sua publicação.

7. COMENTÁRIOS

A atividade de inteligência vai muito além das ações de Estado e de Governo, envolvendo um conjunto de ações interligadas que tem como propósito a busca da certeza e

verdade sobre os fatos que possam, direta ou indiretamente afetar a vida das pessoas, da sociedade e do próprio governo, principalmente no sentido de se evitarem situações de crise ou de riscos reais ou potenciais. A complexidade das atividades de segurança pública e suas próprias estruturas, torna-se imperativa uma perspectiva multiagencial e interdisciplinar que leve em consideração outras formas de visão sobre as coisas e fatos, quer sejam pretéritos, presentes ou de possíveis cenários futuros, de maneira que áreas distintas do conhecimento possam levar à construção de uma oncologia para a atividade de inteligência em segurança pública.

No âmbito da segurança pública foi criado o subsistema de inteligência de Segurança Pública (SISP) pelo decreto 3.695, de 21 de dezembro de 2000, o qual tem por finalidade:

“coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e os estaduais de informações que subsidiem a tomada de decisões neste campo”.

O regulamento do subsistema de Inteligência de Segurança Pública – SISP prevê sua constituição por rede própria e responsável pelo processo de coordenação e integração das atividades de inteligência de segurança pública no âmbito do território nacional, e estabelece que tem por objetivo:

“fornecer subsídios informacionais aos respectivos governos para a tomada de decisões no campo da segurança pública, mediante a obtenção, análise e disseminação da informação útil, e salvaguarda da informação contra acessos não autorizados”.

A ISP é exercida em perfeita sintonia com as suas finalidades e sob a égide de determinados princípios, de forma que a aplicação de um deles não acarrete prejuízo no emprego dos demais. Esses princípios são as posições diretoras, as bases, os fundamentos, os alicerces, os pilares que orientam e definem os caminhos da atividade. É constituída como um serviço à causa pública, submetida aos princípios constitucionais da legalidade, da impessoalidade, moralidade e da eficiência, e, em especial, tendo em vista a observância da ética, dos direitos e garantias individuais e sociais e o estado democrático de direito.

A atividade possui dois ramos a inteligência e a contra inteligência. Vale resaltar que os dois devem ser compreendidos como indissolivelmente ligados; são partes de um todo,

não possuindo limites precisos, uma vez que se interpenetram, se inter-relacionam e inter-relacionam e interdependem.

8. CONSIDERAÇÕES FINAIS

Nesse patamar, grupos antagônicos têm interesse em saber como se desdobram as operações de segurança pública, deste modo a arquitetarem suas próprias ações; para fazer frente a essas ameaças, a atividade, estrutura e doutrina de contrainteligência deve ser aplicada e fortalecida para que não ocorra prejuízo aos interesses, instalações, equipamentos e pessoal das instituições.

As ações de grupos com intenções voltadas para a atividade criminal desafiam e ajudam a redefinir, constantemente, a distribuição e emprego das forças policiais disponíveis. As atividades que podem comprometer ou superar as medidas de salvaguarda adotadas na segurança pública compreendem, mas não estão limitadas a: obtenção de dados ou conhecimentos sensíveis, espionagem, sabotagem e propaganda adversa. A força da atividade de contrainteligência reside em sua capacidade de reduzir e anular vulnerabilidades que possam comprometer os bens do Estado (físicos e intelectuais), empregados na segurança pública.

Frente ao que antecede, a contrainteligência, utilizada em outros tempos apenas nos campos de batalha, hoje, mostra-se de importância fundamental na esfera da segurança pública. Sua doutrina e princípios, sendo observados e aplicados de maneira correta, contribuem de forma valorosa para a proteção da sociedade, ao dificultar demasiadamente o acesso às informações sigilosas dos órgãos de segurança pública.

A forma de organização da atividade de Inteligência em sistemas e subsistemas resulta em fluxo constante de informações para as ações de segurança.

A criminalidade através do crime organizado usa recursos tecnológicos sofisticados nas ações delituosas, diversas formas de comunicação, mostra uma previsão sobre o sistema e torna-se desafios para os órgãos incumbidos da investigação criminal.

A doutrina de Inteligência Policial do Departamento de Polícia Federal (DPF) define que a produção de conhecimento nesta área é realizada em três níveis – estratégico, tático e operacional – e destina-se a “facilitar o processo decisório de gestão policial bem como para subsidiar o trabalho de Polícia Judiciária na produção de provas e revelação de evidências sobre autoria de crimes.”

O nível estratégico destina-se ao assessoramento em mais alto grau, tratando de assuntos de maior complexidade que dizem respeito ao órgão como um todo, com o objetivo de possibilitar a adoção de medidas preventivas e a tomada de decisões administrativas por parte da Direção-Geral do DPF. Baseado em estimativas de evolução de determinados tipos penais e/ou da criminalidade, estas ações são projetadas para vigorarem por um espaço temporal de longo prazo.

A atividade de inteligência policial em nível tático aborda uma determinada área de interesse do órgão e não a instituição como um todo, objetivando subsidiar a elaboração de políticas internas de atuação para o enfrentamento de determinado fenômeno criminal. Estas políticas são projetadas para um espaço temporal de médio prazo.

Finalmente o nível operacional tem como objetivo a tomada de decisões relativas à investigação criminal, que é a atividade-fim do órgão, com foco específico na formação de escopo probatório para a apuração e comprovação de autoria e materialidade de ilícito penal, possuindo assim, efeito imediato.

9. REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Raimundo Teixeira de. *História Secreta dos Serviços de Inteligência*. São Luís: CEADEMA, 2004.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Resolução nº 01, de 15 de julho de 2009.

CEPIK, Marco A. C. **Espionagem e Democracia**: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV, 2003. 230 p.

DEPARTAMENTO DE POLÍCIA FEDERAL, Manual de Inteligência Policial – Outubro de 2009.

BRAGA, Pedro Luis de Araujo. O Papel da Atividade de Inteligência em uma Sociedade Democrática. Rio de Janeiro: Divisão de Assuntos de Inteligência/ESG — 1998.

BRASIL, Escola Superior de Guerra. Fundamentos doutrinários Básicos. Rio de Janeiro: ESG, 2000.

KENT, Sherman. Informações Estratégicas. Rio de Janeiro: Biblioteca do Exército, 1967.

OLIVEIRA, Lúcio Sérgio Porto. A História da Atividade de Inteligência no Brasil. Agência Brasileira de Inteligência (ABIN).

GOMES, Rodrigo Carneiro. Prevenir o crime organizado: Inteligência policial, democracia e difusão do conhecimento. *Revista do Tribunal Regional Federal da 1ª Região*, v. 21, n. 8, ago. 2009.

PLATT, Washington. Strategic Intelligence Production. New York: Frederick A. Praeger Inc. 1962.

FERRO JÚNIOR, Celso Moreira. *A atividade de inteligencia na policia civil do DF*. MBA Segurança Pública e Defesa Social, disciplina Atividade de inteligência e contra-inteligência policial. Apresentação áudio-visual. Brasília, União Pioneirade Integração Social (UPIS), 2005.

TZUN, Sun. A Arte da Guerra. 3. Ed. Rio de Janeiro: Vozes, 2013.

HOBBS, Thomas, 1588-1679. *Leviatã, ou Matéria, forma e poder de um Estado Eclesiástico e Civil*. 2ª Ed. São Paulo: Martin Claret, 2012.

RESOLUÇÃO Nº 1, de 15 de julho de 2009, regulamenta o Subsistema de Inteligência de Segurança Pública – SISP.

FERREIRA, Romeu Antônio. Inteligência Estratégica. In. *Conferência para o curso de pós-graduação em estratégia militar para gestão de negócios*, Ribeirão Preto, SP: FAAP: 2011.

STANY, Coronel M. D. & Arneson, Tenente-coronel C. W. Jr. (n.d.). FM 100-6 Operações de Informações. Military Review.