UNIVERSIDADE DO SUL DE SANTA CATARINA
ANTONIO VELOSO ROCHA

INTELIGÊNCIA DE DEFESA

Maceió, AL, Brasil
2018

ANTONIO VELOSO ROCHA

INTELIGÊNCIA DE DEFESA

Monografia apresentada ao Curso de Pós-Graduação *Lato Sensu* em Inteligência de Segurança, da Universidade do Sul de Santa Catarina, como requisito à obtenção do título de Especialista em Inteligência de Segurança.

Orientação: Prof. Luiz Otávio Botelho Lento, MSc.

Maceió, AL, Brasil
2018

ANTONIO VELOSO ROCHA

INTELIGÊNCIA DE DEFESA

Esta Monografia foi julgada adequada à obtenção do título de Especialista em Inteligência de Segurança e aprovado em sua forma final pelo Curso de Pós-Graduação *Lato Sensu* em Inteligência de Segurança, da Universidade do Sul de Santa Catarina.

Maceió, 23 de julho de 2018.

Professor orientador: Luiz Otávio Botelho Lento, MSc.

Universidade do Sul de Santa Catarina

Prof. Dr. Camel André de Godoy Farah

Universidade do Sul de Santa Catarina

Universidade do Sul de Santa Catarina

DEDICATÓRIA

A Deus toda glória, pois tudo é Dele, por Ele e para Ele.

AGRADECIMENTOS

Ao meu orientador, à minha família pelo apoio e motivação dado para os estudos e à minha esposa pela paciência, atenção e inspiração e a todos aqueles que de alguma forma contribuíram para essa conquista.

RESUMO

O tema em estudo propicia a elucidação do que vem a ser Inteligência de Defesa, que relação ela tem com tomadas de decisões e que importância exerce essa atividade na soberania de uma nação. A Atividade de Inteligência é instrumento exclusivo do estado, à disposição dos sucessivos governos para assessorá-los na tomada de decisões em defesa da nação, das instituições e dos interesses nacionais. A principal característica da Inteligência de Defesa é a capacidade técnico-militar e é desenvolvida com a finalidade de produzir e salvaguardar conhecimentos de interesse da defesa.

Palavras-chave: Inteligência. Inteligência de Defesa. Inteligência Militar.

ABSTRACT

The theme study provides the elucidation of what is to be Defense Intelligence, what relationship it has with making decisions and how important exercise this activity in the sovereignty of a nation. Intelligence Activity is unique instrument status available to successive governments to advise them in making national defense decisions, institutions and national interests. Its main feature is the military-technical expertise and is developed with the purpose of producing and safeguard the defense of the interests of knowledge.

Keywords: Intelligence. Defense Intelligence. Military Intelligence.

SUMÁRIO

1 INTRODUÇÃO

A atividade de inteligência, seja para atender a curiosidade sobre o desconhecido ou a busca do conhecimento para atender interesses pessoais ou das nações, sempre foi percebida como essencial, na guerra e na diplomacia, para a governabilidade e garantia de segurança. A necessidade de se dispor de informações sobre ambiência física, temporal, de costumes, de potencial e de intencionalidade do inimigo, tem seus primeiros relatos na Bíblia, e caracteriza a busca de conhecimentos e a sua utilização como instrumento de poder.

Os conflitos atuais tendem a ser limitados, não declarados, convencionais ou não, e de duração imprevisível. As ameaças são difusas e também imprevisíveis. O combate ao terrorismo, a proteção da sociedade contra as armas de destruição em massa, a participação em missões de manutenção e/ou imposição da paz sob a égide de organismos internacionais, e o controle de contingentes populacionais ou de recursos escassos demandam capacidades às Forças Armadas que permitam respostas imediatas e pontuais, com o mínimo de efeitos colaterais.

As operações militares podem se desenvolver em áreas habitadas e a preservação de vidas humanas, imersas ou não em conflitos ou catástrofes, caracteriza o emprego das atividades de Inteligência.

Ao longo do processo de planejamento e de execução da ação política, as autoridades decisoras, em qualquer nível hierárquico, necessitam de conhecimentos que lhes permitam decidir, adequadamente, sobre questões de sua competência. Dessa forma, os governantes contam, no âmbito da Defesa, com o assessoramento da inteligência para a condução do processo decisório. Além disso, o planejamento do emprego estratégico de forças militares exige o acompanhamento regular e permanente das conjunturas nacional e internacional, de forma a possibilitar a previsão ou antecipação de eventos que, por sua natureza, o afetem.

Dentro desse cenário de evolução da atividade de inteligência em defesa dos Estados e de seus interesses, tecnologias foram desenvolvidades por meio da atividade de inteligência de defesa.

Este trabalho, portanto, orientar-se-á no sentido de definir a atividade de inteligência de defesa, diferenciá-la da atividade de inteligência de segurança pública, identificar suas funções e apresentar tecnologias desenvolvidas como meios de defesa do Estado a partir de conhecimentos de inteligência contra ameaças reais e/ou potenciais.

Diante das possiblidades de emprego das forças armadas em operações militares para asssegurar a defesa e interesses nacionais, um fator que permanece em evidência é a atividade

de inteligência de defesa, por meio da qual se obtém conhecimentos relevantes para assegurar aos Estados vantagem estratégica.

A partir dessas considerações, visa-se responder as seguintes perguntas: o que é a Atividade de Inteligência de Defesa? Quais disciplinas podem ser empregadas na atividade de Inteligência de Defesa? Como a Inteligência de Defesa pode auxiliar a Segurança Pública?

No que se refere à metodologia, este trabalho baseia-se em fontes primárias e secundárias. Particularmente em manuais militares e estudos publicados por organizações governamentais como Ministério da Defesa e Forças Armadas, Agência Brasileira de Inteligência e Departamento de Defesa dos Estados Unidos. Informações foram obtidas através de livros, manuais e artigos. Para compreender a origem, atividades e emprego da inteligência de defesa, este trabalho revisou literaturas no contexto da atividade e operações de inteligência. Para este fim, foi feito um estudo exploratório sobre a finalidade, as possibilidades, disciplinas, estruturas e emprego da inteligência de defesa, sendo estritamente descritivo.

2 INTELIGÊNCIA DE DEFESA

2.1 CONTEXTUALIZAÇÃO

Os países, em tempos de crise ou não, na condução das questões internas, externas e na garantia de sua segurança e de seus interesses, necessitam conhecer os possíveis cenários e as variáveis que os compõem, bem como suas implicações, desejadas ou indesejadas. Os tomadores de decisão necessitam de informações confiáveis, relevantes e oportunas que possam auxiliá-los na condução de suas atribuições.

O conjunto desses cenários moldam o ambiente estratégico no qual a Atividade de Inteligência também atua e sobre o qual o Estado é instado a oferecer respostas tanto a desafios já identificados quanto respostas àqueles inéditos, derivados das novas circunstâncias.

Para fazer frente a essa conjuntura tão dinâmica e difícil, ampliam-se os investimentos em Inteligência e Defesa no mundo. Os serviços e os sistemas de Inteligência se desenvolvem e se profissionalizam como reflexo do aumento da complexidade dos ambientes interno e externo, em consonância com as características de cada país, seu arranjo institucional, suas prioridades e suas necessidades de informações

Inteligência refere-se a informações relevantes para a política de formulação e implementação de um governo para promover seus interesses de segurança nacional e para lidar com interesses de adversários atuais ou potenciais. Frequentemente mais importante, a inteligência de defesa tem a ver com as questões militares, como os planos do adversário para ação militar. Os inimigos potenciais ou atuais geralmente fazem o possível para manter esse tipo de informação em segredo.

Outros tipos de informações secretas podem ser importantes, por exemplo, informações sobre as atividades e intenções diplomáticas de outros países, bem como informações sobre suas atividades de inteligência.

Como atividade, inteligência compreende a coleta e análise de informações de inteligência - informações relevantes para a formulação e implementação da política de segurança nacional - também incluem atividades para combater as atividades de inteligência dos adversários, seja negando-lhes acesso à informação ou enganando-os sobre os fatos ou seu significado.

O termo "inteligência" também se refere às organizações que realizam essas atividades. Uma das características mais notáveis dessas organizações é o sigilo com que suas atividades devem ser conduzidas. Muitos regras relativas ao acesso à informação decorrem deste requisito. Como as agências de inteligência são organizadas para aumentar sua capacidade de sigilo, elas também podem receber, juntamente com suas funções de obtenção ou disseminação de informações, a responsabilidade de realizar atividades secretas voltadas para o cumprimento dos objetivos de política externa de seu governo.

No combate atual, a Inteligência não é empregada somente na mera descrição das forças militares oponentes e de suas capacidades de combate. Deve possibilitar, também, uma ampla compreensão dos agentes presentes no ambiente operacional: cultura, motivações, perspectivas, objetivos, aprovação popular e apoio que recebe ou pode receber.

A inteligência de defesa compreende o conjunto de atividades, tarefas e sistemas inter-relacionados empregados para assegurar compreensão sobre o ambiente operacional, as ameaças (atuais e potenciais), os oponentes, o terreno e as considerações civis.

Por meio da Inteligência de Defesa, busca-se que todos os planejamentos de inteligência, estratégico, operacional e tático, dos diversos centros decisores e demandam diferentes processos e produtos, a fim de alcançar seus objetivos

No nível estratégico, as condicionantes e as diretrizes políticas são transformadas em ações estratégicas, voltadas para os ambientes externo e interno, a serem desenvolvidas setorialmente pelos diferentes ministérios, de maneira coordenada com as ações da expressão

militar. O nível estratégico de planejamento desdobra-se em todas as expressões do Poder Nacional.

No nível operacional, a inteligência de defesa centra seus esforços na busca de conhecimentos sobre o Teatro de Operações e as forças oponentes que podem atuar sobre o espaço de batalha. A Inteligência de Defesa, assim, analisa e avalia a ameaça real ou potencial quanto à sua importância, intensidade e magnitude.

No nível tático, a Inteligência de Defesa está voltada para o apoio ao planejamento e condução das operações militares.

As informações precisas são condição essencial para o emprego adequado dos meios militares. A Inteligência deve ser desenvolvida desde o tempo de paz, pois é ela que possibilita superar as incertezas. É da sua vertente prospectiva que procedem aos melhores resultados, permitindo o delineamento dos cursos de ação possíveis e os seus desdobramentos. A identificação das ameaças é o primeiro resultado da atividade da Inteligência de Defesa.

2.2 CONCEITOS E DEFINIÇÕES

Inteligência é um conjunto que forma todas as características intelectuais de um indivíduo, ou seja, a faculdade de conhecer, compreender, raciocinar, pensar e interpretar. A inteligência é uma das principais distinções entre o ser humano e os outros animais.

Shulsky (1992) identifica Inteligência como a informação relevante para se formular e implementar políticas voltadas aos interesses de segurança nacional, e lidar com as ameaças atuais ou potenciais. Já como atividade, a Inteligência compreende a coleta e a análise de informações e inclui atividades destinadas a conter as ações de Inteligência adversas.

De acordo com o art. 2° da Lei nº 9.883/99, entende-se por Inteligência “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”. Contra-Inteligência, por sua vez, é a atividade voltada à “neutralização da Inteligência adversa” (art. 3°) – a qual pode ser tanto de governos como de organizações privadas (BRASIL, 1999).

Etimologicamente, a palavra "inteligência" se originou a partir do latim *intelligentia*, oriundo de *intelligere*, em que o prefixo *inter* significa "entre", e *legere* quer dizer "escolha". Assim sendo, o significado original deste termo faz referência a capacidade de escolha de um indivíduo entre as várias possibilidades ou opções que lhe são apresentadas.

Os conceitos foram obtidos do manual de inteligência americano JP 2-0 - *Joint Intelligence,* da Política de Defesa Nacional e do Glossário das Forças Armadas.

Atividade de Inteligência – Atividade baseada em processo mental, que tem por finalidade produzir e salvaguardar conhecimento de interesse. Desdobra-se em dois grandes segmentos: de Inteligência - objetivamente voltado para a produção de conhecimentos; e de Contra-Inteligência - objetivamente voltado para a salvaguarda de conhecimentos.

Contra-Inteligência – Ramo da atividade de inteligência voltado para a detecção, identificação, neutralização, obstrução e prevenção da atuação da Inteligência adversa e das ações de qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de tecnologia da informação) de interesse da sociedade e do Estado.

Defesa Nacional – Conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas.

Inteligência – Ramo da Atividade de Inteligência voltado para a obtenção e a análise de dados e para a produção e a disseminação de conhecimentos de Inteligência, 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 da sociedade e do Estado.

Inteligência Estratégica - Inteligência necessária para a formação de políticas e planos militares a nível nacional e internacional.

Inteligência Militar – Atividade de Inteligência de natureza técnico-militar, especializada e permanente que visa a produzir conhecimentos de interesse do comandante de qualquer nível hierárquico e proteger os conhecimentos sensíveis, as instalações e pessoal, contra as ações de serviços de inteligência do oponente ou do inimigo.

Inteligência Operacional – Atividade militar especializada, com base em processo mental, permanentemente exercida, com a finalidade de produzir e salvaguardar conhecimento requerido para planejar, conduzir e sustentar operações militares.

Inteligência Tática - Inteligência necessária para o planejamento e condução de operações táticas.

Segurança – 1. Condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. 2. Sentimento de garantia necessária e indispensável a uma sociedade e a cada um dos seus integrantes, contra ameaças de qualquer natureza. Condição que resulta do

estabelecimento e conservação de medidas de proteção que assegurem um estado de inviolabilidade contra atos ou influências hostis.

Segurança Externa – Garantia alcançada pela aplicação do Poder Nacional, sob todas as suas formas e expressões, de maneira global, sistemática, permanente e gradual, contra os antagonismos ou pressões de qualquer origem, forma ou natureza, que se manifestem ou possam manifestar-se no domínio das relações internacionais. É integrada na Segurança Nacional.

Segurança Interna – Grau de garantia integrada na segurança nacional, que o Estado proporciona à Nação contra antagonismos ou pressões de qualquer origem, forma ou natureza, que se manifestem ou produzam efeitos no âmbito interno do País.

Segurança Nacional – Condição que permite ao país a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais.

Segurança Pública – Garantia que o Estado proporciona à Nação, a fim de assegurar a ordem pública, ou seja, ausência de prejuízo aos direitos do cidadão, pelo eficiente funcionamento dos órgãos do Estado

Soberania – 1. Última instância do poder de mando do Estado nacional seja para os efeitos externos, seja para os internos. É, também, a supremacia da ordem jurídica do Estado nacional em todo o território. Doutrinariamente, é entendida como absoluta, indivisível, inalienável e imprescritível. 2. Elemento formal, poder supremo de que se acha revestida a autoridade do Estado, poder de auto-determinar-se, auto-governar-se, sem interferência de nenhum outro poder governando e disciplinando juridicamente a população que se encontra no seu território e mantendo relações com outros estados.

2.3 DISCIPLINAS DA INTELIGÊNCIA DE DEFESA

As disciplinas de Inteligência compreendem os meios, sistemas e procedimentos utilizados para observar, explorar, armazenar e difundir informação referente à situação, ameaças e outros fatores das operações de defesa. As disciplinas de Inteligência classificam-se de acordo com a natureza da fonte ou do órgão de obtenção que a explora.

O manual de inteligência americano JP 2-0 - *Joint Intelligence* classifica as disciplinas de Inteligência de Defesa como: inteligência de fontes humanas, inteligência de

imagens, inteligência por assinatura de alvos, inteligência de sinais, inteligência técnica e inteligência de fontes abertas.

2.3.1 Inteligência de Fontes Humanas

A Inteligência de Fontes Humanas (*Human Intelligence - HUMINT*) é a Inteligência que provêm de dados e informações obtidas por fontes humanas.

É a coleta por meio de operadores *HUMINT* de informações de pessoas e multimídia estrangeiras para identificar elementos, intenções, composição, força, vulnerabilidades, dispositivos, táticas, equipamentos, pessoal e capacidades. pessoa de quem se obtém a informação para posterior produção de conhecimento de Inteligência. Essas fontes podem ser amigas, neutras ou hostis, podendo ser prisioneiro de guerra, refugiado, deslocado, população local, forças próprias ou amigas e membros de instituições governamentais ou organizações de qualquer tipo.

2.3.2 Inteligência de Imagens

A Inteligência de imagem (*Imagery Intelligence - IMINT*) é proveniente da análise de imagens fixas e de vídeo, obtidas por meio de fotografia, radar e sensor electro-óptico de tipo térmico, infravermelho ou de amplo espectro, que podem estar em terra ou situados em plataformas navais, aéreas ou espaciais.

A Inteligência de Imagens permite a visualização da área de operações em tempo real. Os recursos visuais podem ser nacionais, civis e comerciais.

Os sistemas nacionais são desenvolvidos especificamente para dar assistência aos governantes, agências nacionais e forças militares. Esses sistemas atendem às demandas da nação e dos forças militares envolvidas nas operações.

Os sistemas de imagens civis são normalmente financiados pelo governo em termos de construção, lançamento e operação do sistema. Em muitos casos, mas não em todos, as agências que operam esses sistemas de imagens também processam, distribuem e arquivam os dados de imagens.

Empresas comerciais constroem, lançam e operam sistemas de imagens para obter lucro. O controle governamental dos sistemas comerciais protege as informações relativas às operações militares da exploração estrangeira dos sistemas.

2.3.3 Inteligência por Assinatura de Alvos

A Inteligência por Assinatura de Alvos (Measurement and Signature Intelligence - MASINT) é a Inteligência proveniente da análise científica e técnica de dados obtidos de fontes emissoras com o propósito de descrever, detectar, mapear, localizar e identificar alvos e objetos fixos e dinâmicos

Os meios MASINT têm capacidades únicas para detectar lançamento de mísseis, detectar e seguir plataformas aéreas, embarcações e veículos em geral, colaborar com a avaliação dos efeitos do combate e na detecção e monitoramento de chuva radioativa provocada por armamento nuclear. Os dados obtidos pela MASINT são dirigidos para os sistemas de Inteligência dos níveis estratégico e tático.

2.3.4 Inteligência de Sinais

A Inteligência de Sinais (*Signals Intelligence* - *SIGINT*) é toda Inteligência derivada do espectro eletromagnéticos. Subdivide-se em:

a) Inteligência de Comunicações (*COMINT*) – é a Inteligência derivada de comunicações eletromagnéticas e sistemas de comunicações; inteligência obtida de dados adquiridos pela interceptação de comunicações e dados de forças adversas;

b) Inteligência Eletrônica (*ELINT*) – é a Inteligência decorrente de transmissões eletromagnéticas de não-comunicações, tais como as produzidas por radares, por sistemas de orientação de mísseis, lasers, dispositivos infravermelhos ou qualquer outro equipamento que produza emissões no espectro eletromagnético; e

c) Inteligência de Sinais de Instrumentos Estrangeiros (*FISINT*) – é a informação técnica e Inteligência derivadas da interceptação de emissões eletromagnéticas estrangeiras associadas ao teste e à implantação operacional de sistemas aeroespaciais, de superfície e de subsuperfície de fora da nação.

O *SIGINT* fornece inteligência sobre recursos, disposição, composição e intenções de ameaças além de fornecer informações de alvo para o emprego de armas com efeitos letais e não letais.

2.3.5 Inteligência Técnica

A Inteligência Técnica (*Technical Intelligence* - *TECHINT*) é a Inteligência obtida da análise de equipamentos tecnológicos e de material com possibilidade de utilização militar.

O papel da *TECHINT* é garantir que a nação compreenda toda a capacidade tecnológica da ameaça para evitar a surpresa tecnológica e avaliar novas capacidades técnicas e científicas, de maneira que se possa desenvolver contramedidas adequadas que neutralizem as vantagens que essas capacidades proporcionam a quem as utilize.

A *TECHINT* assegura que as forças armadas de um país mantenham vantagem tecnológica contra qualquer adversário e fornece suporte personalizado, oportuno e preciso nas operações militares. Isso inclui o fornecimento de inteligência, informações e treinamento das forças militares a sistemas de armas estrangeiros a ponto de permitir seu uso.

2.3.6 Inteligência de Fontes Abertas

A Inteligência de Fontes Abertas (Open Source Intelligence - OSINT) é a Inteligência baseada em informações coletadas de fontes de caráter público, tais como os meios de comunicação (rádio, televisão e jornais), propaganda de estado, periódicos técnicos, internet, manuais técnicos e livros.

A comunidade de Inteligência sempre usou fontes abertas na produção de conhecimento. A legislação sobre o acesso à informação produzida por órgãos públicos, ao redor do mundo, possibilita a obtenção de dados e informações sensíveis de Estados, organizações e instituições, o que é facilitado pela internet. A OSINT é a fonte básica de Inteligência.

2.4 CASOS PRÁTICOS

2.4.1 Míssil *Patriot*

O *Patriot* é um sistema de defesa móvel, baseado em terra, de longo alcance e alta altitude, implantado pelos Estados Unidos e outras nações para combater mísseis balísticos táticos, mísseis de cruzeiro e aeronaves avançadas. O Patriot (MIM-104) é produzido pela Raytheon em Massachusetts e pela Lockheed Martin Missiles and Fire Control na Flórida.

Os sistemas de mísseis *Patriot* foram testados em operações de combate no Oriente Médio durante a Operação Tempestade no Deserto e a Operação Iraqi Freedom, e foram usados para derrubar mísseis balísticos táticos em operações de combate.

Nos últimos anos, numerosos países do Oriente Médio implantaram sistemas *Patriot* para proteger suas fronteiras e proteger suas tropas da ameaça de mísseis balísticos. Entre janeiro de 2013 e o final de 2015, a Turquia hospedou cinco baterias da OTAN *Patriot* para aumentar a capacidade de defesa antimísseis do país contra a ameaça de mísseis balísticos do conflito na Síria. Desde 2012, essas baterias *Patriot* detectaram várias centenas de lançamentos de mísseis balísticos na Síria e rastrearam sua trajetória de vôo, certificando-se de que eles não representam uma ameaça para civis turcos ou forças militares desdobradas ao longo da fronteira.

Os Emirados Árabes Unidos (EAU) e a Arábia Saudita atualmente possuem sistemas de defesa antimísseis *Patriot* para proteger suas tropas destacadas com a coalizão liderada pelos sauditas no Iêmen e populações civis ao longo da fronteira Iêmen / Arábia Saudita. Desde o início do conflito, os rebeldes houthi dispararam vários mísseis *Scud* e *Tochka* nas forças de coalizão sauditas, algumas das quais foram interceptadas por baterias *Patriot*, incluindo as recentemente lançadas no aeroporto da capital da Arábia Saudita, em Riad.

O Japão, a Coreia do Sul e os Estados Unidos atualmente implantaram sistemas *Patriot* no Pacífico para proteger suas populações e/ou tropas desdobradas. Os Estados Unidos colocaram baterias *Patriot* na Coréia do Sul desde 1994 para proteger contra os mísseis balísticos e de cruzeiro de curto alcance da Coréia do Norte, além das baterias *Patriot* usadas pela Coréia do Sul como parte de seu sistema de defesa antimíssil. O Japão também usa baterias *Patriot* como parte de suas defesas antimísseis em torno de Tóquio.

2.4.2 Operação Lança de Netuno

A morte de Osama bin Laden, um dos membros sauditas da família bin Laden e líder-fundador do grupo terrorista al-Qaeda, ocorreu durante a Operação Lança de Neptuno, codinome usado pelas tropas estadunidenses para referir-se a ele, em 1 de maio de 2011. Nesse dia, o então presidente dos Estados Unidos, Barack Obama, informou em conferência à imprensa que bin Laden havia morrido na cidade paquistanesa de Abbottabad. Segundo a versão oficial, Osama teria sido capturado e morto em um esconderijo nos arredores da cidade por forças da *Joint Special Operations Command* em conjunção com a Agência Central de Inteligência Americana, e que o governo desse país colaborou para a localização do paradeiro do terrorista. O cadáver foi mantido sob custódia militar e amostras de DNA, que foram comparadas com as amostras de uma irmã dele, a qual morrera de câncer no cérebro,

confirmaram sua identidade; outros métodos, como reconhecimento facial, garantiram que o capturado era mesmo o terrorista.

Autoridades de inteligência norte-americanas descobriram o paradeiro do terrorista acompanhando as informações de um de seus mensageiros. As primeiras informações foram recolhidas junto de presos em Guantánamo, descobrindo que ele era um protegido de Khalid Sheikh Mohammed. Em 2007, as autoridades dos Estados Unidos descobriram o verdadeiro nome dele e, em 2009, onde morava. Imagens de satélites e relatos da Agência Central de Inteligência americana ajudaram a confirmar a localização correta de Osama e dos outros moradores da mansão onde morava em Abbottabad, no Paquistão.

2.5 PRODUTOS DA ATIVIDADE DE INTELIGÊNCIA DE DEFESA

Os produtos de inteligência de defesa são geralmente colocados em uma das oito categorias de produção: alerta, atual, militar, alvo, científico e técnico, contra-inteligência, inteligência de identidade e inteligência de estimativa. As categorias distinguem-se umas das outras principalmente pelo propósito para o qual a inteligência é produzida.

O manual de inteligência americano JP 2-0 - *Joint Intelligence* (2013) classifica como produtos da Inteligência de Defesa: inteligência de alerta, inteligência atual, inteligência militar, inteligência de alvo, inteligência científica e técnica, contra-inteligência, inteligência de estimativa e inteligência de identidade.

2.5.1 Inteligência de alerta

Fornece uma comunicação distinta para um tomador de decisões sobre ameaças contra a segurança, interesses ou cidadãos nacionais. Carrega um sentido de urgência, implicando que o tomador de decisão deve tomar medidas para deter ou mitigar impacto da ameaça. A análise de advertência enfoca as oportunidades de combater somente as ameaças que têm efeitos prejudiciais para a nação. Isso inclui as forças armadas ou ciclos de decisões políticas, infraestrutura ou perda de governança. A Inteligência de Defesa reconhece dois tipos de advertência: emergentes e duradouros. Os problemas de alerta podem ser formalizados como “permanente” baseado em uma avaliação de risco para a segurança nacional e orientação do planejamento. Este último é geralmente ligado a planos de contingência, que são definidos, e ameaças potenciais aos interesses nacionais.

2.5.2 Inteligência atual

A inteligência atual fornece suporte atualizado para operação contínua. Envolve a integração de informações e informações sensíveis ao tempo e de todas as fontes em relatórios objetivos e concisos sobre a situação atual em uma área específica. O termo “atual” é relativo às sensibilidades de tempo do tomador de decisão e ao contexto do tipo de operação que está sendo suportado. Por exemplo, em alguns contextos, a inteligência pode ser considerada “atual”, enquanto outras circunstâncias podem exigir inteligência em tempo quase real.

2.5.3 Inteligência militar

Centra-se nas capacidades das forças armadas de países e organizações estrangeiras, incluindo atores não-estatais e outros tópicos que poderiam afetar potencialmente as operações militares nacionais ou multinacionais. Esta ampla categoria de inteligência é normalmente associada ao planejamento de longo prazo, e tenta identificar e monitorar as tendências que afetam a segurança nacional para facilitar a aplicação dos finitos recursos. É adaptada para missões de forças conjuntas subordinadas específicas e inclui informações sobre a organização, operações, instalações e capacidades de forças militares estrangeiras.

2.5.4. Inteligência de alvo

A inteligência do alvo retrata e localiza os componentes de um alvo ou complexo de alvos, redes e infra-estrutura de suporte, e indica sua vulnerabilidade e importância relativa para o adversário. A inteligência alvo inclui a caracterização de um alvo e indica sua vulnerabilidade, colocação em sistemas maiores ou redes, e importância relativa para o adversário. A caracterização inclui análises de atributos físicos e virtuais (incluindo os dados biográficos, biológicos, comportamentais e atributos de reputação de alvos humanos para apoiar o uso de armas) e assinaturas (para apoiar detecção de alvo e identificação positiva). A inteligência de alvo também inclui a avaliação dos danos de batalha composta por avaliação de dano / mudança física, avaliação funcional, avaliação de danos / alterações e avaliação funcional do sistema de armas resultante da aplicação da força letal ou não-letal.

2.5.5 Inteligência científica e técnica

Examina o desenvolvimento estrangeiro em ciências básicas e aplicadas e tecnologias com potencial bélico, particularmente melhorias nos sistemas de armas. Inclui características, capacidades, vulnerabilidades e limitações dos sistemas de armas, subsistemas e material associado, bem como pesquisa e desenvolvimento relacionados. Também aborda sistemas globais de armas, análise de táticas e eficácia de equipamentos.

2.5.6 Contra-inteligência

São informações coletadas e atividades conduzidas para identificar, enganar, explorar, perturbar ou proteger contra espionagem, outras atividades de inteligência, sabotagem ou assassinatos conduzidos em nome de potências, organizações ou pessoas estrangeiras, ou seus agentes, ou organizações terroristas internacionais ou actividades. A contra-inteligência inclui a realização de análises estratégicas para identificar e produzir inteligência sobre a ameaça de entidades de inteligência estrangeiras para a defesa nacional. Desenvolve e implementa estratégias e planos de ação para combater a ameaça de inteligência estrangeira e utiliza as disciplias de inteligência de defesa para preencher lacunas de coleta.

2.5.7 Inteligência de estimativa

As estimativas são previsões atuais ou potenciais situações com implicações para o planejamento e execução de operações militares. Inclui uma descrição das capacidades dos atores relevantes e relatórios de suas atividades, e analisa fatores conhecidos usando técnicas como análise de padrões, inferência, probabilidade e estatística para endereçar variáveis não resolvidas. Pode fazer uso de ações de forças aliadas.

2.5.8 Inteligência de identidade

Resulta da fusão de atributos identitários (biológicos, biográficos, informações comportamentais e de reputação relacionadas a indivíduos) e outras informações e inteligência associada a esses atributos coletada em todas as disciplinas de inteligência. Utiliza atividades de inteligência de ativação, como inteligência habilitada por biometria, inteligência forense e exploração de documentos e mídia para descobrir existência de

potenciais agentes de ameaça desconhecidos, ligando indivíduos a outras pessoas, locais, eventos ou materiais, analisando padrões de vida e caracterizando seu nível de ameaças potenciais aos interesses da nação.

2.6 ATIVIDADES DE INTELIGÊNCIA DE DEFESA

As atividades de inteligência de defesa são adicionais às atividades realizadas pela equipe de inteligência de combate e são conduzidas por inteligência pessoal para coleta de informações ou contra-inteligência.

O manual de inteligência australiano *Land Warfare Doctrine 2-0 Intelligence* (2018) classifica as atividades de inteligência de defesa como: inteligência prévia, contra-inteligência, segurança de campo, exploração, operações psicológicas, atividades de rastreamento e de debriefing e inteligência regional.

2.6.1 Inteligência prévia

As operações de inteligência referem-se à aquisição de inteligência por meio de ligação e exploração da fonte humana. Isto é conseguido usando pessoal especializado empregado para apoiar na condução das operações. O emprego antecipado de operadores de inteligência ajudará significativamente a força empregada e seus apoios no recebimento de alerta antecipado de ameaças iminentes de natureza local.

As operações subsequentes da fonte garantirão que a compreensão e a conscientização da situação da área de operações seja continuamente atualizada. Isto é alcançado principalmente através do desenvolvimento contínuo de contatos com a comunidade.

O tamanho e a composição da força desdobrada, a natureza da operação, a missão, a complexidade do espaço de batalha e a capacidade e intenção da força ameaçadora determinará a composição e a estrutura do elemento de operações de inteligência.

As operações de inteligência prévia não são conduzidas isoladamente. Elas fazem parte do esforço coordenado de inteligência, que inclui segurança de campo, segurança de operações, exploração, guerra eletrônica e ações de informação.

2.6.2 Contra-inteligência

É o aspecto da inteligência dedicada a neutralizar a eficácia do serviço hostil de inteligência estrangeira e das atividades de ameaças internas e à proteção de informações contra espionagem. A contra-inteligência complementa a segurança das operações, a guerra eletrônica, as operações psicológicas e o engano operacional, e é um dos fatores que contribuem para as ações de informação.

A contra-inteligência é um componente defensivo e ofensivo das operações. A contra-inteligência defensiva concentra-se em medidas de segurança de proteção, como segurança física ou segurança pessoal, e é principalmente no domínio de segurança de campo. Em contrapartida, a contra-informação ofensiva está focada na condução das operações com o objectivo específico de explorar, neutralizar ou degradar a capacidade de um adversário de coletar, processar e disseminar inteligência.

A ligação entre a contra-inteligência e a segurança de campo pode ser quantificada dessa forma: a contrainteligência tem seu foco externo, identificando e explorando a capacidade de vigilância, reconhecimento e inteligência do inimigo; enquanto a segurança de campo é interna, fornecendo conselhos sobre segurança das operações, segurança dos movimentos, segurança pessoal e segurança contra sabotagem.

As atividades de contra-inteligência podem incluir:

a) o contínuo desenvolvimento e manutenção da rede de inteligência;

b) vigilância;

c) contra-vigilância;

d) apoio a investigações de segurança;

e) ligação interinstitucional; e

f) o desenvolvimento de contramedidas de contrainteligência como parte do esforço de contrainteligência de engano militar.

2.6.3 Segurança de campo

Segurança de campo "é um termo abrangente que descreve o suporte de segurança local fornecido pelo pessoal da inteligência dentro de uma área de operações ou área de retaguarda. Inclui a prestação de aconselhamento e supervisão da segurança operacional, segurança de movimento, segurança pessoal, segurança contra-subversão e censura de campo.

Segurança de campo (também conhecida como segurança de proteção) é a provisão de aconselhamento de segurança e suporte de inteligência de segurança para o ambiente operacional. Este apoio é conseguido através da coleta e análise de inteligência de segurança, bem como a prestação de segurança de proteção e conselhos de segurança de operações. Faz parte de uma coordenação esforço de inteligência que inclui ativos de contrainteligência especializados, inteligência de campo, exploração, guerra eletrônica e operações de informação.

A composição e estrutura da força desdobrada, a natureza da operação, a missão, sofisticação, capacidades e intenções da força de ameaça irá determinar a composição e estrutura de elemento de segurança de campo.

2.6.4 Exploração

A exploração de pessoal, material e documentos é uma fonte potencial de informação.. Todo esforço deve ser feito para explorar essas fontes em sua extensão.

O objetivo da exploração é a extração oportuna de informações do pessoal, do material e dos documentos e da eficiente disseminação desses produtos.

Embora a exploração seja principalmente uma responsabilidaprimária de de inteligência, sua eficácia depende muito da cooperação de pessoal na coleta, custódia segura, administração e evacuação rápida de pessoal, documentos e material.

2.6.5 Operações psicológicas

Embora as operações psicológicas caibam no âmbito da equipe de inteligência, elas são uma função de operações dentro de ações de informação. Elas não são classificados como atividades de inteligência sob a definição, mas como um usuário de inteligência e um contribuinte de informação e deve ser considerado como cliente e como fonte.

A partir de estudos da história moderna é amplamente reconhecido que a dimensão psicológica do conflito é tão importante quanto a física. Ao estabelecer objetivos estratégicos e militares sobre uma área-alvo, as percepções desse público e as atitudes têm a capacidade de moldar o resultado de um conflito ou guerra.

O objetivo das operações psicológicas é influenciar e moldar as atitudes e comportamento de uma área alvo em um esforço para persuadir o adversário, neutro e aliados

a se comportarem favoravelmente de acordo com os objetivos nacionais e militares. Operações psicológicas operam de forma contínua durante a paz, conflito e guerra.

Operações psicológicas apóiam todos os tipos de atividades militares dentro de uma operação, incluindo guerra convencional, apoio à paz e atividades das Forças Especiais.

As operações psicológicas são reconhecidas como um elemento essencial nos conflitos e operações militares. Também são um elemento crítico de operações de informação e um meio não letal de persuadir as partes beligerantes a se comportem de maneira favorável na conquista de objetivos. As operações psicológicas devem ser consideradas como elementos críticos de manobra dentro do poder de combate de uma nação. O impacto psicológico do espaço de batalha é uma consideração importante no planejamento de qualquer atividade militar ou diplomática.

2.6.6 Atividades de rastreamento e de debriefing

O rastreamento refere-se ao processo de identificação de quem tem as informações requeridas e que está disposto a fornecer essa informação dentro dos prazos estabelecidos pela coleta de inteligência. O objetivo rastreamento é identificar indivíduos ou grupos que são de interesse para atividades de coleta e contrainteligência de inteligência humana.

Debriefing é o processo pelo qual a informação é extraída de indivíduos que sãodispostos a fornecer oluntariamente informações em resposta às perguntas feitas ou, no caso de exploração, pessoas cuja vontade de resistir ao processo de questionamento tem sido convencidas. O objetivo do debriefing é extrair sistematicamente informações de pessoal civil e militar que foram identificados pelo processo de rastreamento como detentor das informações necessárias.

2.6.7 Inteligência regional

A inteligência regional é uma atividade de coleta aprovada e conduzida como parte de uma vigilância coordenada de inteligência e plano de reconhecimento.

É geralmente conduzida para coletar informações sobre grandes áreas. No entanto, também é adequada para a coleta de informações específicas de áreas focais. Compartilha muitos recursos dos operadores de inteligência e obtém suas informações de uma variedade de contatos da comunidade e agências civis. É capaz de fornecer coleta de inteligência de baixo

custo para comandantes de nível tático e operacional que estão conduzindo tarefas de vigilância em uma grande área.

A inteligência regional é baseada quase inteiramente na inteligência obtida de interação com a comunidade local e a criação e exploração de relatórios de redes civis. É diferenciada das operações de inteligência pelo fato de que a coleta e o contato são mais evidentes.

3 DIFERENÇAS ENTRE INTELIGÊNCIA DE DEFESA E INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Enquanto Inteligência de Segurança Pública atua na área específica de segurança do cidadão, a Inteligência de Defesa é aplicada em todas as áreas de interesse nacional, internas ou externas. Os órgãos de inteligência criados no âmbito da segurança pública especialmente para a produção de conhecimentos, objetivam subsidiar as investigações policiais, entre outras missões enquanto que os componentes da defesa voltam-se às operações militares.

Segundo a Doutrina Nacional de Segurança Pública, a atividade de Inteligência de Segurança Pública (ISP) é o exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais na esfera de Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os governos federal e estaduais a tomada de decisões para o planejamento e execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza ou atentatótios à ordem pública.

Para a execução da Inteligência de Segurança Pública, é necessário que haja um corpo permanente e dedicado de integrantes nas agências de Inteligência das instituições de segurança pública. Gonçalves (2016,pp. 48-49) destaca que são objetivos da ISP “identificar, acompanhar e avaliar ameaças reais ou potenciais de segurança pública e produzir conhecimentos e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza”. Para atingir tais objetivos, os profissionais de ISP precisam lidar rotineiramente com recursos especializados, o que exige um preparo para a função desempenhada.

A disciplina Inteligência de Segurança Pública demanda, como competência associada, o conhecimento dos fundamentos das Atividades de Inteligência, cujo objetivo é criar condições para que os profissionais de segurança pública possam:

> Ampliar conhecimentos para: conhecer os conceitos da atividade de inteligência de segurança pública, as redes e os respectivos sistemas de inteligência. Desenvolver e exercitar habilidades para: utilizar técnicas de inteligência de segurança pública; produzir conhecimentos necessários à tomada de decisões. Fortalecer atitudes para: proteger redes e sistemas de inteligência; reconhecer a importância de um comportamento devidamente regrado por princípios, características e valores éticos da atividade de inteligência de segurança pública (BRASIL, 2014, p. 173).

Conduzida em caráter permanente mesmo em situação de paz, a Atividade de Inteligência de Defesa (AID) é definida como o conjunto de ações de Inteligência desenvolvidas com a finalidade é produzir e salvaguardar conhecimentos de interesse da Defesa.

Na defesa, a Inteligência está presente em todos os níveis de seus processos decisórios. Seu emprego é essencial para que todas as ações desenvolvidas no campo da defesa sejam conduzidas com base em conhecimentos confiáveis e oportunos.

Na Segurança Pública, o ramo de inteligência se destina à produção de conhecimentos de interesse da Segurança Pública e o ramo de contra-inteligência se destina a produzir conhecimentos para neutralizar a inteligência adversa, a proteção da atividade e da instituição a que pertence enquanto que na Defesa, o ramo de inteligência se destina à produção de conhecimentos, relativos a fatos e situações atuais ou potenciais que afetem o processo decisório no âmbito da Defesa e o ramo de contra-inteligência se destina à detecção, identificação, neutralização, obstrução e prevenção da atuação da inteligência adversa e das ações de qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas, instalações, pessoal, material e meios de tecnologia da informação) de interesse da Defesa.

As atividades de Inteligência de Defesa e de Segurança Pública também diferenciam-se entre si quanto à finalidade.

São finalidades da Inteligência de Segurança Pública:

a) proporcionar diagnósticos e prognósticos sobre a evolução de situações do interesse da Segurança Pública, subsidiando seus usuários no processo decisório;

b) contribuir para que o processo interativo entre usuários e profissionais de inteligência produza efeitos cumulativos, aumentando o nível de efetividade desses usuários e de suas respectivas organizações;

c) subsidiar o planejamento estratégico integrado e a elaboração de planos específicos para as diversas organizações da Segurança Pública;

d) apoiar diretamente com informações relevantes as operações policiais de prevenção, repressão, patrulhamento ostensivo e de investigação criminal;

e) prover alerta avançado para os responsáveis civis e militares contra crises, grave perturbação da ordem pública, ataques surpresa e outras intercorrências;

f) auxiliar na investigação de delitos; e

g) preservar o segredo governamental sobre as necessidades informacionais, as fontes, fluxos, métodos, técnicas e capacidades de inteligência das agências encarregadas da gestão de segurança pública.

São finalidades da Inteligência de Defesa:

a) o acompanhamento e o estudo das diversas expressões do poder nacional (militar, psicossocial, política, econômica e científico-tecnológica), além de outros aspectos;

b) o acompanhamento e o estudo de organismos supranacionais e das expressões do poder nacional, bem como dos aspectos geográficos, relacionados aos países estrangeiros;

c) a produção e a difusão de conhecimentos a respeito das forças adversas (campo interno) ou oponentes (campo externo);

d) a produção e a difusão de conhecimentos, na situação de conflito, sobre a provável área de operações e suas condições ambientais;

e) estabelecer um quadro de ameaças efetivas ou potenciais à salvaguarda dos conhecimentos de interesse da Defesa e seus suportes, representadas pelas ações de serviços de inteligência adversa e ações de qualquer natureza;

f) identificar deficiências e vulnerabilidades na salvaguarda dos conhecimentos de interesse da Defesa e seus suportes;

g) propor medidas que resultem no estabelecimento do nível desejável de salvaguarda dos conhecimentos de interesse da Defesa e seus suportes; e

h) propor ações especializadas a serem empregadas com a finalidade de iludir e confundir o processo decisório adverso.

As atividades de inteligência de defesa e de segurança pública diferenciam-se ainda quanto à área de interesse. A Inteligência de Segurança Pública é direcionada à produção de conhecimentos necessários à criação e planejamento de política de seguraça pública enquanto que a Inteligência de Defesa pode abranger as seguintes áreas:

a) assuntos de não-inteligência;

b) mísseis balísticos;

c) força terrestre;

d) força naval;

e) força aérea;

f) questões nacionais;

g) guerra nuclear, química e biológica;

h) equipamentos e tecnologias eletrônicas para uso bélico;

i) ciência e tecnologia;

j) recursos e economia (materiais estratégicos e capacidades industriais);

k) transporte;

l) ambiente físico;

m) terrorismo; e

n) inteligência e segurança.

Enquanto a atividade de inteligência de segurança pública concentra-se na coordenação e integração dos elementos de segurança pública a inteligência de defesa concentra-se no desdobramento de forças militares em operações de defesa nacional.

3.1 CASO PRÁTICO

3.1.1 Operação de Inteligência de Defesa

A Operação Ciclone foi o nome em código do programa da Agência Central de Inteligência (CIA) para armar os mujahideen no Afeganistão durante a invasão soviética do Afeganistão (1979-1989). A Operação Ciclone é uma das operações da CIA mais longas e dispendiosas já realizadas.

O programa baseou-se fortemente no uso da inteligência paquistanesa, o ISI, apoiado pelos serviços de inteligência da Grã-Bretanha (MI6), Egito, Arábia Saudita, China e Israel, como um intermediário para a distribuição dos fundos, repassar armas, treinamento militar e apoio financeiro aos grupos da resistência afegã.

Na administração de Ronald Reagan, o apoio dos EUA aos mujahideen afegãos evoluiu para se converter numa parte central da política externa norte-americana, a chamada de "Doutrina Reagan", pelo qual os Estados Unidos forneceram assistência militar a movimentos de resistência anti-comunistas no Afeganistão, Angola, Nicarágua e outros países. Para implementar essa política, o presidente Ronald Reagan implantou a oficiais paramilitares da Divisão de Atividades Especiais da CIA para treinar, equipar e comandar as forças de mujahedin contra o Exército Vermelho.

Através do ISI, a CIA ajuda tropas de Ahmad Shah Massoud, mas também movimentos islâmicos, como os de Jalaluddin Haqqani (futuro ministro das fronteiras do Taliban) ou de Gulbuddin Hekmatyar, um dos "senhores da guerra" mais favorecidos pelo

ISI paquistanês. A equipe do ISI e treina mais de 100 mil homens entre 1978 e 1992 com um orçamento americano progressivo no total entre 3 e 20 bilhões. Cerca de 35 mil muçulmanos estrangeiros de 43 países islâmicos, participaram nesta guerra.

4 POSSIBILIDADES DA INTELIGÊNCIA DE DEFESA NAS AÇÕES DE SEGURANÇA PÚBLICA

O crime organizado, em especial o tráfico de drogas e o contrabando de armas, as atividades financeiras ilegais, entre as quais a lavagem de dinheiro, são objetos da preocupação dos governos e representam um desafio para os Serviços de Inteligência de qualquer país.

Quando um Estado decide realizar alguma ação, aplicando a força para fazer valer interesses dentro ou fora do seu território, geralmente, as Forças Armadas formam o componente preponderante em relação aos demais instrumentos disponíveis.

Como uma função de combate, a inteligência é uma atividade interagência, intergovernamental e multinacional. A inteligência também é uma função que facilita o entendimento situacional e apóia a tomada de decisão.

Na segurança pública, a Inteligência de Defesa pode executar ações de coleta de dados, vigilância e reconhecimento através de operações e processos de inteligência.

A Inteligência de Defesa facilita aos tomadores de decisão na área de segurança pública a visualização e entendimento da ameaça e outros aspectos relevantes do ambientes onde estão se desencadeando as ações de segurança pública.

As atividades da Inteligência de Defesa ocorrem frequentemente de modo simultâneo e pode propiciar às políticas e ações de segurança pública:

a) o apoio à geração de força - o conhecimento de inteligência relativo ao ambiente onde se desenvolve as ações de segurança pública facilita futuras operações;

b) o apoio ao entendimento situacional – a disponibilidade de informações e conhecimentos de inteligência aos administradores da segurança pública auxilia no alcance de um entendimento claro e preciso das capacidades da força policial com relação às ameaças e outros aspectos relevantes do ambiente onde atuam;

c) a condução da coleta de informações – a atividade de inteligência de defesa sincroniza e integra o emprego de seus meios de coleta para exploração e disseminação de dados em apoio direto às ações presentes e futuras de segurança pública; e

d) fornecer aos administradores de segurança pública subsídios para um emprego eficiente e eficaz de seus meios operativos.

4.1 CASO PRÁTICO

4.1.1 Operação Onerat

Forças de segurança estadual e federal realizaram no dia 5 de agosto de 2017 a Operação Onerat, contra o roubo de cargas e o crime organizado no Rio. Com um efetivo de quase 5 mil homens, a ação fez 15 prisões. Policiais e militares apreenderam 3 pistolas e duas granadas, mas não encontraram fuzis ou munições na intervenção no Complexo do Lins de Vasconcelos, na Zona Norte da cidade.

Dos 40 mandados de prisão da Onerat – carga, em latim – 18 foram cumpridos, sendo que nove alvos já estavam detidos. Os agentes também apreenderam dois adolescentes.

A ação que ocupou o Complexo do Lins contou com cerca de 5 mil homens – quase o dobro da ocupação do Complexo do Alemão, em 2010.

A operação teve início às 3h30 da madrugada quando militares da Brigada Paraquedista, do Exército, e fuzileiros navais, da Marinha entraram na mata para evitar fugas de traficantes. Por volta das 4h30, homens da Coordenadoria de Operações Especiais (Core), da Polícia Civil, e dos Batalhões de Choque e com Cães (BAC) iniciaram a entrada na comunidade. O alvo principal era o roubo de cargas, e as ações foram claramente orientadas pela inteligência militar e policial.

O comando da operação esperava iniciar o cumprimento dos 40 mandados de prisão às 6h, mas a Polícia Civil iniciou as ações a partir das 6h30, um 'delay' que foi comentado nas reuniões após a operação. Com base em registros de ocorrência e dados passados por informantes, os policiais foram a escolas e creches municipais à procura de cargas roubadas, mas não encontraram nada.

Ao todo, foram apreendidas três pistolas, duas granadas, quatro rádios, 16 carros e uma motocicleta e entorpecentes.

A integração entre as polícias e Forças Armadas, principalmente na área de inteligência e investigação, foi um ponto crítico para o sucesso da operação.

5 DEFESA CIBERNÉTICA

Nós vivemos em um mundo conectado. Empresas e países dependem espaço cibernético para tudo, de transações financeiras a movimentos de forças militares.

Atores estatais e não-estatais conduzem operações no espaço cibernético para alcançar objetivos políticos, econômicos ou militares. Ao conduzir suas operações esses atores podem atacar ativos de uma nação conforme seus interesses e propósitos.

O crescente uso de ataques cibernéticos como um instrumento político pode refletir como uma ameaça perigosa às relações internacionais.

Durante um conflito, adversários reais ou potenciais podem procurar atingir infraestruturas críticas ou militares para obter uma vantagem estratégica. Um ciber ataque representa um risco significante à economia e segurança nacionais se vidas são perdidas, propriedades destruídas ou interesses econômicos afetados.

É necessário criar capacidades para operações cibernéticas e integrá-las às ações governamentais como meio de defesa dos interesses diplomáticos, informacionais, militares, financeiros e econômicos.

Segundo o Departamento de Defesa dos Estados Unidos (*DoD_Cyber Strategy)* as missões primárias de defesa cibernética são:

a) defender a rede de dados, sistemas e informações;

b) estar preparado para defender a nação e seus interesses contra ciber ataques de consequências significantes; e

c) se ordenado por governantes, precisa fornecer capacidades cibernéticas para apoiar operações militares e planos de contingência.

Defesa Cibernética é conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente.

A Defesa Cibernética vem se estabelecendo como atividade fundamental ao êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle, por meio da proteção dos ativos de informação, ao mesmo tempo permitindo que esse exercício seja negado ao oponente. Na condição de atividade especializada, sua execução se baseia em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares.

A denominação Defesa Cibernética será utilizada quando do planejamento e da execução de ações cibernéticas afetas ao nível estratégico de decisão.

São princípios relevantes de emprego da Defesa Cibernética:

a) Princípio do Efeito - as ações no Espaço Cibernético devem produzir efeitos que se traduzam em vantagem estratégica, operacional ou tática que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos.

b) Princípio da Dissimulação - medidas ativas devem ser adotadas para se dissimular no Espaço Cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias levadas a efeito contra os sistemas de tecnologia da informação e de comunicações do oponente. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.

c) Princípio da Rastreabilidade - medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de tecnologia da informação e de comunicações amigos. Quase sempre, as ações adotadas no Espaço Cibernético envolvem a movimentação ou a manipulação de dados, as quais podem ser registradas nos sistemas de TIC.

d) Princípio da Adaptabilidade - consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do Espaço Cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis.

Além de atender aos seus princípios relevantes e de guerra, a Defesa Cibernética dispõe de características apresentadas a seguir:

a) Insegurança Latente - nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas.

b) Alcance Global - a Defesa Cibernética possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao Espaço Cibernético.

c) Vulnerabilidade das Fronteiras Geográficas - as ações de Defesa Cibernética não se limitam a fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar.

d) Mutabilidade - não existem leis de comportamento imutáveis no Espaço Cibernético, pois podem adaptar-se as condições ambientais e da criatividade do ser humano.

e) Incerteza - as ações no Espaço Cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.

f) Dualidade - na Defesa Cibernética, as mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvos e, por administradores, para descobrir as fraquezas de equipamentos e redes.

g) Paradoxo Tecnológico - quanto mais tecnologicamente desenvolvido estiver um sistema, mais dependente da TI estará e consequentemente mais vulnerável às ações cibernéticas. Contudo, paradoxalmente, este mesmo oponente possuirá mais condições de se defender dos ataques cibernéticos, em virtude de seu alto grau de desenvolvimento tecnológico.

h) Dilema do Atacante - dúvida que o atacante enfrenta na busca ou não da correção de uma vulnerabilidade identificada, sabendo que a correção tornará mais eficiente a sua defesa, enquanto que a não correção aumenta sua capacidade de ataque.

i) Função Assessoria - as ações de Defesa Cibernética não são um fim em si mesmas, sendo, geralmente, empregadas para apoiar a condução de outros tipos de operação.

j) Assimetria - baseada no desbalanceamento de forças, causado pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais que podem vir a causar danos tão prejudiciais quanto aqueles perpetrados por Estados ou organizações com maiores condições econômicas.

A Defesa Cibernética tem como objetivos estratégicos:

a) contruir e manter capacidades de conduzir operações cibernéticas, por meio de pessoal especializado e obtenção de capacidades técnicas para operações cibernéticas;

b) defender a rede de dados e informações e reduzir os riscos das operações de defesa;

c) estar preparado para defender os interesses vitais e nacionais das consequências significantes de ataques cibernéticos;

d) obter e manter opções cibernéticas e planejar seu uso para controlar a escalada de conflito; e

e) obter e manter alianças e parcerias internacionais para deter ameaças compartilhadas e aumentar a segurança e estabilidade internacionais.

São possibilidades da Defesa Cibernética:

a) atuar no Espaço Cibernético, por meio de ações ofensivas, defensivas e exploratórias;

b) cooperar na produção do conhecimento de Inteligência por meio da Fonte Cibernética;

c) atingir infraestruturas críticas de um oponente sem limitação de alcance físico e exposição de tropa;

d) cooperar com a Segurança Cibernética, inclusive, de órgãos externos ao MD, mediante solicitação ou no contexto de uma operação;

e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da Defesa Cibernética;

f) obter a surpresa com mais facilidade, baseado na capacidade de explorar as vulnerabilidades dos sistemas de informação do oponente;

g) realizar ações contra oponentes mais fortes, dentro do conceito de Guerra Assimétrica; e

h) realizar ações com custos significativamente menores que as operações militares nos demais domínios.

São limitações da Defesa Cibernética:

a) limitada capacidade de identificação da origem de ataques cibernéticos;

b) existência de vulnerabilidades nos sistemas computacionais;

c) dificuldade de identificação de talentos humanos;

d) grande vulnerabilidade a ações de oponentes com poder assimétrico;

e) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e

f) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

Apesar de a Organização das Nações Unidas (ONU) encontrar dificuldades para definir o Terrorismo (ANNAN, 2005), ela fornece um indicativo conceitual, ao apontar que determinadas ações criminosas, ligadas à produção de terror social, devam ser combatidas como se terroristas fossem

Assim como ocorre com o conceito de Terrorismo, o de Terrorismo Cibernético é, por vezes, amplo e vago (CALVELTY, 2007, p. 20; GERCKE, 2009), conquanto gere crescente interesse político, acadêmico e militar.

Nos Estudos de Segurança Internacional, uma corrente majoritária define Terrorismo Cibernético como o conjunto de ataques cibernéticos envidados com o objetivo de gerar temor e direcionados contra infraestruturas críticas ou estruturas estratégicas (BARRETO, 2007; CAVELTY, 2007; 2010; GERCKE, 2009, p. 51; WENDT, 2011). A partir dessa visão, que associa ataques cibernéticos a Terrorismo Cibernético, Cavelty (2010, p. 2) cria a famosa tipologia hierarquizada dos conflitos cibernéticos, a qual tem o Terrorismo Cibernético como o segundo tipo de conflito que, potencialmente, pode gerar mais danos a pessoas, empresas e Estados.

5.1 CASO PRÁTICOS

5.1.1 Irã

Em junho de 2010, o Irã foi vítima de um ataque cibernético quando sua instalação nuclear em Natanz foi infiltrada pelo cyberworm 'Stuxnet', considerado o mais avançado malware já descoberto e aumenta significativamente o perfil da guerra cibernética. Ele destruiu talvez mais de 1.000 centrífugas nucleares e, de acordo com um artigo da Business Insider, "[define] o programa atômico de Teerã de volta em pelo menos dois anos."

5.1.2 China

Em 2013, Edward Snowden, ex-administrador de sistemas da Agência Central de Inteligência (CIA) e instrutor de contrainteligência da Agência de Inteligência da Defesa (DIA), revelou que o governo dos Estados Unidos invadiu empresas chinesas de telefonia móvel para coletar mensagens de texto e espionou a Universidade de Tsinghua, uma das maiores instituições de pesquisa da China, além de abrigar uma das seis principais redes de espinha dorsal da China, a Rede de Educação e Pesquisa da China (CERNET), de onde dados da Internet de milhões de cidadãos chineses poderiam ser extraídos. Ele disse que as agências de espionagem dos EUA vêm observando a China e Hong Kong há anos. [10]

De acordo com documentos confidenciais fornecidos por Edward Snowden, a Agência Nacional de Segurança (NSA) também se infiltrou nos servidores da sede da Huawei, a maior empresa de telecomunicações da China e a maior fabricante de equipamentos de telecomunicações do mundo. O plano é explorar a tecnologia da Huawei para que quando a empresa vendesse equipamentos para outros países - incluindo aliados e nações que evitassem comprar produtos americanos - a NSA pudesse percorrer suas redes de

computadores e telefones para conduzir a vigilância e, se ordenada pelo presidente, ciberoperações ofensivas.

6 CONSIDERAÇÕES FINAIS

O trabalho analisou a Inteligência de Defesa nos cenários nacional e internacional, tendo como foco a atividade de inteligência de defesa como meio de defesa nacional e de interesses políticos, econômicos e militares. O trabalho teve por finalidade também apresentar conceitos e definições da atividade de inteligência, suas disciplinas e possibilidades de atuação nas ações de segurança pública.

Mesmo sendo um meio de defesa que permite à uma nação o conhecimento das possibilidades de um agressor real ou potencial, a atividade de inteligência de defesa possibilita à nação o desenvolvimento de capacidades que lhe permitam vantagem estratégica que lhe assegure a defesa do Estado e da sociedade contra tais agressores, sejam internos ou externos.

No Brasil, a Política Nacional de Defesa (PND) é o documento condicionante de mais alto nível do planejamento de ações destinadas à defesa nacional coordenadas pelo Ministério da Defesa. Voltada essencialmente para ameaças externas, estabelece objetivos e orientações para o preparo e o emprego dos setores militar e civil em todas as esferas do Poder Nacional, em prol da Defesa Nacional.

Pesquisas futuras poderiam ser desenvolvidas sobre a atividade de inteligência de defesa no Brasill, identificando sua organização, estrutura, componentes e sistemas relacionados.

Este trabalho contribui como fonte de pesquisa sobre a inteligência de defesa, orientando pesquisas futuras sobre tecnologias desenvolvidas para uso pelas Forças Armadas nas operações militares de defesa da soberania nacional contra agressão.

REFERÊNCIAS

ANNAN, K. **Uma estratégia mundial de combate ao terrorismo**. *Público*, Lisboa, 12 mar. 2005. Disponível em: <http://publico.pt/espaco-publico/jornal/uma-estrategia-mundial-de-combate-ao-terrorismo-10842>. Acesso em: 20 JUL 18. 2018.

ARAÚJO, Raimundo Teixeira de. **História Secreta dos Serviços de Inteligência**: origens, evolução e institucionalização. São Luís: Ed. do autor, 2004. 204p.

BARRETO, E. M. **Terrorismo Cibernético e cenários especulativos**. *Revista Brasileira de Inteligência*, v. 3, n. 4, p. 63-76, set. 2007

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa.** Brasília, DF: Ministério da Defesa, 2012.

_____. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública. Brasília, 2009

_____. Secretaria Nacional de Segurança Pública. Matriz curricular nacional para ações formativas dos profissionais da área de segurança pública. Coordenação: Andréa da Silveira Passo [et al.]. Brasília: Secretaria Nacional de Segurança Pública, 2014.

BRASÍLIA. Regina Marques Braga Farias. Abin (Ed.). **História Secreta dos Serviços de Inteligência**: origens, evolução e institucionalização. **Revista Brasileira de Inteligência,** Brasília, v. 1, n. 1, p.89-96, nov. 2005. Anual. Disponível em: . Acesso em: 20 Jul 2018.

CAVELTY, M. D. **Cyber-Terror – Looming Threat or Phantom Menace?** The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics*, v. 4, n. 1, p. 19-36, 2007.

Decreto nº 5.848, de 30 de junho de 2005. Aprova a Politica de Defesa Nacional.

FM 34-130. Intelligence Peparation of the Battlefield. 8 July 1994.

GERCKE, M. *Understanding cybercrime*. Genebra: ONU/ITU, 2009.

GONÇALVES, Joanisval Brito. Atividade de inteligência e legislação correlata. 4. Ed. Niterói: Impetus, 2016.

JP 2-0. Joint Intelligence. 2013.

Land Warfare Doctrine 2-0 Intelligence. 2018.

MINISTÉRIO DA DEFESA (Brasil). **Doutrina de Inteligência de Defesa – MD52-N-01.** Brasília, 1ª Edição/2005.

_____. **Doutrina de Operações Conjuntas (Volumes 1, 2 e 3) – MD30-M-01.** Brasília, 1ª Edição/2011.

_____. **Glossário das Forças Armadas – MD35-G-01.** Brasília, 4ª Edição/2007.

_____. **Doutrina Militar de Defesa Cibernética**. – MD31-M07. Brasília, 1ª Edição/2014.

Rapoza, Kenneth (2013-06-22). **"U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press"**. Forbes.

SANGER, DAVID; PERLROTH, NICOLE (22 March 2014). **"N.S.A. Breached Chinese Servers Seen as Security Threat"**. The New York Times.

SHULSKY, Abraham. **Silent Warfare: Understanding the World of Intelligence** New York: Brassey's, 1992.

US General: **Iran's Cyber War Machine 'A Force To Be Reckoned With**. *Business Insider*. Retrieved September 15, 2016.