RISP

REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

v.7, n.1, 2024

ISSN 2675-7168 ; 2966-0254

https://esisperj-ead.pcivil.rj.gov.br

risp.esisperj@pcivil.rj.gov.br

RISP – Revista de Inteligência de Segurança Pública

v. 7, n. 1, 2024

ISSN 2675-7168 (Impressa); 2675-7249 (CD-Rom); 2966-0524 (Online)

EXPEDIENTE

Secretaria de Estado de Polícia Civil
Subsecretaria de Inteligência
Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro

Governador do Estado do Rio de Janeiro
Cláudio Bomfim de Castro e Silva

Secretário de Polícia Civil
Marcus Vinícius Amin Fernandes

Subsecretário de Inteligência
Flávio Porto de Moura

Diretora-Geral da ESISPERJ
Carolina Salomão Albuquerque

Editora Chefe da RISP
Carolina Salomão Albuquerque

Editor Executivo da RISP
Leandro Martins de Paiva Passos

Revisores
Alessandra de Oliveira Rodrigues de Paiva Passos
Anderson Pereira Tavares
Maria Isabel Maia Marmello Henderson
Rafaela Silva Santos

Capa e Editoração Gráfica
Leandro Martins de Paiva Passos

Disponível em:
https://esisperjead.pcivil.rj.gov.br/login/index.php
http://www.policiacivilrj.net.br/risp.php

Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro
Rua do Lavradio, 162. Centro. Rio de Janeiro, RJ.
Tel: (21) 3132-3007 e 3132-3007. E-mail: esisperj@pcivil.rj.gov.br

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

Revista de Inteligência de Segurança Pública [impressa] [CD-Rom] / Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro, Subsecretaria de Inteligência, Secretaria de Estado de Polícia Civil. v. 7, n.1 (2024). Rio de Janeiro: ESISPERJ, 2024.
V.

Anual
ISSN 2675-7168(Impressa);2675-7249(CD-Rom);2966-0524 (Online).

1. Inteligência – periódicos. 2. Segurança Pública – periódicos. 3. Segurança e Defesa – periódicos. 4. Educação Profissional e Inteligência – periódicos. Secretaria de Estado de Polícia Civil, Subsecretaria de Inteligência, Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro.

CDD 300

Dados internacionais de catalogação na publicação (CIP)

Sumário

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

Editorial

Há mais de 10 anos, a Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ), pioneira em capacitação e aperfeiçoamento em Inteligência de Segurança Pública, incentiva a produção acadêmica e científica nessa temática que cada vez mais é tema de estudos e de pesquisas, não só nas entidades públicas como também nas privadas.

A Revista de Inteligência de Segurança Pública (RISP), criada em 2020, é o resultado enriquecedor desta produção, abrilhantada pela diversidade de perfis profissionais que contribuem para as edições da Revista.

A ESISPERJ, mantendo seu compromisso precípuo com o aperfeiçoamento contínuo dos profissionais, dos estudos e pesquisa de Inteligência de Segurança Pública (ISP), lança a sétima edição da RISP que traz quatro artigos sobre temas relevantes para a Inteligência.

O primeiro artigo, intitulado "O Relatório Técnico na Inteligência de Segurança Pública", discute a interessante controvérsia na interpretação institucional em relação ao documento de inteligência Relatório Técnico (RT), buscando sugerir parâmetros de aplicação para promover a uniformidade de seu uso com base analítica nas Doutrinas nacional e estadual.

O segundo artigo, "Inteligência Estratégica no Espaço Cibernético na Segurança Pública", destaca a importância de três elementos na prevenção e resposta a ameaças, bem como na mitigação de riscos: Segurança Operacional (OpSec), Inteligência de Fontes Abertas (OSINT) e Retorno sobre o Investimento (ROI) do adversário.

Posteriormente temos o artigo, "A Reestruturação do Sistema Brasileiro de Inteligência (SISBIN) e suas Implicações para o Subsistema de Inteligência de Segurança Pública (SISP)", que busca discutir quais são as consequências da nova configuração do SISBIN para a atividade de inteligência no Brasil, especialmente para a ISP.

Finalizando a série de produções extremamente valiosas para todos os interessados na atividade de Inteligência, temos o artigo "Cybercrime-as-a-Service (CaaS): O Desafio da Terceirização do Cibercrime para a Atividade de Inteligência", que traz à luz a atuação de cibercriminosos e a importância do desenvolvimento de habilidades referentes à Inteligência Cibernética, considerando o futuro desafiador da cibersegurança.

Carolina Salomão
Editora-chefe da RISP

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

O RELATÓRIO TÉCNICO NA INTELIGÊNCIA DE SEGURANÇA PÚBLICA*

Mario Jessen Lavareda**

RESUMO

Relatório Técnico, um dos tipos de documentos de Inteligência no âmbito da Inteligência de Segurança Pública, apesar de disciplinado pela Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro e pela Doutrina Nacional de Inteligência de Segurança Pública, possui interpretações controvertidas nas diferentes instituições públicas e na suas respectivas Agências de Inteligência de Segurança Pública. Almejando incrementar a discussão sobre o tema e a uniformidade de atuação dos órgãos incumbidos da segurança pública, buscou-se sugerir parâmetros de aplicação do Relatório Técnico, notadamente em relação à sua iniciativa, à conveniência e oportunidade de sua produção, ao seu conteúdo, às suas finalidades e à sua classificação. Para tanto, analisou-se as Doutrinas de Inteligência de Segurança Pública, obras de autores especializados do Brasil e do exterior, a legislação nacional e a jurisprudência dos Tribunais Superiores.

Palavras-chave: Inteligência; Inteligência de Segurança Pública; Relatório Técnico; Prova.

THE TECHNICAL REPORT IN PUBLIC SECURITY INTELLIGENCE

ABSTRACT/RESUMEN

The Technical Report, one of the types of Intelligence documents within the scope of Public Security Intelligence, despite being disciplined by the Public Security Intelligence Doctrine of the State of Rio de Janeiro and by the National Public Security Intelligence Doctrine, has controversial interpretations in the different public institutions and their respective Public Safety Intelligence Agencies. Aiming to increase the discussion on the subject and the uniformity of action of the bodies responsible for public security, an attempt was made to suggest parameters for applying the Technical Report, notably in relation to its initiative, the convenience and opportunity of its production, its content, its purposes and its classification. For this purpose, the Public Security Intelligence Doctrines, works by specialized authors from Brazil and abroad, the national legislation and the jurisprudence of the Superior Courts were analyzed.

Keywords*: Intelligence; Criminal Intelligence; Law Enforcement Intelligence; Technical report; Evidence.*

* Artigo adaptado a partir do Trabalho de Conclusão de Curso apresentado na Pós-graduação em Inteligência Aplicada pelo Instituto de Educação Roberto Bernardes Barroso do Ministério Público do Estado do Rio de Janeiro.

** Especialista em Inteligência Aplicada pelo Instituto de Educação Roberto Bernardes Barroso do Ministério Público do Estado do Rio de Janeiro. Promotor de Justiça do Ministério Público do Estado do Rio de Janeiro. Endereço eletrônico: mario.lavareda@mprj.mp.br.

INTRODUÇÃO

A Inteligência de Segurança Pública (ISP), descendente direta da denominada Inteligência Clássica, foi idealizada e surgiu para integrar o ferramental de combate à criminalidade, com destaque àquela organizada. Dentre os diversos documentos de ISP (Doc ISP), instrumentos da maior relevância, na medida em que corporificam o conhecimento produzido pela ISP e que, através deles, difunde-se tal saber, assume grande importância o Relatório Técnico (RT).

Tradicionalmente, os conhecimentos elaborados ficavam restritos ao (Sub)Sistema de ISP (SISP), formado pelo conjunto de Agências de ISP (AISPs), e às chefias dos órgãos públicos por elas assessorados. O RT, contudo, abriu a possibilidade de se estabelecer interação entre as AISPs e outros atores do campo da segurança pública, mesmo aqueles externos ao SISP. Além disso, permitiu que a Inteligência propalasse informações não sigilosas para fins de produção de prova.

Esses traços inovadores do RT em comparação com outros Doc ISP, aliados à natural abertura interpretativa dos textos das Doutrinas[1], as quais não podem esgotar os temas tratados sob pena de perderem flexibilidade e engessarem a atividade de Inteligência, fazem com que o RT seja compreendido, e por conseguinte aplicado, de maneiras diversas pelas variadas AISPs existentes, principalmente quando pertencentes a órgão públicos de naturezas díspares.

Em que pese a disciplina genérica do RT, conceituado como "o documento externo, padronizado, passível de classificação, que transmite, por iniciativa da AISP produtora e de forma excepcional, ainda que fora do canal técnico, análises técnicas e de dados, destinados a subsidiar seu destinatário, inclusive, na produção de provas" (DISPERJ, 2015), pouco se escreve acerca da iniciativa de elaboração, da conveniência e oportunidade de sua produção, da abrangência do conteúdo, de sua finalidade, aplicações práticas e da classificação desse documento.

Assim, o presente artigo objetiva, em primeiro lugar, fomentar o debate sobre o RT e suas características distintivas. Paralelamente, busca-se aprofundar os conceitos doutrinários, sugerindo-se parâmetros de aplicação do aludido tipo de Doc ISP, sempre tendo em mira o incremento da uniformidade de trabalho das diferentes AISPs. O que se defenderá a seguir é uma visão específica do RT, sem prejuízo de

1 Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ) e Doutrina Nacional de Inteligência de Segurança Pública (DNISP).

outras, capaz de auxiliar a investigação criminal a cargo das Polícias Judiciárias e do Ministério Público, mas que ao mesmo tempo preserva a natureza típica da Inteligência, sem desviar os recursos da AISP para ações que não são de sua responsabilidade nata.

Nesse contexto, mostra-se importante assentar a premissa, inequívoca no presente artigo, de que ISP e investigação criminal consubstanciam atividades distintas. Ambas comungam de certos objetos aos quais são aplicadas (crimes e seus autores, por exemplo) e de algumas técnicas operacionais para obtenção de dados, mas seus traços marcantes não deixam espaço para confusão conceitual.

A Inteligência, de modo geral, consiste na atividade de angariar dados, por vezes negados, e processá-los, com vistas à criação de um conhecimento inédito, que servirá para subsidiar a tomada de decisões de um usuário final. Tal caráter nitidamente assessório alia-se, ademais, ao sigilo decorrente da sensibilidade dos temas abordados, regido pela Lei nº 12.527/2011, e a um método de produção do conhecimento voltado precipuamente para garantir a máxima veracidade das informações lato sensu fornecidas ao usuário.

De outra parte, a investigação criminal destina-se apenas a elucidar delitos, comprovando sua materialidade e desvelando a autoria, sem pretensão de que o esclarecimento do crime sirva para assessorar a decisão de quem quer que seja. O sigilo, aqui, não é a regra. Apesar de amplamente utilizado para assegurar a efetividade de diligências investigatórias, seu destino inexorável é ser levantado, preferencialmente para toda a sociedade e no mínimo para os alvos das apurações e seus Advogados. Por fim, a busca da verdade no campo investigativo cede muito para a imprescindível obediência a normas processuais penais que regulam a admissibilidade de provas na ação penal, passo seguinte às investigações criminais.

O problema central reside justamente em saber como navegar na interseção dessas duas atividades tão cruciais, cada qual a seu modo, para o combate à criminalidade e para a manutenção da segurança pública.

Uma fundação segura para o desenvolvimento da questão parte da própria definição de RT consagrada na DNISP (2014) e na DISPERJ (2015). Vale dizer, reconhece-se a possibilidade de transmissão, "de forma excepcional", "ainda que fora do canal técnico", de "análises técnicas e de dados", destinadas inclusive à "produção de provas", em documento externo "passível de classificação", com o adendo de que, no Estado do Rio de Janeiro, o

compartilhamento depende de "iniciativa da AISP produtora".

1 INICIATIVA

Em primeiro lugar, no que se refere à iniciativa da produção do RT, entendo que deva ser conferida tanto à AISP quanto à Autoridade Policial ou Ministerial. Com efeito, essa iniciativa dupla, além de não violar a independência da AISP, serve melhor aos propósitos do RT, pois nem sempre a AISP terá ciência das necessidades de dados dos seus possíveis destinatários. Afigura-se salutar conceder a iniciativa de pedidos de RT à Autoridade Policial ou Ministerial tendo em conta o emprego ótimo dos dados de Inteligência na investigação criminal, pois, em razão de liderarem a apuração, são as mais preparadas, ao menos em tese, para indicar à AISP quais dados desejam obter, bem como para determinar o momento ideal de emprego do RT na investigação em curso, em consonância com o princípio da oportunidade.

Talvez a DISPERJ tenha inserido esse requisito, de exclusividade da iniciativa, como um mecanismo de proteção da AISP contra eventuais direcionamentos externos. Devendo o RT ser produzido ao alvitre da AISP, consequentemente esta nunca assumiria o papel de braço investigativo das Polícias Judiciárias ou do Ministério Público, nem teria suas ações ditadas por órgão alheio à Inteligência.

Entretanto, a iniciativa de terceiros, isoladamente, não se mostra apta a comprometer a integridade da Inteligência. Por mais que a AISP receba pedidos de RT, a efetiva elaboração do documento e a definição do seu conteúdo sempre estarão sob o absoluto controle da área de Inteligência, visto inexistir relação hierárquica entre a AISP e a Autoridade solicitante. Analogamente ao que sucede nos Pedidos de Busca (PBs) entre AISPs, a Autoridade solicitante do RT nunca poderá determinar quais dados serão compartilhados, nem mesmo poderá exigir que o RT seja de fato produzido. Em suma, estando a iniciativa com a Autoridade solicitante ou com a AISP, esta sempre terá sua independência preservada.

2 EXCEPCIONALIDADE

O RT deve ser obrigatoriamente um documento excepcional, mas o que é a exceção e quem a define podem suscitar debates. Trata-se de adjetivo abstrato, aberto a múltiplas interpretações, todas com elevado teor de subjetividade. Entretanto, apesar da dificuldade de se estabelecer uma definição hermética sobre o que constitui a exceção à regra, existem balizas que podem ajudar na tarefa.

De pronto, a literalidade do termo "excepcional" já serve para excluir os extremos que não se encaixam nesse conceito. O RT não pode ser regra, não pode ser produzido com a mesma frequência que outros documentos de Inteligência, até mesmo porque serve mais a uma atividade executiva, de produção de provas, finalidade estranha ao assessoramento típico da Inteligência. Paralelamente, a produção de RTs não deve ser nula, pois, se assim fosse, sequer teria sido inserido nas atualizações da DISPERJ e da DNISP ou então seria expressamente vedado.

Outro ponto a ser considerado na decisão acerca da pertinência da produção e da difusão de um RT é se a formalização desse documento atende prioritariamente aos objetivos da AISP e da instituição à qual ela serve. Em razão de se destinar à produção de provas, o RT sempre terá utilidade para o destinatário incumbido da investigação criminal, mas isto não pode ser a única motivação para sua elaboração. A AISP, em regra, não é subordinada hierarquicamente aos destinatários dos RTs e, por conseguinte, mesmo quando produz tal documento, deve ter como norte o cumprimento de sua própria missão, compartilhando dados caso isso favoreça de alguma forma o serviço da AISP ou os interesses do Decisor ao qual está atrelada.

Aliás, o sistema ou subsistema no qual a AISP se encontra inserida figura como mais um parâmetro acerca da "excepcionalidade". Naturalmente, AISPs de órgãos precipuamente investigativos, a exemplo das Polícias Judiciárias e dos diversos ramos do Ministério Público, justamente por conta da alta carga conferida à investigação criminal nestas instituições, terão um padrão de "excepcionalidade" mais amplo do que aquelas AISPs cujos órgãos não tenham a investigação como carro-chefe, podendo-se citar a título de exemplos as Polícias Militares e os Corpos de Bombeiros Militares, que desenvolvem apenas a investigação de crimes militares.

Sob perspectiva diversa, mostra-se necessário avaliar igualmente a relação de custo-benefício da produção do RT. Este documento, em decorrência de poder assumir a natureza de prova, não classificada, acaba, mesmo que indiretamente, expondo quais são os objetos de estudo da AISP, seus integrantes e por vezes seus meios de obtenção de dados, informações críticas no âmbito de um serviço que preza pelo sigilo. É imprescindível, destarte, ponderar se os resultados almejados com a difusão do RT superam esse risco.

3 CONTEÚDO

A DISPERJ (2015) e a DNISP (2014) estabeleceram que o RT deve veicular

"análises técnicas e de dados", mas novamente essas Doutrinas deixaram de definir com precisão em que consistiriam tais análises. Não obstante, na DISPERJ (2015) há a explicitação de que dado "é toda e qualquer representação de fato, situação, comunicação, notícia, documento, extrato de documento, fotografia, gravação, relato, denúncia etc, ainda não submetida, pelo profissional de ISP, à metodologia de Produção de Conhecimento", conceituação seguida pela DNISP (2014), a qual é complementada pelas definições de documento ("unidade de registro de informações, qualquer que seja o suporte ou formato") e de denúncia ("notícia ostensiva ou sigilosa que se faz de algo ou alguém, sobre falta ou crime cometido ou na iminência de ser cometido, podendo ser realizada de maneira formal ou anônima").

Portanto, mostra-se razoável afirmar, inclusive com base doutrinária, que o RT pode ser utilizado para transmitir tudo aquilo que não seja conhecimento, ou seja, todo e qualquer dado, de livre acesso, protegido ou negado, não processado, não submetido às etapas de avaliação, análise, integração e interpretação.

Referida conclusão aparentemente não gera maiores polêmicas quando se trata de dados materiais ou materializáveis, como aqueles plasmados em documentos ou usualmente oriundos da Inteligência Eletrônica, a exemplo de imagens ou de interceptações de telecomunicações. Isso porque, na hipótese de o RT ser utilizado como prova judicial, a AISP produtora ficaria isenta de questionamentos acerca da veracidade ou confiabilidade do dado transmitido. A origem do RT, aliás, remonta justamente ao compartilhamento de escutas telefônicas.

Percebe-se certa resistência, por outro lado, ao emprego do RT para o compartilhamento de dados originados da Inteligência Humana, em especial daqueles consistentes em relatos de informantes. Nestes casos, alguns entendem que a AISP seria colocada em posição de fragilidade por não poder revelar suas fontes, bem como diante da impossibilidade de se comprovar a veracidade do dado transmitido, cabendo destacar que, a rigor, no RT, tais dados não poderiam sequer ser avaliados quanto à credibilidade da fonte e do conteúdo, sob pena de se transmitir conhecimento de Inteligência através de documento inadequado.

Apesar de concordar com essas ponderações, não enxergo uma vedação doutrinária ou uma incompatibilidade absoluta entre o conceito de RT e a transmissão de dados não demonstráveis no plano fático. Em verdade, essas reflexões se encaixam mais na discussão acerca da conveniência ou utilidade de se produzir um

RT com dados oriundos da Inteligência Humana do que propriamente na possibilidade abstrata de se elaborar um RT com o mencionado tipo de dado.

Exemplificativamente, mesmo sendo possível, realmente seria difícil encontrar justificativa para a elaboração de um RT contendo o relato isolado (e obrigatoriamente não avaliado) de um informante anônimo. O valor probatório desse dado em Juízo seria praticamente nulo e poderia, quando muito, servir de ponto de partida para a realização de diligências investigatórias preliminares.

O cenário mudaria, porém, no caso de se tratar de um RT compilando diversos relatos de informantes diferentes ou expondo de forma cronológica vários Disques-Denúncias (DDs) acerca de determinado crime. Ainda que continuem sendo dados não avaliados e de fontes anônimas e que não constituam, por si só, prova de um fato, certamente o conjunto de indícios terá maior peso, seja para orientar os trabalhos da Autoridade incumbida da investigação criminal, seja para corroborar provas produzidas em sede judicial.

Desta feita, muito embora seja inegável que os dados obtidos por meio da Inteligência Eletrônica tenham em princípio maior lastro probatório material e que, por conseguinte, assumam posição de maior relevância em um eventual RT, não considero adequada a exclusão pura e simples da possibilidade de transmissão de dados de Inteligência Humana. A uma, porque a DISPERJ e a DNISP não fazem essa distinção. A duas, porque, segundo exemplificado, os dados, ainda quando não materializáveis, dependendo do seu volume e/ou da sua compatibilidade com outros dados objetivamente aferíveis, podem munir a Autoridade destinatária com informações importantes.

4 FINALIDADES

No plano normativo, de acordo com a DNISP, a investigação e a Inteligência Policial, apesar de constituírem atividades diversas, acabam se interligando. Inclusive, à Inteligência é dada a missão de assessorar a própria investigação, não apenas a formulação e execução de políticas públicas ou ações concretas para neutralizar ameaças.

Ao tratar dos objetivos geral e específico da Inteligência Policial Judiciária, espécie de ISP, a DNISP (2014) preceitua que a Inteligência deve servir, respectivamente, à segurança pública, produzindo "conhecimentos acerca de fatos e situações de interesse da Polícia Judiciária, notadamente no assessoramento das ações especializadas da investigação policial" e como assessoria à investigação policial, produzindo "conhecimentos e, excepcionalmente, provas, mediante

Relatórios Técnicos, acerca de fatos e situações relativas às organizações criminosas ou aos crimes cuja complexidade exija o emprego de ações especializadas".

No mesmo sentido, a DISPERJ (2015) prevê que "na investigação de ISP há a possibilidade de obtenção de provas, em virtude de sua atividade investigativa, embora excepcionalmente", sendo que uma das vantagens da ISP expressamente reconhecida pela DISPERJ é a de "aumentar a velocidade das investigações".

Romeu Antônio Ferreira (2021) afirma que a investigação, no seu sentido amplo, de busca da verdade, não é atividade exclusiva das Polícias nem mesmo de qualquer grupo. Citando como exemplos a investigação científica e a investigação filosófica, entende que a ISP também investiga e, assim, diferencia a Inteligência da investigação policial com base não na natureza intrínseca de cada atividade, mas principalmente a partir dos objetivos (assessoramento de um tomador de decisão x produção de provas), da faixa de tempo investigada (a ISP produz conhecimentos igualmente sobre o futuro, não apenas acerca do presente e do passado) e do sigilo típico da Inteligência.

Referida ideia, de investigação como um conceito amplo e instrumento compartilhado por diversas áreas do saber, também é defendida por Denilson Feitoza Pacheco (2005):

> "A pesquisa científica, as atividades e operações de inteligência, a investigação criminal e o processo penal buscam a verdade. A evolução de seus métodos, técnicas e instrumentos de busca da verdade, portanto, podem ser reconduzidos a um modelo único de comparação. (...). As diferenças fundamentais são os critérios de aceitabilidade da verdade, objetivos, marcos teóricos e regras formais específicas de produção". (DENILSON, 2005)

Partindo-se de tais premissas, vislumbro duas finalidades principais para o RT. A primeira, mais harmônica com a separação estanque entre Inteligência e investigação, é a de indutor das apurações criminais. Nesta hipótese, o RT não seria incorporado aos autos, ou seja, não serviria como prova, mas seu conteúdo seria utilizado para direcionar os trabalhos da Autoridade incumbida de elucidar determinado crime, indicando, por exemplo, suspeitos, testemunhas, possíveis linhas investigativas ou meios de obtenção de provas do fato delituoso que se busca esclarecer. Por outro lado, dando um passo além, o RT poderia ser empregado para desde já fornecer evidências, as quais seriam juntadas ao procedimento investigatório e comporiam, ao final da instrução processual, o conjunto probatório a ser avaliado pelo Poder Judiciário.

Não se trata de ideia inédita; pelo contrário. E. Drexel Godfrey Junior e Don R. Harris (1971, p. 12-13 e 28) diferenciaram

quatro categorias de usos para a chamada Inteligência criminal. A Inteligência premonitória ou indicativa e a Inteligência estratégica cumpririam o papel clássico de assessoramento através do acompanhamento sistemático e preventivo das ações de grupos criminosos. A Inteligência tática estaria voltada para a ação (e.g. prisões) e, assim, deveria ser preferencialmente destinada a unidade diversa da de Inteligência. Finalmente, a Inteligência de evidência, formada por informações concretas e precisas, poderia ser apresentada em Juízo como prova. Comparando ainda a Inteligência indicativa e a Inteligência de evidência, ou probatória, afirmaram que esta também pode ser produzida para auxiliar outro setor da agência policial ou o Promotor de Justiça, responsáveis diretos pela produção de prova, podendo contribuir com a interpretação das evidências angariadas e indicando meios de encontrar novas provas.

O Escritório das Nações Unidas sobre Drogas e Crime (UNODC) (2011, p. 10) preceituou de modo semelhante em seu Manual de Inteligência Criminal, na parte em que diferencia a Inteligência da prova. Embora tenha deixado a cargo da legislação local a regulamentação da forma de aproveitamento da Inteligência na persecução criminal, expressamente reconheceu as possibilidades de ser usada como prova e de ser empregada como catalisador dos trabalhos investigativos.

Registre-se ainda, no caso de a difusão do RT objetivar instruir diretamente o procedimento investigatório, a imperiosa necessidade de observância das normas jurídicas que disciplinam a validade das provas. De nada adiantaria munir a Autoridade destinatária do RT com provas processualmente inadmissíveis. Além de estas serem desconsideradas por completo pelo Poder Judiciário, mostrando-se inúteis para a pretendida condenação do criminoso, sua publicização certamente seria explorada pela defesa para pôr em xeque a investigação como um todo, em que pese haver diferenças entre aquilo que é permitido nas ações de busca da Inteligência e aquilo que é juridicamente aceito para fins de prova processual penal.

Assim, deve-se ter especial cautela quando os dados compartilhados via RT forem originados de infiltração, provocação do criminoso-alvo, entrevista ou interrogatório do criminoso, interceptação de sinais, interceptação postal e entrada. Todas essas são ações mais invasivas e suscetíveis a nulidades no processo penal na eventualidade de não atenderem aos requisitos previstos em Lei e consagrados na jurisprudência pátria.

5 CLASSIFICAÇÃO

No que se refere ao sigilo do RT, tanto a DISPERJ (2015) quanto a DNISP (2014) dispõem que esse documento é "passível de classificação", isto é, pode ou não ser ostensivo, tendo a Doutrina novamente deixado em aberto em quais hipóteses o RT será sigiloso e em que casos assumirá caráter público.

Procurando-se compatibilizar o dilema da classificação com as principais finalidades do RT abordadas (direcionar a investigação criminal e fornecer provas), parece lógico concluir que, se a difusão do RT pretende proporcionar evidências de um crime para a formação de provas destinadas ao convencimento do órgão jurisdicional, o documento não deve ser classificado. Por outro lado, se o Chefe da AISP objetivar somente contribuir com a investigação de determinado fato delituoso, sem qualquer pretensão de que os dados angariados pela Inteligência assumam a qualidade de prova ou, ainda, necessitando que tais dados não sejam disponibilizados ao público em geral, o caminho é a classificação do documento, de acordo com os parâmetros legais e a sensibilidade de seu conteúdo.

Caso haja necessidade absoluta de sigilo, a classificação se impõe e o RT não deve ser produzido para fins de constituição de prova. E, mesmo que o sigilo não seja forçoso, inexistindo a finalidade de utilização do RT como prova, afigura-se recomendável a classificação, pois, conforme registrado, ao se tratar da excepcionalidade, há de se ponderar que a difusão de um RT não classificado expõe reflexamente os objetos de estudo da AISP, seus meios de obtenção de dados e até alguns de seus integrantes, o que poderia comprometer a segurança da Agência e do pessoal e diminuir a chance de êxito de futuras ações de Inteligência.

CONCLUSÃO

Verifica-se que o surgimento do RT representou significativa inovação na ISP quando comparadas as versões iniciais e as atuais da DISPERJ e da DNISP e, principalmente, se cotejada essa espécie de Inteligência com a Inteligência Clássica. Justamente por ter sido concebido para regulamentar o fluxo de informações entre a Inteligência e os órgãos públicos incumbidos da investigação criminal, o RT ostenta notas características frente aos outros Doc ISP, em especial a possibilidade de envio de "análises técnicas e de dados" para destinatários que não integram o SISP e a capacidade de que as análises encaminhadas sejam empregadas como provas em investigações e ações penais.

A exemplo do que ocorreu em outros países, o emprego da Inteligência na área policial, ou criminal, sob escopo mais amplo, desvelou a oportunidade de os

serviços de Inteligência auxiliarem na resolução de crimes, mormente daqueles mais complexos e perpetrados por organizações criminosas, acrescendo-se essa finalidade, mais voltada para o plano executivo, àquelas de assessoramento tradicionalmente ligadas à Inteligência Clássica.

Se, por um lado, essa nova forma de agir da Inteligência encerra vantagens inegáveis, na medida em que acelera e potencializa os trabalhos investigativos, até mesmo robustecendo o acervo probatório submetido à apreciação do Poder Judiciário, por outro suscita riscos que não podem ser ignorados e, aliás, que devem ser constantemente debelados. Dentre eles, destacam-se a confusão conceitual entre Inteligência e investigação criminal, em cuja tênue fronteira o RT transita, a concentração de atividades de Inteligência e executivas em um único órgão, a exposição indevida das AISPs, particularmente de seu pessoal (orgânico ou não) e de suas operações, e a anulação de investigações e processos criminais na hipótese de a prova fornecida pela Inteligência não atender aos padrões legais e jurisprudenciais de validade.

Em decorrência, mostra-se construtivo o debate sobre referido Doc ISP e o estabelecimento de balizas as quais, desdobrando o conceito doutrinário naturalmente sintético, permitam uma atuação cada vez mais uniforme por parte das diferentes AISPs quando da elaboração e difusão do RT, explorando seus benefícios e abrandando ao máximo seus pontos negativos.

Nesse propósito, partindo-se da inarredável premissa de independência da atividade de Inteligência, defendeu-se que a elaboração de um RT não pode ser imposta à AISP, devendo ser fruto de uma decisão do Chefe, sem embargo da possibilidade de o RT ser solicitado por eventual interessado. Compete ao Chefe da AISP, igualmente, aquilatar a excepcionalidade que justifica a produção do RT, levando-se em conta a missão da instituição a que pertence e os prós e contras da difusão do RT no caso concreto. Adicionalmente, seu conteúdo deve ficar restrito a dados não submetidos ao denominado Ciclo de Produção de Conhecimento (CPC). Sustentou-se, ademais, que o RT pode servir a duas finalidades básicas, de mera orientação dos procedimentos apuratórios, caso no qual deveria ser preferencialmente classificado e não juntado aos autos, e de produção de evidências, situação em que não poderia ser sigiloso e na qual haveria a imperiosa necessidade de observância do regramento de validade das provas.

REFERÊNCIAS

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Disponível em: <*http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm*>. Acesso em: 07 fev. 2024.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública - DNISP. 4. ed. rev. e atual. - Brasília: Secretaria Nacional de Segurança Pública, 2014.

BRASIL. ESTADO DO RIO DE JANEIRO. Decreto nº 45.126, de 13 de janeiro de 2015. Aprova a nova doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ) e dá outras providências.

FERREIRA, Romeu Antônio. Nota de Aula 01.02.03: Investigação de ISP. Rio de Janeiro: versão de 25 de março de 2021.

JUNIOR, E. Drexel Godfrey; HARRIS, Don R. *Basic Elements of Intelligence: A Manual of Theory, Structure and Procedures for Use by Law Enforcement Agencies Against Organized Crime*. *U. S. Department of Justice*, 1971.

PACHECO, Denilson Feitoza. Atividades de Inteligência e Processo Penal. *In*: IV Jornada Jurídica da Justiça Militar da União – Auditoria da 4ª CJM, 30 set. 2005, Juiz de Fora/MG. Disponível em: <*https://pointinteligencia.blogspot.com/2012/05/atividades-de-inteligencia-e-processo.html*>. Acesso em: 07 fev. 2024.

UNODC. *United Nations Office on Drugs and crime*. *Criminal Intelligence Manual for Managers*. *United Nations Publication*. Austria, 2011.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

INTELIGÊNCIA ESTRATÉGICA NO ESPAÇO CIBERNÉTICO NA SEGURANÇA PÚBLICA

Richard Brito Guedes de Sousa*

RESUMO

A inteligência estratégica é fundamental para a segurança pública, especialmente diante das crescentes ameaças enfrentadas pelas comunidades. Este artigo explora a aplicação da inteligência estratégica na Segurança Pública, com foco em três componentes essenciais: Segurança Operacional (OpSec), Inteligência de Fontes Abertas (OSINT) e Retorno sobre o Investimento (ROI) do adversário. Destaca-se a importância desses elementos na prevenção e resposta a ameaças, bem como na mitigação de riscos. Analisamos como a OpSec protege operações sensíveis, a OSINT fornece insights valiosos de fontes abertas e o ROI do adversário avalia a eficácia das medidas de segurança. Compreender e integrar esses conceitos é fundamental para fortalecer a segurança pública, promovendo uma abordagem proativa e eficiente na proteção dos cidadãos e na manutenção da ordem e da paz social.

Palavras-chave: Inteligência Estratégica, Espaço Cibernético, OpSec, OSINT, ROI do Adversário, Segurança Pública.

STRATEGIC INTELLIGENCE IN CYBERSPACE IN PUBLIC SECURITY

ABSTRACT/RESUMEN

Strategic intelligence is critical to public safety, especially in the face of growing threats facing communities. This article explores the application of strategic intelligence in Public Security, focusing on three essential components: Operational Security (OpSec), Open Source Intelligence (OSINT), and adversary Return on Investment (ROI). The importance of these elements in preventing and responding to threats, as well as mitigating risks, is highlighted. We analyze how OpSec protects sensitive operations, OSINT provides specific insights into open sources and adversary ROI available for the effectiveness of security measures. Understanding and integrating these concepts is fundamental to strengthening public security, promoting a proactive and efficient approach to protecting citizens and maintaining order and social peace.

Keywords*: Strategic Intelligence, Cyberspace, OpSec, OSINT, ROI of the Adversary, Public Security.*

* Pesquisador de Segurança da Informação, Operações Cibernéticas Defensivas e Ofensivas, PenTest, Inteligência e Contrainteligência. Mestre em Direção Estratégica em Tecnologias da Informação pela Universidad Europea del Atlántico (UNEATLANTICO), Pós-graduado no Curso Superior de Segurança e Defesa Cibernética (CSSDC) pela Escola Superior de Guerra (ESG), Pós-graduado em Ethical Hacking e CyberSecurity e MBA em Gestão de Projetos em TI pela Vincit, Bacharel em Sistemas de Informação pela Universidade Castelo Branco (UCB). Presidente do Instituto de Defesa Cibernética (IDCiber). Endereço eletrônico: richardg7@outlook.com

INTRODUÇÃO

Nos últimos anos, a crescente complexidade e sofisticação das ameaças à segurança pública têm impulsionado a necessidade de estratégias avançadas de inteligência. Nesse contexto, a inteligência estratégica, combinada com abordagens como a Segurança Operacional (OpSec), a Inteligência de Fontes Abertas (OSINT) e a análise do Retorno sobre o Investimento (ROI) do adversário, tornou-se essencial para fortalecer as defesas e aumentar a eficácia das operações de segurança pública. Este artigo explora a importância da inteligência estratégica no contexto da segurança pública, destacando como as técnicas de OpSec, OSINT e análise do ROI do adversário podem ser empregadas para proteger comunidades, antecipar ameaças e promover a segurança em sociedade.

À medida que as tecnologias avançam e as ameaças se tornam mais sofisticadas, as agências de segurança pública enfrentam um ambiente operacional cada vez mais desafiador. Nesse cenário, a inteligência estratégica surge como uma ferramenta crucial para antecipar e responder a ameaças emergentes, bem como para garantir a segurança e o bem-estar da população. Ao integrar princípios de OpSec, aproveitar os recursos da OSINT e entender o ROI do adversário, as agências de segurança pública podem tomar decisões informadas e eficazes, promovendo uma abordagem proativa para enfrentar os desafios de segurança contemporâneos. Ao longo deste artigo, exploraremos como essas abordagens podem ser aplicadas de maneira prática e eficiente no contexto da segurança pública.

1 REFERENCIAL TEÓRICO

1.1 Orientações gerais do referencial teórico

A inteligência estratégica cibernética representa um conjunto complexo de práticas destinadas a entender e mitigar as ameaças no espaço digital.

Segundo Watters (2023), o ambiente operacional cibernético exige uma abordagem multifacetada para a segurança, integrando técnicas de OpSec, OSINT e Contrainteligência. Alsmadi (2023) complementa essa visão, destacando a importância do planejamento operacional cibernético na prevenção de ataques e na resposta a incidentes de segurança

No contexto da segurança pública, a inteligência estratégica cibernética é crucial para antecipar e neutralizar ameaças. A implementação eficaz do OpSec envolve a proteção de informações operacionais para evitar que sejam exploradas por adversários. O OSINT, por sua vez, permite a coleta de informações publicamente disponíveis para

identificar potenciais ameaças e vulnerabilidades. Já a Contrainteligência foca na detecção e neutralização de esforços de inteligência adversários, protegendo as operações e as informações críticas da interferência inimiga.

1.1.1 Operational Security (OpSec)

O OpSec, a OSINT e a Contrainteligência são pilares fundamentais da inteligência estratégica no espaço cibernético. OpSec refere-se às medidas adotadas para proteger informações sensíveis e evitar que sejam exploradas por adversários. Isso inclui ações como criptografia de dados, autenticação multifatorial e conscientização sobre segurança da informação. OSINT, por sua vez, envolve a coleta e análise de informações disponíveis publicamente na internet e outras fontes abertas. Essas informações podem ser utilizadas para identificar ameaças em potencial, mapear redes criminosas e entender tendências e padrões de atividades ilícitas.

Desafios da OpSec para Operações de Inteligência de Segurança Pública:

- Ameaças Cibernéticas: as operações de inteligência de segurança pública estão cada vez mais dependentes de tecnologias digitais para coletar e analisar informações. Isso as torna vulneráveis a ataques cibernéticos, como phishing, malware e ataques de negação de serviço, que podem comprometer a segurança das informações e interromper as operações.
- Vazamento de Informações: a divulgação não autorizada de informações confidenciais pode comprometer investigações em andamento, expor fontes confidenciais e colocar em risco a segurança de agentes e informantes.
- Infraestrutura Física Vulnerável: as instalações utilizadas pelas operações de inteligência de segurança pública, como centros de comando e bases de operações, podem ser alvos de ataques físicos, como invasões e sabotagem, representando uma ameaça à continuidade das operações e à segurança dos envolvidos.

1.1.2 Open-Source Intelligence (OSINT)

A OSINT refere-se à coleta e análise de informações que estão disponíveis publicamente para identificar ameaças e oportunidades. Essa prática é extremamente valiosa para os órgãos de segurança pública, pois permite o monitoramento de fontes abertas, como redes sociais, *websites*, fóruns, e bases de dados, para coletar dados que podem indicar atividades ilícitas ou planos de ataques. O uso efetivo do OSINT pode auxiliar na prevenção de crimes e ataques cibernéticos, além de contribuir para a rápida resposta a incidentes de segurança.

Para enfrentar esses desafios, é fundamental a adoção de uma abordagem multidisciplinar que integre tecnologia avançada, análise de dados e colaboração entre agências. Ferramentas de análise de big data e aprendizado de máquina podem ser utilizadas para processar e analisar grandes volumes de informações de OSINT, enquanto a criptografia e a segurança de redes são essenciais para reforçar o OpSec. A formação e o treinamento contínuo de profissionais de segurança também são cruciais para desenvolver habilidades avançadas.

A OSINT permite às agências de segurança pública acessarem uma grande quantidade de informações disponíveis publicamente na internet, incluindo dados geoespaciais, registros públicos, postagens em redes sociais e notícias online. A análise de dados da OSINT pode ajudar na identificação de ameaças emergentes, como protestos, distúrbios civis e atividades criminosas, permitindo uma resposta proativa por parte das autoridades.

Pode ser usada para coletar evidências digitais, identificar suspeitos e mapear redes criminosas, complementando as investigações tradicionais realizadas pelas agências de segurança pública. As ferramentas de OSINT permitem o monitoramento contínuo de eventos em tempo real, como desastres naturais, incidentes de segurança e movimentos sociais, facilitando a tomada de decisões informadas pelas autoridades.

Desafios da OSINT em Inteligência de Segurança Pública:

- Volume e veracidade dos dados: lidar com grandes volumes de dados da OSINT pode ser desafiador, e nem sempre é fácil verificar a autenticidade e a veracidade e a autenticidade das informações coletadas.

- Análise e interpretação de dados: a análise de dados da OSINT requer habilidades especializadas para interpretar informações complexas e identificar padrões significativos, destacando a necessidade de treinamento adequado para os analistas de inteligência.

1.1.3 ROI (Return Over Investment) do adversário

A inteligência estratégica desempenha um papel crucial na prevenção e resposta a ameaças à segurança pública. Para avaliar adequadamente o impacto dessas operações, é essencial considerar o ROI (Retorno do Investimento) do adversário, ou seja, a eficácia das medidas tomadas em resposta às informações coletadas sobre as ações e estratégias dos adversários.

A análise do ROI do adversário na segurança pública é essencial para entender

como as organizações criminosas operam, alojam recursos e desenvolvem suas capacidades. Isso permite que as agências de segurança pública aloquem recursos de forma mais eficaz, identificando áreas de vulnerabilidade e priorizando esforços de combate ao crime.

- ROI Tradicional vs. ROI do Adversário: enquanto o ROI tradicional se concentra nos benefícios financeiros diretos de um investimento, o ROI do adversário avalia os benefícios decorrentes da capacidade de antecipar e neutralizar as ações dos adversários, incluindo criminosos, terroristas e outros agentes de ameaça à segurança pública.

- Benefícios Tangíveis e Intangíveis: o ROI do adversário pode incluir benefícios tangíveis, como a redução do crime, o aumento da segurança da comunidade e a economia de recursos, bem como benefícios intangíveis, como a dissuasão de atividades criminosas e o fortalecimento da capacidade de resposta a ameaças.

Os Métodos de Cálculo do ROI (Retorno sobre Investimento) do Adversário no contexto da segurança pública pode ser desafiador devido à natureza multifacetada dos resultados e à dificuldade de quantificar certos aspectos.

- Análise de Custos-Benefícios: avaliação dos custos associados à coleta e análise de inteligência, em comparação com os benefícios resultantes da prevenção de crimes e da mitigação de ameaças.

- Análise de Impacto: exame dos efeitos das operações de inteligência na redução de crimes específicos, na desarticulação de organizações criminosas e na melhoria da segurança geral da comunidade.

- Avaliação Qualitativa: consideração dos benefícios intangíveis da inteligência estratégica, como a percepção pública de segurança, o fortalecimento da capacidade de respostas.

Avaliar o Retorno sobre o Investimento (ROI) do adversário na segurança pública apresenta uma série de desafios e limitações, muitos dos quais são inerentes à natureza da própria segurança pública e à dinâmica dos adversários envolvidos.

- Dificuldade na Quantificação de Benefícios: muitos dos benefícios da inteligência estratégica são difíceis de quantificar, especialmente os intangíveis, o que pode dificultar a análise do ROI do adversário.

- Incerteza e Variabilidade: a eficácia das operações de inteligência pode variar de acordo com a natureza e a gravidade das ameaças, bem como com a capacidade

dos adversários de se adaptarem e evitarem a detecção.

• Avaliação Pós-evento: em muitos casos, a verdadeira eficácia das operações de inteligência só pode ser avaliada após a ocorrência de um evento, o que torna desafiadora a avaliação do ROI do adversário em tempo real.

1.1.4 Desafios e estratégias na Segurança Pública

A inteligência estratégica desempenha um papel fundamental na gestão e eficácia das operações de segurança pública. Este artigo analisa a importância da inteligência estratégica no contexto da segurança pública, destacando suas abordagens, métodos e o impacto na prevenção e combate ao crime. A coleta, análise e disseminação de informações estratégicas podem informar políticas, estratégias operacionais e intervenções táticas para melhorar a segurança da comunidade.

Um dos maiores desafios no campo da inteligência estratégica cibernética é a constante evolução das ameaças digitais. Adversários tornam-se cada vez mais sofisticados em suas técnicas, exigindo que as práticas de OpSec e OSINT sejam continuamente atualizadas e adaptadas. Além disso, a grande quantidade de dados gerados diariamente torna a coleta e análise de informações uma tarefa complexa.

O processo de inteligência estratégica envolve várias etapas, incluindo coleta de dados, análise de informações, produção de inteligência, disseminação e feedback, que são iterativos e contínuos. As abordagens para a coleta de inteligência estratégica incluem fontes abertas, fontes humanas, técnicas de vigilância e monitoramento, análise de dados e modelagem preditiva.

• Identificação de Ameaças e Tendências: a inteligência estratégica permite às autoridades identificar ameaças emergentes, padrões criminais e tendências sociais que podem impactar a segurança da comunidade.

• Formulação de Políticas e Estratégias: as informações geradas pela inteligência estratégica informam a formulação de políticas públicas e estratégias operacionais para prevenir e combater o crime, promover a segurança comunitária e proteger os cidadãos.

• Apoio a Operações e Intervenções: a inteligência estratégica fornece suporte operacional às agências de segurança pública, ajudando na alocação de recursos, planejamento de operações e condução de investigações criminais.

1.2 Aspectos Conceituais

A inteligência estratégica na segurança pública, quando combinada com princípios como Segurança Operacional (OpSec), Inteligência de Fontes Abertas (OSINT) e análise do Retorno sobre o Investimento (ROI) do adversário, desempenha um papel essencial na prevenção e resposta eficaz às ameaças emergentes. Para entender melhor esses aspectos, é fundamental compreender o ciclo de inteligência e como ele se aplica ao contexto da ameaça.

1.2.1 Ciclo da Inteligência

O ciclo de inteligência é um processo fundamental para transformar dados brutos em inteligência acionável, pronta para ser utilizada por decisores. Este processo garante que as atividades sejam direcionadas de forma eficiente para atender às necessidades do consumidor. Embora o ciclo de inteligência geralmente seja composto por quatro fases, ele é cíclico, permitindo revisões contínuas para garantir que o material necessário seja processado e entregue de maneira adequada, mantendo sempre as necessidades do consumidor no centro das operações.

O ciclo de inteligência, segundo Nascimento et al. (2023), se configura como um processo cíclico e contínuo composto por cinco etapas interdependentes: planejamento, coleta, processamento, análise e difusão. A análise de riscos se insere de forma transversal em todas as etapas do ciclo, fornecendo subsídios para a tomada de decisões estratégicas no âmbito da segurança pública.

No contexto da inteligência de ameaças cibernéticas, o ciclo de inteligência é dividido em cinco etapas distintas, conforme definido pelo *CREST Cyber Threat Intelligence:*

1. Direção: nesta fase inicial, a organização estabelece seus objetivos e determina quais informações são necessárias para entender e mitigar as ameaças.

2. Coleta: durante esta etapa, a organização reúne informações relevantes sobre ameaças cibernéticas de uma variedade de fontes, incluindo feeds de notícias, relatórios de segurança, redes sociais e plataformas especializadas de inteligência de ameaças.

3. Processamento: as informações coletadas são organizadas e analisadas para identificar tendências, padrões e indicadores de comprometimento que possam indicar atividades maliciosas.

4. Análise: nesta etapa crítica, as informações processadas são avaliadas para identificar ameaças específicas que representam um risco significativo para a

organização. Isso envolve a avaliação do potencial impacto das ameaças e a probabilidade de sua ocorrência.

5. Disseminação: as informações analisadas são compartilhadas com os tomadores de decisão dentro da organização, permitindo que eles ajam proativamente para se proteger contra as ameaças identificadas.

Essas etapas fornecem uma estrutura clara para a coleta, análise e disseminação de inteligência de ameaças cibernéticas, permitindo que as organizações identifiquem e respondam efetivamente a incidentes e vulnerabilidades no ambiente.

1.2.2 Correlação e extração de Inteligência na Segurança Pública

Na segurança pública, a correlação e extração de inteligência desempenham um papel essencial na identificação de padrões, tendências e ameaças, permitindo às autoridades antecipar incidentes e tomar medidas proativas para garantir a segurança da comunidade. Esses processos envolvem a análise de uma ampla gama de dados e informações, tanto internas quanto externas, para produzir insights valiosos que informam as operações e políticas de segurança pública.

A correlação de dados na segurança pública envolve a análise e conexão de informações provenientes de diversas fontes, como relatórios de incidentes, registros criminais, vídeos de vigilância, dados de redes sociais e registros de comunicações. Através da correlação, os analistas buscam identificar padrões e relações entre eventos, pessoas e locais, permitindo uma compreensão mais abrangente da atividade criminosa e da dinâmica social em uma determinada área.

- Por exemplo, a correlação de dados pode ajudar a identificar associações entre indivíduos envolvidos em atividades criminosas, mapear rotas de fuga de criminosos ou detectar áreas geográficas com maior incidência de crimes. Além disso, a correlação de dados pode revelar tendências sazonais ou comportamentais, ajudando as autoridades a ajustarem suas estratégias de policiamento e prevenção.

A extração de inteligência na segurança pública envolve o processo de analisar dados brutos e transformá-los em informações acionáveis e significativas. Isso pode incluir a identificação de indicadores-chave de desempenho, a avaliação de ameaças potenciais e a previsão de padrões futuros com base em dados históricos.

- Por exemplo, os dados coletados de fontes abertas, como mídias sociais e fóruns online, podem ser analisados para identificar atividades suspeitas ou discursos de ódio que possam representar uma ameaça à segurança pública. Da mesma

forma, a análise de dados criminais pode ajudar a identificar *modus operandi* comuns usados por determinados grupos criminosos, permitindo uma resposta mais eficaz por parte das autoridades.

A correlação e extração de inteligência são fundamentais para o trabalho das agências de segurança pública em várias áreas, incluindo policiamento preventivo, investigações criminais, resposta a emergências e formulação de políticas de segurança. Ao entender os padrões e tendências subjacentes aos incidentes de segurança, as autoridades podem desenvolver estratégias mais eficazes para proteger a comunidade e prevenir a ocorrência de crimes.

Também desempenham um papel importante na identificação de lacunas de segurança e na alocação eficiente de recursos para áreas de maior necessidade. Ao analisar e contextualizar os dados disponíveis, as autoridades podem tomar decisões informadas e baseadas em evidências que promovam a segurança e o bem-estar da população.

1.2.3 Níveis da Inteligência na Segurança Pública

Na segurança pública, os diferentes níveis de inteligência são essenciais para apoiar a tomada de decisões em diferentes contextos e escalas. Esses níveis variam desde o operacional, que lida com questões imediatas e específicas, até o político, que aborda preocupações mais amplas e de longo prazo.

- Inteligência Operacional: a inteligência operacional concentra-se nas atividades diárias e operacionais das agências de segurança pública. Ela fornece informações detalhadas e específicas sobre incidentes, atividades criminosas e operações em andamento. Os analistas operacionais coletam, processam e analisam dados em tempo real para apoiar as operações policiais, identificar ameaças imediatas e orientar a resposta a emergências. Essa inteligência é fundamental para as unidades de patrulha, investigação criminal e outras equipes operacionais no terreno.

- Inteligência Tática: a inteligência tática está relacionada à tomada de decisões em níveis intermediários de comando e planejamento. Ela aborda questões específicas de curto a médio prazo, como a identificação de padrões criminais em determinadas áreas, a análise de atividades de gangues ou a coordenação de operações especiais. A inteligência tática é utilizada por supervisores de unidades, investigadores de crimes especializados e equipes de resposta rápida para direcionar recursos e desenvolver estratégias de curto prazo.

- Inteligência Estratégica: a

inteligência estratégica tem uma perspectiva mais ampla e abrangente, voltada para questões de longo prazo e políticas de segurança pública. Ela visa entender as tendências sociais, econômicas e criminais que afetam uma comunidade ou região e desenvolver estratégias de prevenção de crimes e promoção da segurança a longo prazo. Os analistas estratégicos coletam e analisam dados de longo prazo para informar políticas públicas, alocação de recursos e programas de prevenção de crimes. Essa inteligência é utilizada por líderes de alto escalão em agências de segurança pública e formuladores de políticas para orientar a direção geral das iniciativas de segurança.

• Inteligência Política: a inteligência política aborda questões ainda mais amplas e complexas relacionadas à segurança pública. Ela envolve a análise de fatores políticos, sociais, econômicos e culturais que influenciam as políticas de segurança e a governança em nível local, estadual ou nacional. A inteligência política é utilizada por líderes políticos, legisladores e formuladores de políticas para entender as necessidades da comunidade, antecipar tendências futuras e desenvolver estratégias abrangentes para promover a segurança e o bem-estar da população.

Esses diferentes níveis de inteligência na segurança pública trabalham em conjunto para fornecer uma compreensão abrangente das ameaças e desafios enfrentados pelas comunidades, permitindo respostas eficazes em todos os níveis de comando e governança.

CONCLUSÃO

Diante da crescente complexidade e sofisticação das ameaças à segurança pública nos últimos anos, a importância de estratégias avançadas de inteligência tornou-se cada vez mais evidente. A inteligência estratégica, aliada a abordagens como Segurança Operacional (OpSec), Inteligência de Fontes Abertas (OSINT) e análise do Retorno sobre o Investimento (ROI) do adversário, emergiu como um pilar fundamental para fortalecer as defesas e aumentar a eficácia das operações de segurança pública. Este artigo procurou explorar essa importância, destacando como técnicas como OpSec, OSINT e análise do ROI do adversário podem ser implementadas para proteger comunidades, antecipar ameaças e promover a segurança em sociedade.

Com o avanço tecnológico e a crescente sofisticação das ameaças, as agências de segurança pública enfrentam um ambiente operacional cada vez mais desafiador. Nesse contexto, a inteligência estratégica surge como uma ferramenta crucial para antecipar e responder a ameaças emergentes, garantindo o bem-estar da

população. Integrando os princípios da OpSec, aproveitando os recursos da OSINT e compreendendo o ROI do adversário, as agências podem tomar decisões informadas e eficazes, adotando uma abordagem proativa para enfrentar os desafios contemporâneos de segurança.

Ao longo deste artigo, exploramos como essas abordagens podem ser aplicadas de maneira prática e eficiente no contexto da segurança pública. Ao fazê-lo, destacamos a importância de se adaptar e evoluir constantemente para enfrentar as ameaças em constante mutação, garantindo assim a segurança e proteção de nossas comunidades.

REFERÊNCIAS

CTIPs. CREST. O que é inteligência contra ameaças cibernéticas e como ela é usada? 2019. Disponível em: <https://www.crest-approved.org/wp- content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf>. Acesso em: 10 fev. 2024.

DO NASCIMENTO, C. A., das Chagas, F. F., & Neto, L. N. (2023). Contribuições da análise de riscos ao assessoramento estratégico de inteligência de segurança pública: perspectivas voltadas ao enfrentamento às organizações criminosas. Revista Brasileira de Ciências Policiais, 14(12), 125-150.

WATTERS, P. A. (2023). *The Cyber Operational Environment. In Counterintelligence in a Cyber World* (pp. 19-29). *Cham: Springer International Publishing*.

ALSMADI, I. (2023). *Cyber operational planning. In The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics* (pp. 131-178). *Cham: Springer International Publishing*.

DANCIU, D. (2023). *Social Media and the Security of Military Operations*. Studia Securitatis, 17(2), 242-249.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

A REESTRUTURAÇÃO DO SISTEMA BRASILEIRO DE INTELIGÊNCIA (SISBIN) E SUAS IMPLICAÇÕES PARA O SUBSISTEMA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA (SISP)

Fillipe Augusto da Silva*

RESUMO

Com a missão de integrar as ações de planejamento e execução da Atividade de Inteligência do país, o Sistema Brasileiro de Inteligência (Sisbin) remete à ideia original de organização, controle e gerenciamento entre os órgãos da comunidade de Inteligência. Na esteira da criação do Sisbin e diante da necessidade de uma estrutura que atendesse às demandas específicas em Segurança Pública, o Decreto n° 3.695/2000 instituiu o Subsistema Brasileiro de Inteligência de Segurança Pública (Sisp), vinculado ao Sisbin. Em setembro de 2023, em ato publicado pelo Presidente da República, o Decreto nº 11.693/2023 instituiu a reestruturação do Sisbin, com importantes inovações conceituais e práticas. Este artigo busca discutir, através de pesquisa de natureza exploratória, baseada em levantamento bibliográfico especializado, quais são as implicações desta nova formatação do Sisbin para a Atividade de Inteligência no Brasil, em especial para a Inteligência de Segurança Pública. Como resultado, foram apontadas as principais implicações para o Sisp, como uma atuação mais integrada entre órgãos e entidades de Inteligência; o fortalecimento do intercâmbio de dados, informações e conhecimentos; o desenvolvimento de ferramentas seguras de comunicação e troca de documentos; e uma maior participação das Unidades da Federação em ações de Inteligência. Em vista das oportunidades e dos desafios apontados neste estudo, torna-se fundamental que as autoridades de segurança estejam comprometidas em promover a efetiva implementação e utilização das inovações propostas pelo Decreto nº 11.693/2023.

Palavras-chave: Sistema Brasileiro de Inteligência; Subsistema de Inteligência de Segurança Pública; Sisbin; Sisp.

* Mestre em Segurança Internacional e Defesa, pela Escola Superior de Guerra (ESG). Atualmente cursa o Doutorado Profissional em Políticas Públicas, pela Escola Nacional de Administração Pública (ENAP). Servidor Público Federal lotado na Casa Civil da Presidência da República (CC/PR). Endereço eletrônico: fillipeas92@gmail.com

THE RESTRUCTURING OF THE BRAZILIAN INTELLIGENCE SYSTEM (SISBIN) AND ITS IMPLICATIONS FOR THE PUBLIC SECURITY INTELLIGENCE SUBSYSTEM (SISP)

ABSTRACT/RESUMEN

With the mission of integrating the planning and execution actions of the country's Intelligence Activity, the Brazilian Intelligence System (Sisbin) refers to the original idea of organization, control and management between the bodies of the Intelligence community. Following the creation of Sisbin and given the need for a structure that met specific Public Security demands, Decree No. 3,695/2000 established the Brazilian Public Security Intelligence Subsystem (Sisp), linked to Sisbin. In September 2023, in an act published by the President of the Republic, Decree No. 11,693/2023 instituted the restructuring of Sisbin, with important conceptual and practical innovations. This article seeks to discuss, through research of an exploratory nature, based on a specialized bibliographical survey, what are the implications of this new format of Sisbin for Intelligence Activity in Brazil, especially for Public Security Intelligence. As a result, the main implications for Sisp were highlighted, such as more integrated action between Intelligence bodies and entities; strengthening the exchange of data, information and knowledge; the development of secure communication and document exchange tools; and greater participation of Federation Units in Intelligence actions. In view of the opportunities and challenges highlighted in this study, it is essential that security authorities are committed to promoting the effective implementation and use of the innovations proposed by Decree No. 11,693/2023.

Keywords*: Brazilian Intelligence System; Public Security Intelligence Subsystem; Sisbin; Sisp.*

INTRODUÇÃO

A sensação de insegurança generalizada observada por grande parte da população brasileira decorre principalmente da presença da criminalidade permeando diversos estratos e setores da sociedade. Além de sua natureza organizada, grupos criminosos têm estabelecido colaborações entre si, resultando na formação de verdadeiros conglomerados transnacionais dedicados à prática de atividades ilícitas, fato que demanda uma resposta mais eficaz por parte do Estado.

O Brasil possui um sistema de Segurança Pública bastante robusto, com a divisão de responsabilidades entre a União, os Estados e os Municípios para preservação da ordem pública. Essa missão, portanto, envolve dezenas de órgãos e desafios que perpassam as fronteiras e os limites das Unidades da Federação (ARAÚJO; JÚNIOR, 2023). Neste contexto, a Segurança Pública no Brasil é caracterizada por um conjunto de sistemas adaptativos complexos, marcado pela existência de um grupo diverso de agentes, que interagem entre si de maneira intensa, mas que atuam de maneira autônoma (BORGES, 2020).

Diante de tal complexidade, o combate ao crime organizado não pode ser feito exclusivamente por atividades de caráter policial. Assim, a Atividade de Inteligência surge como importante ferramenta para criação e planejamento de uma política de Segurança Pública mais efetiva. A produção de conhecimentos de Inteligência pode auxiliar no mapeamento da criminalidade, identificação de atores, seus *modus operandi* e demais informações para uma leitura real de cenários, o que possibilita ao decisor adotar medidas mais efetivas de prevenção e combate à criminalidade (PATRÍCIO, 2006).

1 INTELIGÊNCIA DE SEGURANÇA PÚBLICA

A Inteligência de Segurança Pública (ISP) representa exatamente este instrumento estatal que fornece apoio e aprimora a abordagem contra a criminalidade, especialmente aquela de natureza organizada. A ISP pode ser definida como ações especializadas para 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, além das ações para prevenir, neutralizar e reprimir atos criminosos de qualquer natureza, de forma integrada e em subsídio à investigação e à produção de conhecimentos (BRASIL, 2009).

A ISP pode ser analisada, portanto, sob dois prismas: um de natureza tática,

relacionada à prevenção direta de práticas delituosas e repressão criminal; e outro de essência estratégica, vinculada à análise de cenários e prospecção, em apoio ao planejamento e à execução de políticas públicas na área de segurança. A importância dada à criminalidade organizada decorre da real ameaça que esta representa ao Estado Democrático de Direito, usurpando suas funções e explorando cenários de caos urbano e político para estabelecer seu domínio paralelo (BARBOSA, 2011).

No Brasil, a ISP é regida pela Doutrina Nacional de Inteligência de Segurança Pública (DNISP), normatizada pela Portaria nº 22 da Secretaria Nacional de Segurança Pública (SENASP), de 22 de julho de 2009. Tendo a Constituição Federal como seu principal suporte, a DNISP trata do conjunto de conceitos, características, princípios, valores, normas, métodos, procedimentos, ações e técnicas que orientam e disciplinam a atividade de ISP (BRASIL, 2009). Em 2016, foi publicada a 4ª versão revisada da DNISP, publicada pela Portaria nº 2 da SENASP.

2 SISTEMAS DE INTELIGÊNCIA

O conjunto de organismos de Inteligência de um país constitui a chamada Comunidade de Inteligência, expressão que denota, no entanto, a natureza informal e fática das interações porventura existentes. Quando a Comunidade de Inteligência de um país está submetida, total ou parcialmente, a normativos formais e institucionalizados que regem sua interação, é constituído um Sistema de Inteligência (BRASIL, 2023). No Brasil, os órgãos de Inteligência são regidos por um sistema próprio definido legalmente, o Sistema Brasileiro de Inteligência (Sisbin), instituído pela Lei nº 9.883/1999.

Na esteira da criação do Sisbin e diante da necessidade de uma estrutura que atendesse às demandas específicas em Segurança Pública, o Decreto n° 3.695/2000 instituiu o Subsistema Brasileiro de Inteligência de Segurança Pública (Sisp), com a finalidade de "coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e estaduais de informações que subsidiem a tomada de decisões neste campo" (BRASIL, 2000). Em síntese, a ISP, no Brasil, é coordenada pelo Sisp, que é um subsistema vinculado ao Sisbin.

A própria concepção de um sistema remete à ideia de organização, controle e gerenciamento de alguma atividade, sobretudo aquelas que atuam em um cenário complexo, como o caso da Inteligência. Ao definir essa estrutura, suas atribuições e os mecanismos de exercício, a atividade de Inteligência torna-se mais eficiente e compatível com os princípios do Estado Democrático de Direito (MAIA; COLA, 2021). Apesar do importante papel de

institucionalização da Inteligência no Brasil, o Sisbin enfrentou, desde sua concepção, importantes desafios práticos, principalmente relacionados à integração de seus membros e ao compartilhamento de dados, informações e conhecimentos.

Em setembro de 2023, em ato publicado pelo Presidente da República, o Decreto 11.693/2023 instituiu a reestruturação do Sisbin. Neste contexto, cabe discutir quais são as implicações dessa nova formatação do Sistema para a Atividade de Inteligência no Brasil, em especial para a ISP. Para isso, foi realizada pesquisa de natureza exploratória, baseada em levantamento bibliográfico especializado, com o intuito de discutir a estrutura do novo Sisbin, as implicações para o Sisp e os desafios e perspectivas que se impõem à nova estrutura da Inteligência brasileira.

3 ESTRUTURA E ORGANIZAÇÃO DO NOVO SISBIN

Com o objetivo principal de integrar as ações de planejamento e execução da atividade de Inteligência do País, além de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional, o Sisbin abrange os órgãos e entidades que desenvolvem, de forma integrada e cooperativa, ações de planejamento e execução das atividades de Inteligência e Contrainteligência no Brasil. Entre as principais inovações da nova norma, destacam-se: (I) a classificação dos órgãos em categorias; (II) a definição de critérios e procedimentos para a efetiva inclusão de novos membros no Sisbin; e (III) o reposicionamento do Conselho Consultivo, tornando-o uma estrutura consultiva de alto nível formada por Ministros de Estado.

3.1 Categorias de órgãos

Além de fortalecer o papel de facilitador e coordenador da Agência Brasileira de Inteligência (ABIN) como órgão central do sistema, o Decreto nº 11.693/2023 atribuiu diferentes categorias para seus órgãos integrantes, nos seguintes termos:

QUADRO 1: CATEGORIAS DE ÓRGÃOS DO SISBIN

Órgãos Permanentes	Aqueles que expressam as funções essenciais do poder do Estado, com competências relativas à governabilidade, à defesa externa, à segurança interna e às relações exteriores do País.
Órgãos Dedicados	Órgãos e entidades do Poder Executivo Federal com unidades dedicadas às atividades de Inteligência e que atuam em assuntos estratégicos relacionados a temas da Política Nacional de Inteligência.
Órgãos Associados	Órgãos e entidades do Poder Executivo Federal que não possuem unidades ou frações dedicadas à Inteligência, mas atuam em assuntos estratégicos relacionados à Política Nacional de Inteligência.
Órgãos Federados	Órgãos e entidades das Unidades da Federação, que integram o Sisbin, ouvido o órgão de controle externo da atividade de Inteligência.

Fonte: adaptado do Decreto nº 11.693/2023.

A nova estrutura, além de dar maior organicidade ao Sistema, acaba por ajustar as expectativas na participação dos órgãos em relação à obtenção e à integração de dados, informações e conhecimentos, conforme previsão em planos de trabalho específicos para cada membro. Ainda de acordo com o texto da normativa, o Diretor-Geral da ABIN editará ato com o rol dos órgãos e das entidades que integram o Sisbin sempre que ocorrer mudanças, com a indicação de suas respectivas categorias.

3.2 Critérios para entrada

Qualquer órgão ou entidade do Poder Executivo Federal e das Unidades da Federação poderá solicitar ao Órgão Central o ingresso no Sisbin, observados os seguintes critérios: (I) competências que o órgão exerce e sua correlação com temas da Política Nacional de Inteligência; (II) sensibilidade dos dados, das informações e dos conhecimentos a serem compartilhados ou potencialmente acessados pelo órgão; (III) padrão de segurança adotado no órgão; e (IV) recursos disponíveis de pessoal, suporte tecnológico e estrutura organizacional (BRASIL, 2023).

Para os pedidos de ingresso de novos órgãos no Sisbin em âmbito federal, a ABIN deverá ouvir os Órgãos Permanentes, que terão o prazo de, pelo menos, cinco dias úteis para suas manifestações. Para o ingresso de órgãos das Unidades da Federação (Órgãos Federados), também será ouvida a Comissão Mista de Controle das Atividades de Inteligência (CCAI), colegiado do Poder Legislativo responsável pelo controle externo da Inteligência no Brasil. Também está prevista a possibilidade de alteração de categoria de Órgãos Associados para o nível imediatamente superior (Órgãos Dedicados), caso os critérios exigidos sejam atendidos.

3.3 Conselho Consultivo do SISBIN

Na reestruturação do Sisbin, o Conselho Consultivo ganhou maior relevância, tornando-se uma estrutura consultiva de alto nível formada por Ministros de Estado das seguintes pastas: Casa Civil (CC/PR, que o presidirá); Gabinete de Segurança Institucional (GSI/PR); Ministério da Justiça e Segurança Pública (MJSP); Ministério das Relações Exteriores (MRE); Ministério da Defesa (MD); além da Agência Brasileira de Inteligência (ABIN, que exercerá papel de Secretaria-Executiva).

O colegiado, que se reúne ao menos duas vezes por ano em caráter ordinário, desempenha um papel importante ao oferecer assessoramento estratégico ao Presidente da República no âmbito da segurança e inteligência nacional. Em suas reuniões, o Conselho Consultivo do Sisbin também pode convidar cidadãos com notório saber e especialistas em assuntos específicos, fornecendo análises sólidas e recomendações

fundamentadas sobre questões relacionadas à segurança do país.

4 IMPLICAÇÕES PARA O SISP

Apesar de ser constituído de rede própria, possuir escopo de atuação bem definido e objetivos estabelecidos em norma específica, o Sisp responde legalmente às necessidades do Sisbin no que se refere à segurança pública, conforme disposto em seu decreto de criação (BRASIL, 2000). Assim, uma reestruturação do Sisbin tende a exercer influência direta em uma governança mais robusta e eficiente também no âmbito da ISP, conforme discutido nos tópicos a seguir.

4.1 Integração de órgãos e entidades

A integração representa um fator determinante para o sucesso de ações de combate sistemático ao crime organizado. Após o ciclo de grandes eventos realizados no Brasil, desenvolveu-se um empirismo acerca da integração de diferentes órgãos, em face da lacuna legislativa que, apesar de fomentar a integração, não disciplinava como esta deveria ocorrer. Apesar de representar um marco em relação a investimentos e promoção da cultura de atuação integrada e colaborativa, verificou-se que as interações muitas vezes eram afetadas por questões de cunho pessoal, desprendidas dos princípios que regem a Administração Pública (RIBEIRO; JÚNIOR; SILVA, 2023).

Neste aspecto, o Decreto nº 11.693/2023 inova ao trazer a figura dos Centros Integrados de Inteligência, que podem ocorrer de forma esporádica ou sistemática, para fomentar a cooperação entre os órgãos e as entidades integrantes do Sisbin. A publicação de atos complementares ao Decreto pode dispor de forma mais específica sobre essas estruturas. Na área de Segurança Pública, cinco Centros Integrados de Inteligência de Segurança Pública (CIISP) já estão estabelecidos em todas as regiões do país, além do CIISP Nacional, em Brasília/DF, que representam uma importante rede de cooperação da ISP (ARAÚJO; JÚNIOR, 2023).

4.2 Compartilhamento de dados, informações e conhecimentos

O compartilhamento de dados, informações e conhecimentos representa um dos principais processos da Atividade de Inteligência. Na prática, o compartilhamento de capacidades permite que informações, que de forma isolada não teriam o mesmo impacto de análise, sejam utilizadas de maneira mais abrangente e integrada, resultando em uma análise holística da situação (BEZERRA; LIMA, 2023).

Diversos autores já descreveram os principais obstáculos para uma efetiva troca de informações entre os órgãos de Inteligência, como: (I) cultura de

compartimentalização excessiva; (II) ideia institucional de desconhecimento da atividade de Inteligência; (III) critérios pessoais de interação prevalecendo sobre critérios institucionais; (IV) ausência de uma linguagem compartilhada; e (V) diferenças de culturas organizacionais (GONÇALVES, 2003; MELO; URPIA; SARTORI, 2021; JÚNIOR; RAMOS, 2022; RIBEIRO; JÚNIOR; SILVA, 2023; BEZERRA; LIMA, 2023).

Sobre este aspecto, o Art. 6º do novo Decreto do Sisbin determina que: "os órgãos e as entidades integrantes do Sisbin poderão compartilhar dados, informações e conhecimentos e conceder acesso a bancos de dados, observadas as diretrizes do Órgão Central do Sisbin, o princípio da segurança jurídica, a necessidade de conhecer, o interesse público e a devida motivação". Essa redação, ausente na antiga norma, representa um importante passo para superar as barreiras para o compartilhamento efetivo de informações e, como consequência, a atuação interagências.

Na ISP, algumas experiências de sucesso podem ser destacadas, como o Sistema Nacional de Integração de Informações em Justiça e Segurança Pública (INFOSEG), que representa uma ferramenta de integração de bancos de dados, facilitando a atuação das polícias na identificação de indivíduos com pendências criminais junto à Justiça (FERRO, 2006). Outro exemplo de sucessos são os próprios CIISP regionais, que disponibilizam aproximadamente 400 bases de dados entre seus integrantes (ARAÚJO; JÚNIOR, 2023). Essas experiências podem ser fortalecidas e multiplicadas com o novo texto instituído pelo Decreto do Sisbin.

4.3 Tecnologia e inovação

Ainda como parte importante da reestruturação do Sisbin, o Decreto nº 11.693/2023 determina como obrigação do órgão central do Sistema: "disponibilizar ferramentas para a comunicação segura e plataformas digitais para suporte ao compartilhamento de dados, informações e conhecimentos do Sisbin". Em última análise, essa obrigação reforça o compromisso da ABIN com o aperfeiçoamento da gestão e dos instrumentos de controle da Atividade de Inteligência (BRASIL, 2023).

Dos diversos obstáculos que dificultam a precisão da análise de Inteligência, aqueles inerentes às limitações do processo racional humano estão, certamente, entre os mais importantes e os mais difíceis de lidar. O uso da tecnologia da informação é capaz de sistematizar e impulsionar esse processo de análise, além de auxiliar nas atividades de coleta, busca e gerenciamento de dados, informações e conhecimentos de Inteligência.

Na ISP, demonstra-se ainda mais relevante esta carência por uma constante inovação tecnológica, buscando a atualização constante de métodos e recursos para que o Estado possa se adaptar às novas situações advindas de ações reais ou potenciais de organizações criminosas (MELO; URPIA; SARTORI, 2021). No entanto, a implementação dessa política pode encontrar diversos obstáculos, como a falta de recursos humanos, financeiros e materiais. Fato é que este compromisso assumido no âmbito do Sisbin pode favorecer também as atividades desenvolvidas no Sisp.

4.4 Órgãos Federados

A própria Lei nº 9.883/1999, que instituiu o Sisbin, já previa que Unidades da Federação pudessem compor o Sistema, mediante ajustes específicos e convênios. Na prática, entretanto, era através do Sisp que os órgãos estaduais, como as polícias civis e militares, estavam ligados ao Sisbin. Desse modo, a sistematização do fluxo de informações ocorria pela criação dos núcleos de gerenciamento de Inteligência estaduais nos moldes preconizados pelo Subsistema e inserção destes na rede do Sisbin (PATRÍCIO, 2006).

Com a publicação do novo Decreto, surgem duas figuras: a dos Órgãos Federados, que devem dar maior concretude à participação das Unidades da Federação, e a dos órgãos estaduais vinculados diretamente ao Sisbin. A medida é importante para fortalecimento, padronização e uniformidade das ações de ISP entre os diferentes estados, passo relevante na busca por uma atuação em rede e de integração entre órgãos estaduais de Segurança Pública de forma institucionalizada.

Avalia-se como tendência para os próximos anos o aumento do ingresso de órgãos de Segurança Pública e áreas correlacionadas no âmbito do Sisbin, como órgãos do sistema prisional, defesa civil, guardas municipais e polícias em geral. Tal movimento será relevante para sistematizar as trocas de dados e informações tático-operacionais, bem como desenvolver uma mentalidade de Inteligência entre os integrantes dos organismos estaduais de Segurança Pública.

CONCLUSÃO

A constante evolução das organizações criminosas no Brasil demanda uma abordagem especializada para a identificação, coleta, análise e compartilhamento de conhecimentos que possam orientar as intervenções por parte das autoridades de segurança. A ISP, por meio dos diversos órgãos que estão conectados através do Sisp e, por consequência, pelo Sisbin, constitui uma ferramenta diferenciada de abordagem para prevenção e repressão ao crime, notadamente pela criação de um

conhecimento tático e estratégico, com uma perspectiva macro e de longo prazo (BARBOSA, 2011; RIBEIRO; JÚNIOR; SILVA, 2023).

Matriz fundamental de todas as outras, é a Inteligência de Estado tradicionalmente utilizada no trato de grandes questões políticas e estratégicas de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado. Nessa perspectiva, a ISP representa um componente relevante de poder e de recurso de ação do Estado brasileiro na detecção e prevenção da criminalidade, tornando-se imprescindível ao aparato de controle de ameaças à sociedade e ao Estado brasileiros.

Neste sentido, as inovações trazidas pelo Decreto nº 11.693/2023 vão além de uma reforma do sistema nacional de Inteligência, mas também fortalecem de maneira concreta as ações de ISP no Brasil. Entre os principais aspectos citados neste estudo, destacam-se: (I) atuação mais integrada entre órgãos e entidades de Inteligência; (II) fortalecimento do intercâmbio de dados, informações e conhecimentos; (III) desenvolvimento de ferramentas de comunicação segura e de troca de documentos; e (IV) maior participação das Unidades da Federação em ações de Inteligência.

O decreto permite também a criação de atos complementares, como a regulamentação de protocolos de atuação integrada, a promoção da capacitação e do desenvolvimento de recursos humanos e a formação de câmaras técnicas e temáticas. Tendo sido o Sisp criado no âmbito do Sisbin, todos os produtos criados no âmbito do Sisbin beneficiarão também os órgãos que compõem o Subsistema. Entre os principais desafios, destacam-se as limitações orçamentárias e a criação de um ambiente centrado na confiança e na responsabilidade entre os órgãos.

Em vista das oportunidades e dos desafios apontados, torna-se fundamental que as autoridades de segurança estejam comprometidas em promover a efetiva implementação e utilização das inovações propostas pelo Decreto nº 11.693/2023. Além disso, é necessário investir na capacitação contínua dos profissionais da ISP, aprimorando suas habilidades técnicas e promovendo a troca de experiências e boas práticas. Com o fortalecimento do Sisbin e, consequentemente, do Sisp, o Brasil dá um passo importante na luta contra o crime organizado, construindo um ambiente de segurança mais robusto e resiliente.

REFERÊNCIA

ARAÚJO, Prigulin Andrade de; JÚNIOR, Erly Ribeiro Crispim. Cooperação interagências: Uma Análise do Programa de Proteção Integrada de Fronteiras (PPIF). Revista de Inteligência de Segurança Pública, Rio de Janeiro, v. 6, n. 6, p. 42-56, jun. 2023.

BARBOSA, Adriano Mendes. A Atividade de Inteligência de Segurança Pública. Revista Brasileira de Ciências Policiais, Brasília, v. 2, n. 1, p. 11-30, jun. 2011.

BEZERRA, Emerson Gustavo dos Santos; LIMA, Virginia Souza. A importância de um órgão coordenador na cooperação interagências no âmbito da Inteligência de segurança pública em grandes eventos: a experiência dos Jogos Olímpicos Rio 2016. Revista de Inteligência de Segurança Pública, Rio de Janeiro, v. 6, n. 6, p. 25-41, jun. 2023.

BORGES, Zeca. Segurança Pública e Complexidade. Revista de Inteligência de Segurança Pública, Rio de Janeiro, v. 2, n. 2, p. 105-111, dez. 2020.

BRASIL. Decreto nº 3.695, de 21 de dezembro de 2000. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências. Brasília: Presidência da República, 21 dez. 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3695.htm. Acesso em: 29 fev. 2024.

BRASIL. Resolução SENASP nº 1, de 15 de julho de 2009. Regulamenta o Subsistema de Inteligência de Segurança Pública - SISP, e dá outras providências. Brasília, jul. 2009.

BRASIL. Doutrina da Atividade de Inteligência. Brasília, 2023. p. 1-184. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023. Acesso em: 29 fev. 2024.

BRASIL. Decreto nº 11.693, de 6 de setembro de 2023. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. Brasília, set. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11693.htm. Acesso em: 29 fev. 2024.

FERRO, Alexandre Lima. Inteligência de Segurança Pública e Análise Criminal. Revista Brasileira de Inteligência, Brasília, v. 2, n. 2, p. 77-92, abr. 2006.

GONÇALVES, Joanisval Brito. A Atividade de Inteligência no Combate ao Crime Organizado: o Caso do Brasil. Center For Hemispheric Defense Studies, Santiago, v. 1, p. 1-19, out. 2003.

MAIA, Marcus Castro Nunes; COLA, Marcelo dos Santos Dias. As agências de Inteligência intermediárias e a sua importância para aperfeiçoamento do sistema de Inteligência da Secretaria de Estado de Polícia Civil do Rio de Janeiro. Revista de Inteligência de Segurança Pública, Rio de Janeiro, v. 3, n. 3, p. 9-25, dez. 2021.

MELO, Felipe Pereira; URPIA, Arthur Gualberto Bacelar; SARTORI, Rejane. A gestão do conhecimento como auxílio à Inteligência de Segurança Pública. Brazilian Journal of Development, [S.L.], v. 6, n. 12, dez. 2020.

MELO, Felipe Pereira; URPIA, Arthur Gualberto Bacelar; SARTORI, Rejane. O Compartilhamento de Conhecimentos entre as unidades de Inteligência de Segurança Pública no Estado do Paraná. Informação & Informação, [S.L.], v. 26, n. 3, p. 628, out. 2021.

PATRÍCIO, Josemária da Silva. Inteligência de Segurança Pública. Revista Brasileira de Inteligência, Brasília, v. 2, n. 3, p. 53-58, set. 2006.

RIBEIRO, Anna Carolina Mendonça Lemos; JÚNIOR, Almir de Oliveira; SILVA, Marcos Paulo Hyath. Uma visão crítica sobre a ausência de protocolo geral de integração de agências na Inteligência em Segurança Pública. Revista Brasileira de Inteligência, Brasília, v. 1, n. 18, p. 167-186, dez. 2023.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

CYBERCRIME-AS-A-SERVICE (CaaS): O Desafio da Terceirização do Cibercrime para a Atividade de Inteligência

Flávio Queiroz*

RESUMO

"*Cybercrime-as-a-Service*" (CaaS) é um modelo em que cibercriminosos oferecem habilidades, ferramentas e serviços de cibercrime, tornando-os acessíveis a indivíduos sem conhecimento técnico avançado. Isso inclui fraude financeira, malwares, ataques de negação de serviço, *ransomware*, *phishing* e engenharia social. Neste aspecto, há uma crescente dificuldade em distinguir entre grupos de cibercrime e grupos de espionagem cibernética patrocinados por Estados, conhecidos como Ameaças Persistentes Avançadas, que frequentemente compartilham recursos e técnicas. Aprofundando-se no modelo de negócios do CaaS, explora-se a cadeia de valor desse ecossistema, evidenciando como cibercriminosos monetizam suas operações e reduzem custos por meio de uma variedade de serviços ofensivos e de suporte. Considerando as competências funcionais, destaca-se a necessidade de profissionais de Inteligência de cibercrime possuírem habilidades específicas para lidar com este cenário complexo, focando na análise, pesquisa e produção de conhecimento acionável. O futuro da cibersegurança é apresentado como desafiador, com previsões de aumento nos custos do cibercrime e uma evolução nas ameaças cibernéticas, que se tornam mais diversas e complexas, exigindo uma abordagem proativa e adaptativa na defesa cibernética. Por fim, ressalta-se algumas das medidas preventivas, como melhorar a capacidade de Inteligência Cibernética, colaboração internacional, treinamento e conscientização, parcerias público-privadas e o uso de ferramentas avançadas para análise preditiva, enfatizando a necessidade de vigilância, inovação e colaboração contínuas no combate ao cibercrime.

Palavras-chave: Cibercrime; Cibercrime como serviço; Inteligência de Ameaças Cibernéticas.

[*]Mestre em computação pela Universidade Federal Fluminense, especialização em Política e Estratégia Cibernética pela Escola Superior de Guerra, especialização em Guerra Cibernética pelo Centro de Guerra Eletrônica do Exército, MBA em Cibersegurança pelo Ibmec e pós-graduação em Cloud Computing pela Universidade do Texas. Possui certificações profissionais gerenciais em segurança da informação e certificações técnicas em Threat hunting, Threat Intelligence, Threat modeling, SecOps e Gestão de incidentes. Foi coordenador de Equipe de Tratamento de Incidentes do Ministério da Defesa nos Jogos Olímpicos Rio 2016 e está há 9 anos à frente do setor de Threat Intelligence na Marinha. Endereço eletrônico: fl.queiroz@proton.me

CYBERCRIME-AS-A-SERVICE (CaaS): The Challenge of Cybercrime Outsourcing for Intelligence Activity

ABSTRACT/RESUMEN

"Cybercrime-as-a-Service" (CaaS) is a model where cybercriminals offer skills, tools, and cybercrime services, making them accessible to individuals without advanced technical knowledge. This includes financial fraud, malware, denial-of-service attacks, ransomware, phishing, and social engineering. In this regard, there is a growing difficulty in distinguishing between cybercrime groups and state-sponsored cyber espionage groups, known as Advanced Persistent Threats, which often share resources and techniques. Delving into the business model of CaaS, the value chain of this ecosystem is explored, highlighting how cybercriminals monetize their operations and reduce costs through a variety of offensive and support services. Considering functional competencies, there is a highlighted need for cybercrime intelligence professionals to possess specific skills to deal with this complex scenario, focusing on analysis, research, and the production of actionable knowledge. The future of cybersecurity is presented as challenging, with predictions of an increase in the cost of cybercrime and an evolution in cyber threats, which are becoming more diverse and complex, requiring a proactive and adaptive approach to cyber defense. Finally, some preventive measures are emphasized, such as improving Cyber Intelligence capabilities, international collaboration, training and awareness, public-private partnerships, and the use of advanced tools for predictive analysis, emphasizing the need for vigilance, innovation, and continuous collaboration in combating cybercrime.

Keywords*: Cybercrime; Cybercrime as a service; Cyber Threat Intelligence.*

1 A EVOLUÇÃO DO CRIME CIBERNÉTICO COMO SERVIÇO

A evolução do cibercrime passou de incidentes isolados que envolviam apenas ações individuais para uma operação "como serviço" a partir de um ecossistema complexo e hierárquico.

A expressão Cibercrime como Serviço, ou do inglês *Cybercrime-as-a-Service* (CaaS) refere-se a um modelo de atividade ilegal em que os cibercriminosos oferecem as suas competências, suas ferramentas e seus serviços a terceiros, muitas vezes através de sites especializados ou fóruns na *Dark Web*.

Este modelo permite que mesmo aqueles sem conhecimentos técnicos avançados se beneficiem com estas atividades criminosas, tornando-as mais acessíveis, incluindo fraude financeira, ataques por malwares, ataques distribuídos de negação de serviço, ou do inglês *Distributed Denial-of-Service* (DDoS), *ransomware, phishing* e engenharia social.

O CaaS funciona como um gerenciamento por estruturas organizadas para criar e vender ferramentas e serviços ofensivos explorando vulnerabilidades no ciberespaço. O crescimento e a sofisticação do modelo CaaS indicam uma ameaça crescente para usuários e organizações, provocando a atenção das agências de Inteligência (HEIMDAL SECURITY, 2023).

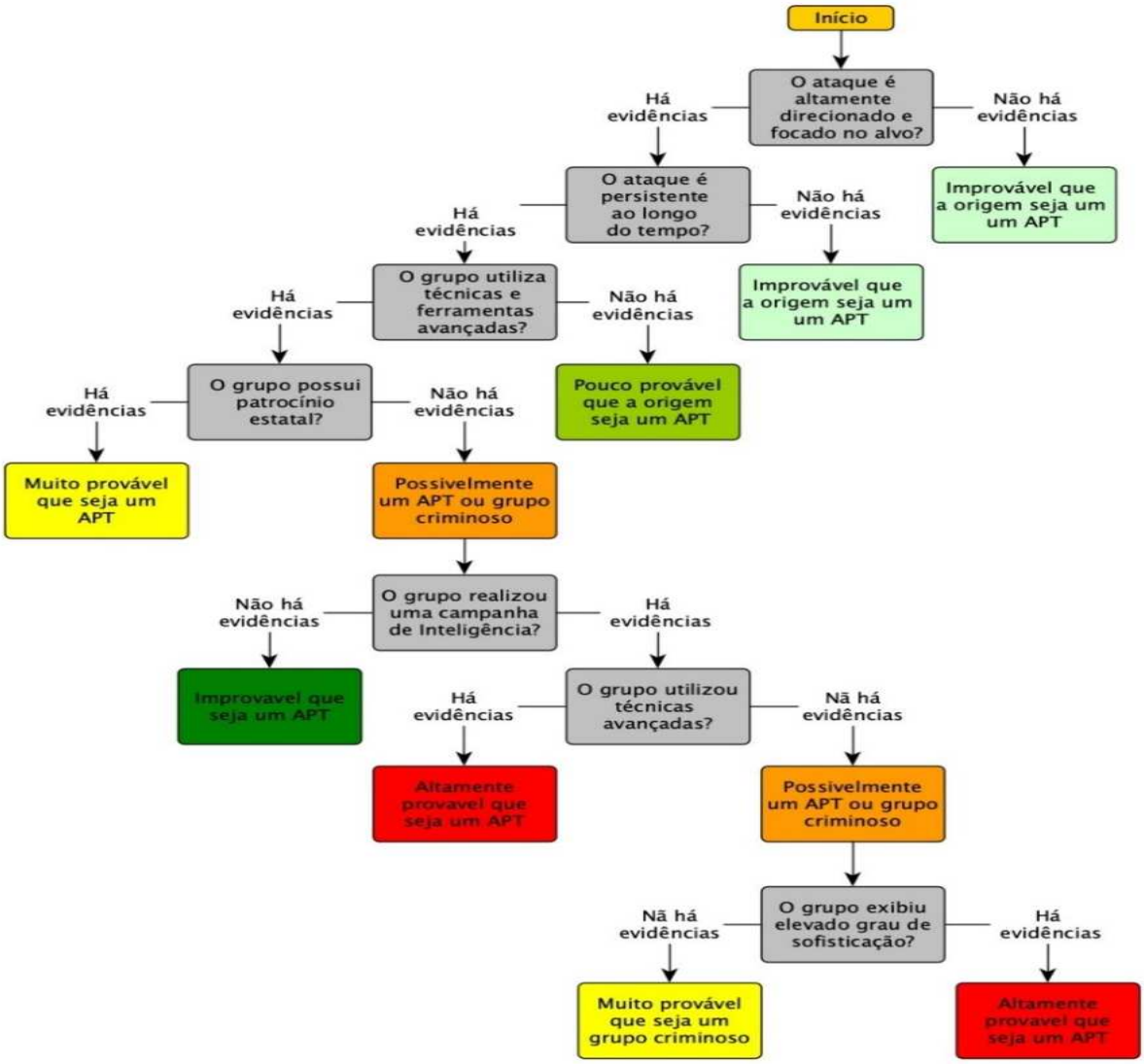
2 A DIFERENÇA ENTRE GRUPOS CRIMINOSOS E GRUPOS DE ESPIONAGEM CIBERNÉTICA

Com esta evolução, as fronteiras estão cada vez mais confusas entre os grupos de cibercrime e as atividades de grupos vinculados a Estados-nação, denominados Ameaças Persistentes Avançadas, ou do inglês *Advanced Persistent Threats* (APT), que combinam a utilização de técnicas avançadas, persistência, recursos humanos e financeiros significativos e seleção de alvos estratégicos, com ambos os grupos utilizando táticas, técnicas e procedimentos semelhantes e, ocasionalmente, a compartilharem recursos ofensivos.

O objetivo de um APT é muitas vezes a espionagem cibernética ou a sabotagem e não necessariamente o ganho financeiro. Esses grupos realizam campanhas prolongadas de vigilância e roubo de dados, visando a entidades específicas, como governos, organizações militares e corporações importantes (SHARMA et al. 2023). Esta complexidade no cenário do cibercrime representa desafios significativos para os profissionais de segurança pública e de Inteligência.

Na tentativa de contribuir para diferenciar grupos de cibercrimes e grupos de APT, definiu-se uma árvore de decisão (SOCRadar, 2023) com perguntas a partir das evidências coletadas de um incidente, ilustrada pela Figura 1

FIGURA 1 – ÁRVORE DE DECISÃO



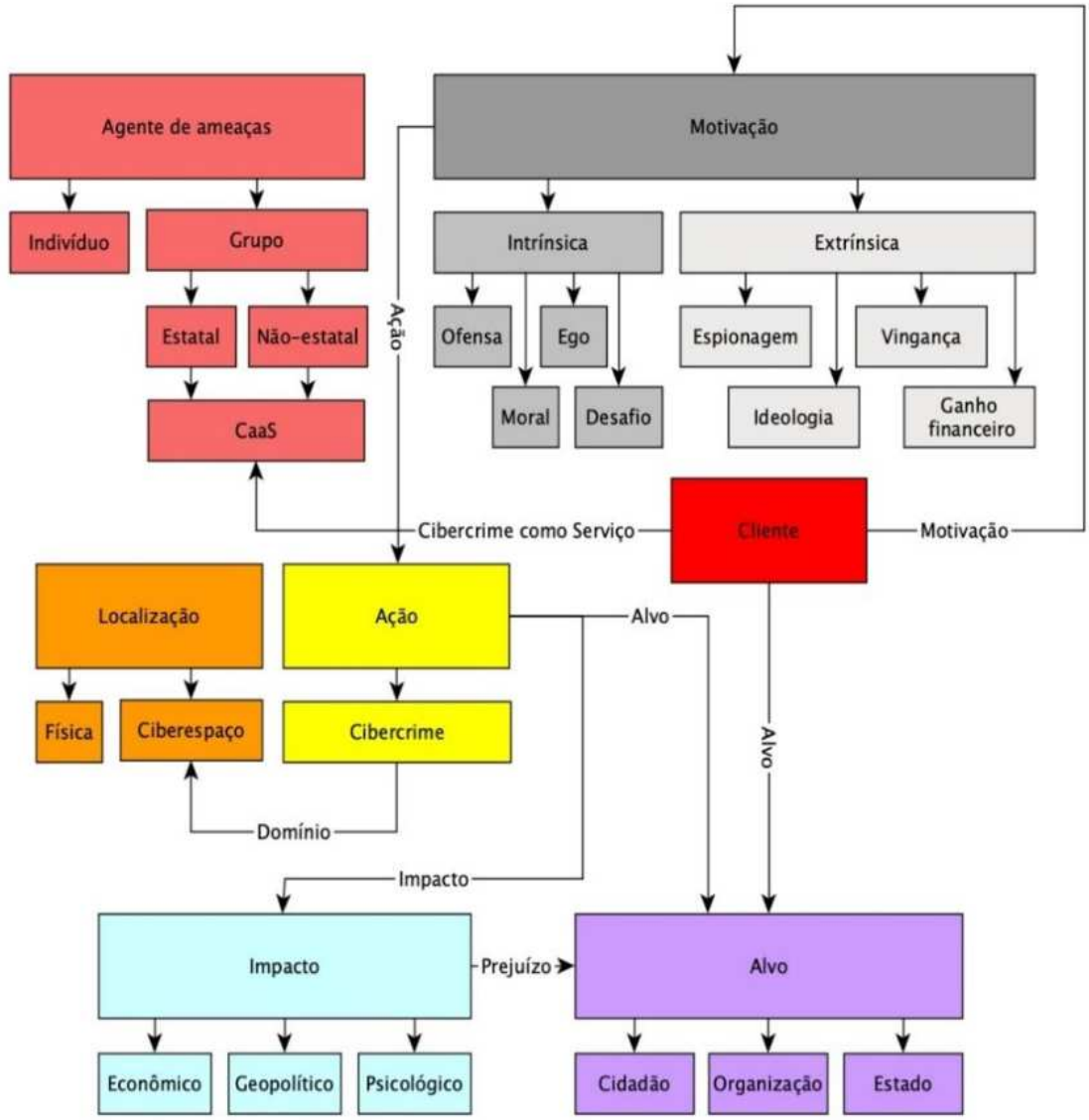
Fonte: SOCRadar, 2023.

Para assimilar ainda mais a evolução do CaaS é crucial compreender o seu impacto no cenário cibernético global. A ascensão do CaaS reduziu significativamente a barreira de entrada do cibercrime, permitindo que indivíduos sem competências técnicas avançadas lançassem ataques sofisticados, democratizando as capacidades cibernéticas ofensivas e acarretando aumento no volume e na variedade de ataques cibernéticos, juntamente com a integração de táticas patrocinadas por agentes de ameaças estatais

nas atividades criminosas, que confundem os limites entre a segurança nacional e o cibercrime tradicional, dificultando as estratégias de resposta dos governos e das agências de Inteligência.

Na tentativa de contribuir para entender a relação entre o cliente e um grupo de ciberciminosos vinculados a uma estrutura de CaaS, definiu-se o diagrama relacional (BARN, 2016) ilustrado pela Figura 2.

FIGURA 2 – DIAGRAMA RELACIONAL



Fonte: adaptado de Barn, 2016.

3 O MODELO DE NEGÓCIO DO CAAS E A SUA CADEIA DE VALOR

À medida que o CaaS vem se tornando um negócio lucrativo para cibercriminosos, faz-se necessário o reconhecimento das atividades que agregam valor às operações de ataque cibernético do ponto de vista de uma cadeia de valor (PORTER, 1985) considerando o CaaS como um sistema composto por subsistemas, cada um com entradas, processos de transformação e saídas, além de atividades de apoio.

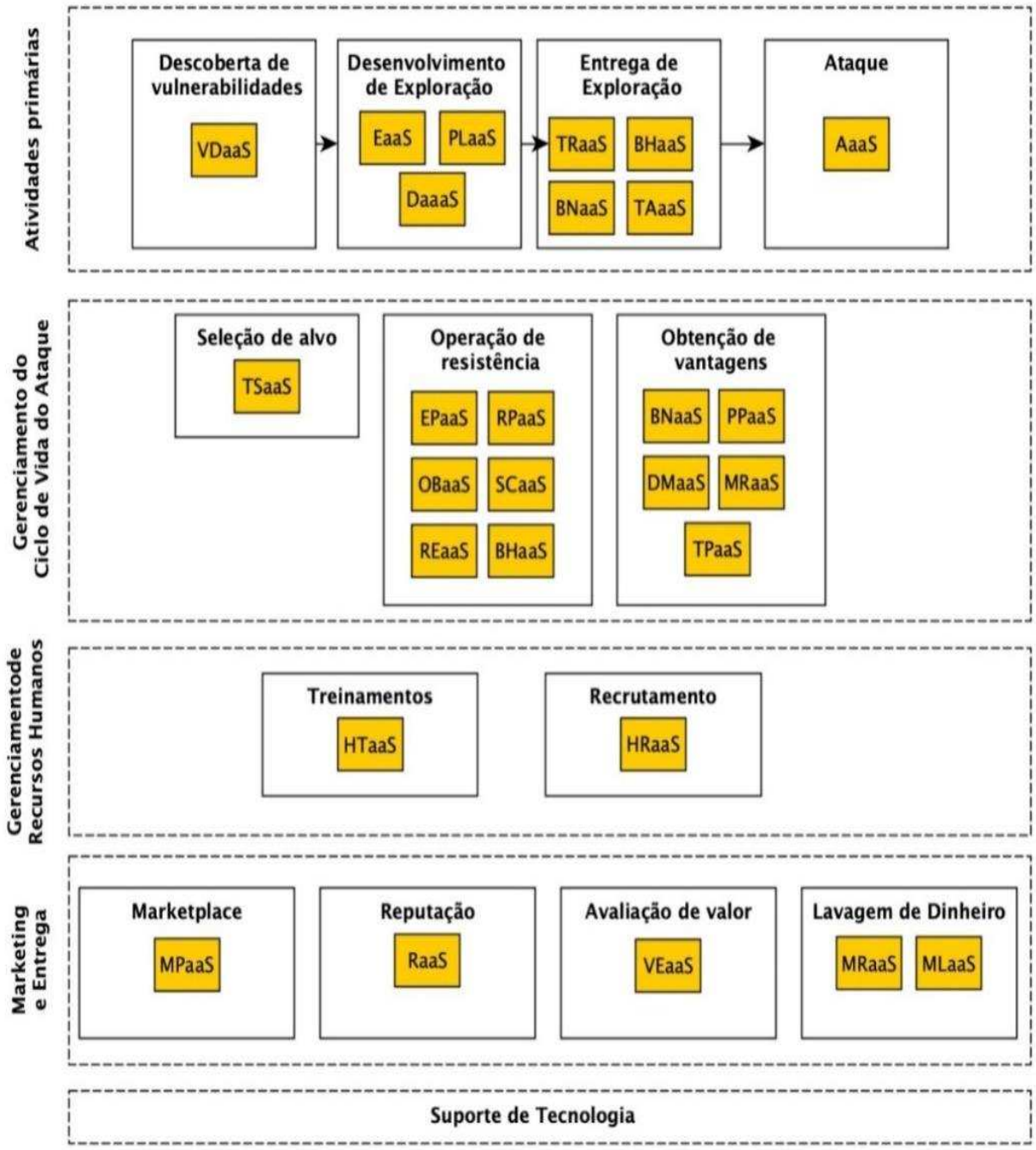
Este processo de identificação de valor agregado inclui qualquer atividade no ecossistema do CaaS que permita ao cibercriminoso minimizar o custo dos ataques cibernéticos e maximizar seus benefícios. Além das atividades primárias, as atividades de apoio também são importantes para promover o funcionamento do cibercrime, pois podem permitir ao atacante realizar um ataque a um custo reduzido e com maior lucro.

Para perceber estes processos, utilizou-se o modelo da cadeia de valor cibercriminosa (HUANG et al. 2017) consistindo nas atividades primárias de descoberta de vulnerabilidades, desenvolvimento de exploração, entrega de exploração e ataque, bem como as funções de apoio das operações do ciclo de vida do ataque cibernético, recursos humanos, propaganda e entrega e suporte técnico, ilustrada pela Figura 3.

São considerados como serviços de atividades primárias ofensivas (HUANG et al. 2017): (a) Descoberta de vulnerabilidades: *Vulnerability Discovery as a Service* (VDaaS); (b) Desenvolvimento de código malicioso para exploração de vulnerabilidades: *Exploit as a Service* (EaaS), *Payload as a Service* (PaaS) e *Deception as a Service* (DaaS); (c) Entrega de exploração de vulnerabilidades: *Traffic Redirection as a Service* (TRaaS), *Bulletproof Hosting as a Service* (BHaaS) e *Botnet as a Service* (BaaS), *Traffic (including* DDoS) *as a Service* (TAaaS); e (d) Ataque: *Attack as a Service* (AaaS).

São considerados como serviços de gerenciamento do ciclo de vida do Ataque (HUANG et al. 2017): (a) Seleção do alvo: *Target Selection as a Service* (TSaaS); (b) Operação de resistência: *Exploit Package as a Service* (EPaaS), *RDP/Proxy/Seedbox as a Servic*e (RPaaS), *Obfuscation as a Service* (OaaS), *Security Checker as a Service* (SCaaS), *Reputation Escalation as a Service* (REaaS) e *Bulletproof Hosting as a Service* (BHaaS); e (c) Obtenção de vantagens: *Botnet as a Service* (BNaaS), *Personal Profile as a Service* (PPaaS), *Domain Knowledge as a Service* (DMaaS), *Money Mule Recruiting as a Service* (MRaaS) e *Tool Pool as a Service* (TPaaS).

FIGURA 3 – CADEIA DE VALOR DO CAAS



Fonte: adaptado de HUANG, 2017.

São considerados como serviços de gerenciamento de recursos humanos (HUANG et al. 2017): (a) Treinamentos: *Hacker Training as a Service* (HTaaS) e (b) Recrutamento: *Hacker Recruiting as a Service* (HRaaS).

São considerados como serviços de propaganda e entrega (HUANG et al. 2017): (a) *Marketplace*: *Marketplace as a Service* (MPaaS); (b) Reputação: *Reputation as a Service* (RaaS); (c) Avaliação de valor: *Value Evaluation as a Service* (VEaaS) e (d)

Lavagem de dinheiro: *Money Mule Recruiting as a Service* (MRaaS) e *Money Laundering as a Service* (MLaaS).

4 COMPETÊNCIAS FUNCIONAIS PARA ANALISTAS DE INTELIGÊNCIA DE CIBERCRIME

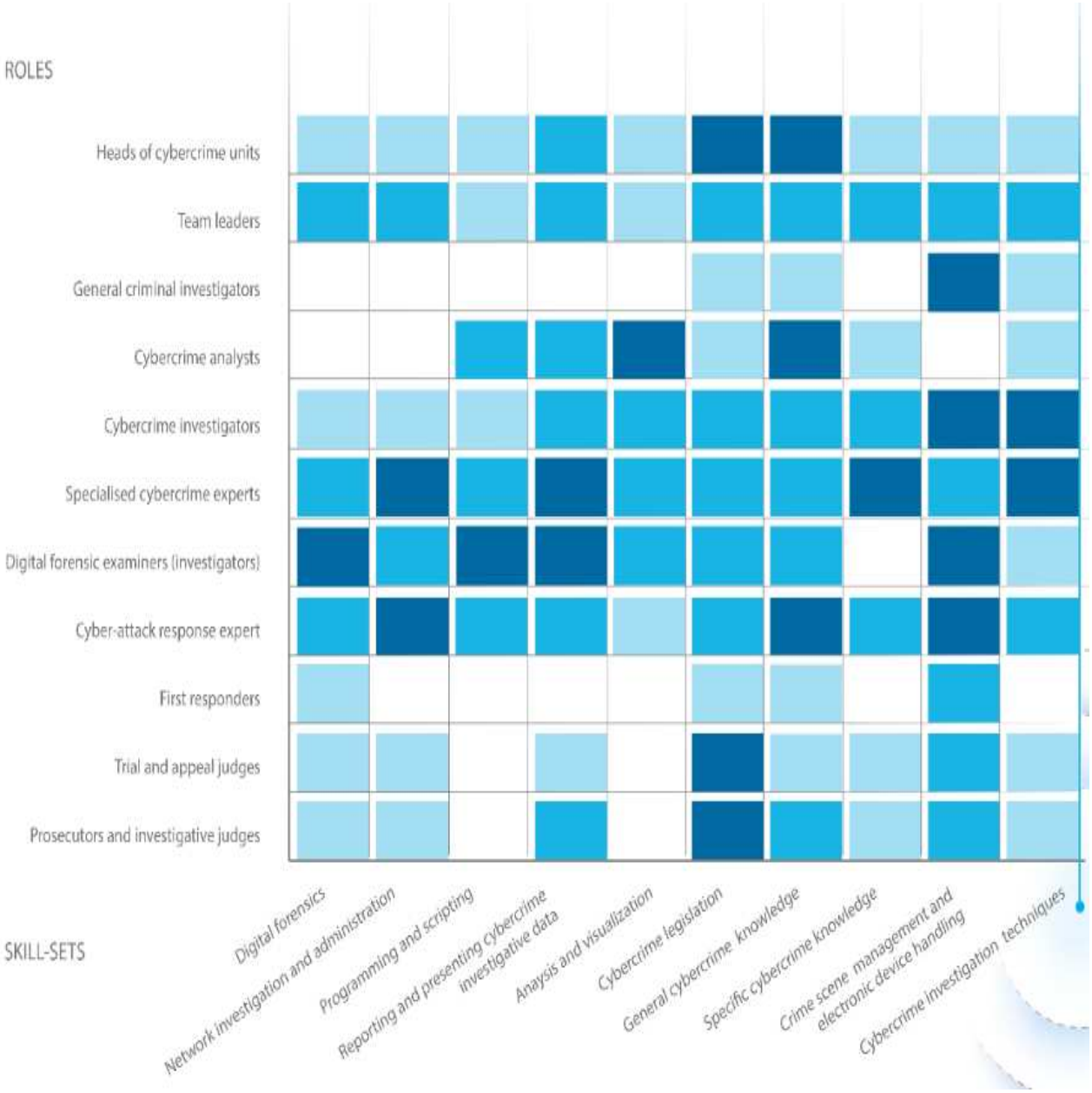
Com o objetivo de identificar os conjuntos de competências necessárias para os principais agentes envolvidos no processo investigatório de cibercrime a Europol publicou, em 2024, o *Cybercrime Training Competency Framework* (EUROPOL, 2024) como uma referência de estrutura de competências e capacidades para as organizações de aplicação da lei, instituições judiciárias e acadêmicas, a partir de um Quadro de Competências de Formação em Crime Cibernético, criado após consultas a múltiplas organizações para identificar as principais funções e os conjuntos de competências necessárias para profissionais da área de crime cibernético.

As funções e os conjuntos de competências destacados no quadro (Figura 4) refletem as competências funcionais exigidas, não sendo uma lista exaustiva de competências específicas, sendo limitado aos profissionais policiais e do poder judiciário envolvidos no domínio do crime cibernético e de investigações digitais. Os conjuntos de competências descritos não refletem todas as competências necessárias para cumprir a função descrita, mas referem-se a competências exclusivas das investigações de crimes cibernéticos e do tratamento de provas digitais.

Os profissionais analistas de crimes cibernéticos atuam em áreas como coleta de informações, análise e produção de conhecimentos acionáveis de Inteligência, análise estratégica, pesquisa, além de apresentarem as ameaças mais recentes e fornecerem dados situacionais por visões gerais.

Os analistas precisam ser capazes de processar grandes quantidades de dados de diferentes fontes e traduzi-los em relatórios concisos que descrevam claramente as questões oferecendo uma assessoria a um público vasto, por exemplo, em relatórios nacionais ou internacionais de interesse geral.

FIGURA 4 – QUADRO DE COMPETÊNCIAS EM CRIME CIBERNÉTICO



Fonte: EUROPOL, 2024.

5 TENDÊNCIAS E DESAFIOS FUTUROS

Espera-se que o futuro da cibersegurança seja moldado por diversas tendências e desafios emergentes. De acordo com a mídia especializada, existe um aumento previsto no custo global do cibercrime, estimado em US$23,84 trilhões até 2027, acima dos US$8,44 trilhões, em 2022 (*WORLD ECONOMIC FORUM*, 2024), realçando a crescente sofisticação e frequência dos ataques cibernéticos.

Uma das principais tendências que moldam o futuro da cibersegurança é o

progresso nas tecnologias de segurança, impulsionado por investimentos públicos e privados. À medida que avançamos em direção a 2030, prevê-se que estes avanços produzam benefícios significativos no combate ao crime cibernético, na defesa de infraestruturas críticas e no aumento da sensibilização do público sobre a segurança cibernética. O foco provavelmente será menos nas medidas defensivas tradicionais e mais na adaptação às novas tecnologias e ameaças.

Outra tendência é a natureza evolutiva das ameaças cibernéticas, que estão a tornar-se mais diversas e complexas. Os cibercriminosos utilizam cada vez mais tecnologias avançadas, como a Inteligência Artificial e aprendizagem automática, para executar ataques sofisticados. Essa tendência representa um desafio significativo para os profissionais de segurança cibernética e requer uma abordagem dinâmica e proativa à defesa cibernética.

6 MEDIDAS PREVENTIVAS

Para as agências de aplicação da lei, a análise de Inteligência desempenha um papel crucial na prevenção do crime cibernético, sendo sugerido manter: (a) a capacidade de Inteligência Cibernética, aprimorando as unidades especializadas focadas na coleta e análise de Inteligência de ameaças cibernéticas para monitoramento de fóruns da *Dark Web* e outras plataformas onde os cibercriminosos operam; (b) a colaboração Internacional, uma vez que o cibercrime muitas vezes transcende fronteiras, sendo essencial colaborar internacionalmente para o compartilhamento de informações, melhores práticas e operações conjuntas; (c) treinamento e conscientização sobre as últimas tendências do crime cibernético e técnicas forenses digitais é fundamental; (d) parcerias público-privadas pela colaboração com especialistas em segurança cibernética do setor privado para obter acesso a tecnologias e insights atuais e (e) o uso de ferramentas avançadas para análise preditiva e processamento mais rápido de dados relacionados ao crime cibernético.

CONCLUSÃO

Ao concluirmos, fica claro que o CaaS representa uma ameaça significativa, uma vez que a junção entre a tecnologia avançada e a intenção criminosa deu origem a uma nova era de crime digital que é sofisticada, generalizada e difícil de se combater. No entanto, com os esforços de Inteligência concentrados em análise de informações, colaboração global e estratégias adaptativas de aplicação da lei, aumentam-se as chances de mitigar estas ameaças. A integração da tecnologia com a visão humana da Inteligência é a potencialização de uma defesa cibernética mais forte. À medida que o

crime cibernético continua a evoluir, também devem evoluir as nossas abordagens para compreendê-lo, preveni-lo e combatê-lo. Esta batalha contínua contra o crime digital reforça a necessidade de se manter vigilância, inovação e colaboração contínuas entre as organizações.

REFERÊNCIAS

*What Is Cybercrime-as-a-Service (CaaS)?*Heimdal Security, Disponível em: https://heimdalsecurity.com/blog/what-is-cybercrime-as-a-service-caas. Acesso em: 20 de mar. de 2024.

SHARMA, Amit et al. *Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures.Journal of Ambient Intelligence and Humanized Computing,* v. 14, n. 7, p. 9355-9381, 2023.

*A for APT: Criteria for Classifying Cyber Threats.*SOCRadar, Disponível em: https://socradar.io/a-for-apt-criteria-for-classifying-cyber-threats. Acesso em: 20 de mar. de 2024.

BARN, Ravinder; BARN, Balbir. *An ontological representation of a taxonomy for cybercrime. In*: *24th European Conference on Information Systems (ECIS 2016)*. 2016.

PORTER MICHAEL, E. *Competitive Advantage: Creating and Sustaining Superior Performance.* New York, 1985.

HUANG, Kemanet al. *Cybercrime-as-a-service: identifying control points to disrupt.Massachusetts Institute of Technology* (MIT), Tech. Rep, 2017.

Cybercrime Training Competency Framework. EUROPOL. Disponível em: https://www.europol.europa.eu/publications-events/publications/cybercrime-training-competency-framework. Acesso em: 20 de mar. de 2024.

2023 was a big year for cybercrime – here's how we can make our systems safer. World EconomicForum. Disponível em:https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety. Acesso em: 20 de mar. de 2024.

A RISP

A Revista de Inteligência de Segurança Pública - RISP (*ISSN 2675-7168; 2699*) é uma publicação continuada, da Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro - ESISPERJ, idealizada como um ambiente de acesso ao conhecimento de forma oficial, objetiva e transparente e que visa divulgar manuais e estudos científicos, pesquisas atuais, além das melhores e mais apuradas práticas, contribuindo assim para a desmistificação do tema. A RISP é, portanto, voltada para a comunidade acadêmico-científica, profissionais do setor e mesmo a qualquer pessoa que tenha interesse em aprofundar seus conhecimentos na área de Inteligência, notadamente vinculados às questões da Segurança Pública.

A ESISPERJ

Criada oficialmente pelo Decreto Estadual nº 40.254/2006, renomeada pelo Decreto Estadual nº 44.528/2013, posteriormente reorganizada e vinculada à Subsecretaria de Inteligência através da Resolução SESEG nº 737/2013 (DOERJ nº 002/2013), a Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ) busca, através de seus cursos, seminários, ações, workshops etc. a uniformização da atuação das Agências de Inteligência de Segurança Pública (AISP) formando, especializando e treinando os servidores nelas lotados, com ênfase nos seguintes pilares:

MISSÃO

Qualificar os profissionais da Comunidade de Inteligência e manter atualizada a Doutrina de ISP, por meio da pesquisa e produção de conhecimento, visando potencializar a capacidade de atuação estatal na área finalística da Segurança Pública.

VISÃO

Ser referência em ensino, doutrina, pesquisa e extensão em Inteligência de Segurança Pública (ISP) para a comunidade de inteligência.

VALORES

Produção de conhecimento em ISP; Valorização do ambiente democrático; Fortalecimento de rede; Integração; Profissionalização técnica; Respeito à diversidade; Interoperabilidade; e Excelência científica e tecnológica.

DIRETRIZES PARA AUTORES

Os textos enviados devem ser produções intelectuais inéditas dos respectivos autores, devendo cuidar para que não haja inserção de conteúdo publicado sem menção da fonte, de modo a não ferir a política editorial adotada pela ESISPERJ e a ética científica.

Os textos devem ter como escopo a atividade de inteligência, com foco na atividade de Inteligência de Segurança Pública, podendo tomar como objeto todas as dimensões e aspectos inerentes à ISP.

O envio dos textos, em recebimento de fluxo contínuo, deve ser realizado para o e-mail: risp.esisperj@pcivil.rj.gov.br, em formato **.doc/.docx** (*Microsoft Office Word*). No mesmo e-mail, deve ser encaminhado o Termo de Cessão de Direitos Autorais, assinado e salvo em formato <.pdf>, além do arquivo contendo elementos pré-textuais. Visando facilitar esse processo, todos os modelos destes e outros documentos podem ser obtidos na página da ESISPERJ.

CONDIÇÕES GERAIS PARA SUBMISSÃO DE TEXTOS

- A contribuição deve ser original e inédita, e não estar sendo avaliada para publicação por outra revista.
- As URLs para as referências devem ser informadas sempre que possível.
- O texto deve ser formatado de acordo com o modelo disponibilizado na página da ESISPERJ.
- O texto deve seguir os padrões de estilo e requisitos bibliográficos descritos e adotados pelo padrão vigente da ABNT.

Resenhas de livros também serão aceitas para publicação, observando-se as diretrizes previstas no tópico seguinte.

DIRETRIZES PARA RESENHA

A resenha deve ser escrita para livros com até dois (2) anos de lançamento e que tenham como foco a atividade de inteligência, em especial, a Inteligência de Segurança Pública, podendo ser escrita para livros em outros idiomas, resguardando-se a devida tradução para o português (BR).

Os autores que tiverem sua proposição aprovada devem declarar que cedem os direitos autorais à RISP, podendo esta incluir o trabalho publicado em bases de dados públicas e privadas, no Brasil e no exterior. Devem ainda declarar que são os únicos responsáveis pelo conteúdo do texto e que o mesmo não contém nada que possa ser considerado ilegal ou difamatório a terceiros.

As submissões em desacordo com as Diretrizes para Autores não serão admitidas para avaliação e seus propositores serão devidamente comunicados.

CONDIÇÕES PARA SUBMISSÃO

Como parte do processo de submissão, os autores são obrigados a verificar a conformidade da submissão em relação a todos os itens listados às diretrizes previstas no AVA ESISPERJ: https://esisperj-ead.pcivil.rj.gov.br/login/index.php. As submissões que não estiverem de acordo com as normas serão recusadas e/ou devolvidas aos autores para adequação.

DECLARAÇÃO DE DIREITO AUTORAL

Autores que publicam nesta revista concordam com os seguintes termos:

1) Autores mantêm os direitos autorais e concedem à revista o direito de primeira publicação, com o trabalho simultaneamente licenciado sob a Licença *Creative Commons Attribution,* que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista.

2) Autores têm autorização para assumir contratos adicionais separadamente, para distribuição não-exclusiva da versão do trabalho publicada nesta revista (ex.: publicar em repositório institucional ou como capítulo de livro), com reconhecimento de autoria e publicação inicial nesta revista.

3) Autores têm permissão e são estimulados a publicar e distribuir seu trabalho *online* (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado.

Juntem-se a nós!