INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

As Informações Policiais no Planeamento de Grandes Eventos: Uma Abordagem ao Processo de Gestão do Risco

Auditor

Bruno Filipe Salvador da Silva Branco

Lisboa, 03 de outubro de 2025

RESUMO

O presente trabalho de investigação abordou a otimização da Inteligência Policial Operacional no planeamento de segurança a grandes eventos. Partindo da premissa de que os modelos de policiamento reativos eram insuficientes para os desafios atuais, defendemos a implementação de uma abordagem proactiva e estratégica, baseada no Policiamento Orientado pelas Informações. A pesquisa focou-se em otimizar a metodologia dos Núcleos de Informações Policiais, com base no desenvolvimento dum processo estruturado na gestão do risco e consequente geração de cenários, por forma a garantir fiabilidade e reforçando o seu contributo para a tomada de decisão dos Comandantes. O processo defendido envolveu a avaliação rigorosa das ameaças, vulnerabilidades e consequências, por forma a aplicar aos grandes eventos uma matriz de avaliação do risco quantitativa. A projeção de cenários plausíveis surgiu como a aplicação prática dessa análise, permitindo preparar respostas adequadas e flexíveis por parte dos Comandantes. O estudo concluiu que a eficácia da segurança em grandes eventos dependia da implementação duma cultura de Inteligência, que exigia investimento em formação especializada e em recursos tecnológicos adequados, transformando a incerteza em risco calculado.

Palavras-chave: inteligência policial; policiamento orientado pelas informações; segurança de grandes eventos

ABSTRACT

This investigation addresses the optimization of Operational Intelligence in security planning for major events. Based on the premises that reactive policing models are insufficient for current challenges, we advocate the implementation of a proactive and strategic approach based on intelligence-led policing. The research focuses on optimizing the methodology of the Intelligence units, based on the development of a structured process for risk management and the consequent generation of scenarios, in order to ensure reliability and reinforce their contribution to the decision-making process of Commanders. The process proposed involves a rigorous assessment of threats, vulnerabilities, and consequences in order to apply a quantitative risk assessment matrix to major events. The projection of plausible scenarios emerges as the practical application of this analysis, allowing commanders to prepare appropriate and flexible responses. The study concludes that the efficiency of security at major events depends on implementing a culture of intelligence, which requires investment in specialized training and adequate technological resources, turning the uncertainty into a calculated risk.

Keywords: intelligence-led policing; police intelligence; security for major events

ÍNDICE

INTRODUÇÃO

Temática e contexto

No contexto geopolítico subsequente aos atentados de 11 de setembro de 2001, e face a um processo de globalização que intensifica as "relações sociais de escala mundial" (Giddens, 2005, citado por Elias, 2011, p. 92), emerge uma necessidade premente de reconfiguração dos modelos de segurança interna dos diferentes Estados (Acosta, Merino & Zometa, 2015; Elias, 2011).

Em resposta a estes desafios, as forças de segurança têm vindo a adotar um conjunto de novos paradigmas e modelos de ação, que passam por estratégias como o policiamento de proximidade, o policiamento orientado para os problemas ou o policiamento orientado pelas informações (POI). Estas mesmas estratégias representam respostas adaptativas que visam aumentar a eficácia operacional e reforçar a legitimidade da função policial perante a sociedade (Acosta, Merino, & Zometa, 2015; Elias, 2011; Fernandes, 2014; Torres, 2015a , 2024).

Esta perspetiva é claramente articulada por Elias (2011, p. 92), que afirma que “um dos principais vectores da nova governação da segurança parece efectivar-se através da implementação de modelos dinâmicos e multidimensionais de policiamento de proximidade, articulados com estratégias orientadas pelas informações”.

Para Fernandes (2014, p. 17), a Inteligência Policial (INTELPOL) constitui um fator *sine qua non* para a eficácia da segurança, uma vez que suporta o processo de tomada de decisão na formulação das estratégias mais adequadas à concretização dos objetivos institucionais, tendo por missão “identificar ameaças emergentes e prospectivar a materialização de futuros riscos, evitando surpresas”.

No contexto de policiamentos a grandes eventos, pela sua elevada complexidade, volatilidade e incerteza, o valor do POI torna-se ainda mais evidente e indispensável, exigindo uma capacidade de antecipação e de planeamento que vai muito além da simples gestão de multidões (Fernandes, 2014). É então que a *intelligence* policial se assume como uma ferramenta estratégica crucial, pela sua capacidade em transformar a informação num ativo estratégico que capacita os Comandantes na tomada de decisões de forma mais preditiva, inteligente e preventiva (Elias, 2011; Fernandes, 2014; Ratcliffe, 2016; Rodrigues, 2024).

É precisamente na fase do planeamento operacional que a INTELPOL adquire nuclear importância, "pois é a inteligência policial que melhor suporta o processo de decisão dos

decisores policiais ao nível estratégico, bem como dos operacionais a atuar no terreno" (Fernandes, 2014, p. 159).

Objetivos e metodologia adotada

O presente trabalho de investigação debruça-se sobre a otimização da Inteligência Policial Operacional no contexto do planeamento de segurança a grandes eventos, visando o reforço da sua contribuição para a tomada de decisão dos Comandantes. Nesse âmbito, a investigação tem como finalidade contribuir para uma otimização da metodologia conduzida pelos Núcleos de Informações Policiais (NIP), especificamente no que se refere ao processo exaustivo de gestão do risco e subsequente geração de cenários.

Assim, o objetivo principal da investigação centra-se em propor um aperfeiçoamento metodológico do trabalho desenvolvido pelos NIP, de forma a que a avaliação e tratamento do risco se constituam como uma ferramenta de inteligência mais robusta e preditiva. Para atingir esta desiderato, apontamos como objetivos secundários: a análise do papel da INTELPOL, em particular da INTELPOL operacional, na definição de policiamentos proativos; a demonstração de como metodologias estruturadas permitem análises rigorosas e de fácil interpretação, servindo de referência na tomada de decisão; e, finalmente, a exploração da forma como a gestão do risco e a projeção de cenários capacitam o planeamento a lidar com a incerteza dos grandes eventos.

Estes propósitos encontram-se espelhados nas questões de investigação que orientam o estudo, culminando na seguinte pergunta de partida: “Que processos metodológicos devem ser adotados pelos NIP para transformar a gestão do risco e a geração de cenários numa ferramenta eficaz de apoio ao planeamento operacional de grandes eventos?”

Da questão de partida derivam as seguintes questões de investigação:

- Qual o papel da Inteligência Policial na transição de um modelo de policiamento reativo, para um modelo proativo e estratégico, essencial na segurança de grandes eventos?
- Como pode a adoção de metodologias estruturadas nos NIP garantir que a inteligência produzida possa influenciar eficazmente a tomada de decisão dos Comandantes?
- Em que medida a avaliação do risco e a projeção de cenários permitem que o planeamento operacional esteja mais adaptado à incerteza dos grandes eventos?

Considerando o objeto de estudo, pretende-se uma investigação de natureza teórico-reflexiva, com recurso a uma abordagem qualitativa, que, partindo de uma base conceptual

consolidada, desenvolve uma reflexão crítica sobre o alcance da INTELPOL operacional, com o propósito de formular recomendações que contribuam para o avanço do conhecimento teórico na área das Informações Policiais.

Síntese dos capítulos

O presente trabalho encontra-se estruturado em dois capítulos fundamentais, sendo o primeiro capítulo dedicado à contextualização teórica (Estado da Arte), no qual se analisam os conceitos de inteligência policial, policiamento orientado pelas informações e a definição de grandes eventos. O segundo capítulo (Perspetivas), explora a importância da inteligência operacional e do POI no planeamento da segurança de grandes eventos, culminando com uma proposta para a otimização do trabalho dos núcleos de informações policiais (NIP) no âmbito da gestão do risco e da geração de cenários.

ESTADO DE ARTE

1. A Inteligência policial

Previamente à análise do conceito, importa clarificar a designação a utilizar, considerando que em Portugal, vários autores diferem na terminologia, referindo-se por vezes ao conceito como Informações (Araújo, 2019; Carvalho, 2016; Clemente, 2009; Elias, 2011), outras como Inteligência (Carvalho, 2015; Fernandes, 2014). Por concordarmos que a designação Inteligência confere uma expressão mais completa e abrangente, utilizaremos essa expressão, referindo-nos a Informações apenas quando mencionarmos os serviços internos ligados ao sistema de informações da Polícia de Segurança Pública (PSP).

A INTELPOL, comummente designada por *intelligence* na literatura especializada, assume-se com uma função fulcral para as organizações policiais contemporâneas, dada a sua relevância, decisiva, para o processo de tomada de decisão e para a eficácia operacional. Surge assim como uma resposta proactiva, permitindo que as forças de segurança se antecipem às ações criminosas, identificando vulnerabilidades e neutralizando, ou minimizando, as ameaças (Acosta, Merino & Zometa, 2015; Bravo, 2011; Fernandes, 2014; Gill & Phythian, 2016; Warner, 2002).

A conceptualização é variada, podendo a sua utilização assumir vários sentidos e ser definida como "uma forma especializada de conhecimento, uma atividade e uma organização" (Moore, 200 citado por Fernandes, 2014, p. 82). Na breve análise que efetuaremos, deixaremos de lado a inteligência enquanto organização, focando-nos, no âmbito da

segurança interna, na inteligência enquanto "atividade destinada à produção de informações de segurança" (Fernandes, 2005, citado por Elias, 2011, p. 201).

Segundo Clemente (2015, p. 75), "as informações exprimem o sistema de recolha, de análise e de processamento de informação, para obter um conhecimento acrescido sobre certa situação específica – a inteligência é a informação relacionada, sistematizada e contextualizada". Nesse sentido, a INTELPOL destina-se à "prossecução directa das missões legalmente atribuídas a serviços de natureza policial, sejam elas de nível estratégico ou operativa" (Clemente, 2015, p. 75), resultando, portanto, "do conjunto de notícias, dados e factos recolhidos, que através de um processo metódico e sistematizado são 'transformados' em informação útil, pertinente e com valor acrescentado para a actividade da Polícia" (Elias, 2011, p.202).

1.1 Níveis de inteligência policial

A INTELPOL pode assumir uma vertente estratégica, uma vertente operacional e uma vertente tática (Acosta, Merino, & Zometa, 2015; Elias, 2011). Já no entendimento da *United Nations Office on Drugs and Crime (UNODC*), citado por Fernandes (2014, p. 101), a INTELPOL poderá expressar-se como "inteligência estratégica e operacional…notando que as duas categorias de inteligência são interdependentes".

Caracterizando o conceito de inteligência estratégica, Mangio & Wilkinson (2008), citado por Fernandes (2014, p. 102) realçam o seu matiz prospetivo, de médio e longo prazo, abordando "os fenómenos criminais e a prossecução dos objetivos da organização policial, identificando possibilidades e tendências emergentes de modo a estimar alterações no ambiente externo e identificar as consequências", podendo consubstanciar-se em "relatórios sobre a evolução e tendências criminais, análise de perfis e análise de métodos" (Elias, 2011, p. 203).

Relativamente à inteligência operacional, a mesma pode ser caracterizada de curto-prazo, "necessária ao planeamento e execução das várias operações de segurança" (Fernandes, 2014, p. 103), sendo os seus destinatários os Comandantes operacionais responsáveis por conduzir, no terreno, a atividade diária dos polícias (Camacho, 2015; Fernandes, 2014). Para Elias (2011, p. 204), a inteligência operacional "tem por objectivo apoiar as unidades operacionais nas suas missões de investigação criminal, ordem pública e prevenção. Visa ações concretas, fundamenta-se em dados específicos e tem objectivos de curto prazo". Nas palavras de Ratcliffe (2016, p. 75), "sandwiched between the offender focus of the tactical

arena, and the strategic nature of intelligence to form strategy, policy and long-term plans, the operational imperative that can drive crime reduction activity and resource planning".

Por último, a inteligência tática, que pode ser definida como aquela que está em curso, num "processo hábil de adquirir conhecimento e informação, com o objetivo de manipular o ambiente e conseguir os objetivos de forma intencional, proporcionando vantagens ao envolver os operadores de inteligência no terreno, prevendo a necessidade de utilização de recursos, dando a perspetiva de iniciativa ao Comandante" (Goldman, 2006, citado por Toscano, 2022, p. 7).

2. Policiamento orientado pelas informações

O POI, conhecido internacionalmente pela sua designação anglo-saxónica *Intelligence-Led Policing* (ILP), emergiu no início dos anos 90, no Reino Unido[1] (Ratcliffe, 2016), e representa uma das mais significativas transformações no paradigma da filosofia securitária contemporânea, passando dum modelo mais reativo, e focado na resposta a incidentes, para um modelo proactivo, estratégico e assente na tomada de decisão célere e assertiva com base na informação recolhida e analisada - *intelligence* (Elias, 2022; Fernandes, 2014; James, 2013; Ratcliffe, 2016; Spiller, 2006).

Destarte, existem diferentes pontos de vista atinente ao conceito de POI e a forma como o modelo é aplicado nas diversas organizações policiais (Carter & Carter, 2009). Para Clemente (2015, p. 76) o "produto informacional dirige o esforço de patrulhamento", dado que, partindo duma análise criminal estratégica baseada em indicadores da criminalidade denunciada, é possível formular programas preventivos, cabendo à polícia a tarefa de "previsão, ou seja, antecipar a prevenção, através da produção de informações".

A concetualização de Ratcliffe (2016, p. 64) descreve o POI como um modelo de gestão dos recursos baseado em evidências e recolha de informação junto dos delinquentes, grupos organizados e locais de maior afluência criminal ("hot people", "hot groups" and "hot places").

Na doutrina de Carter e Carter (2009), o principal desafio para as organizações policiais centra-se na capacidade de se concentrarem nas ameaças que têm implicações direta ou indiretamente na segurança pública, além das iminentemente criminais. Nesse sentido,

[1] A base de partida para o desenvolvimento deste modelo de policiamento teve origem no relatório da *Audit Comission*, de 1993, intitulado *Helping with enquiries: tackling crime effectively*, sugerindo uma abordagem proactiva aos problemas criminais. A mudança do paradigma arrojado pelo relatório é posteriormente reforçada em 1997 com o relatório *Policing with intelligence*, que sugere o recurso a informações policiais por forma a orientar dos escassos recursos, tornando a gestão mais eficiente.

introduzem na equação o conceito de "homeland security intelligence", definindo-o como: "…the collection and analysis of information concerned with non-criminal domestic threats to critical infrastructure, community health and public safety for the purpose of preventing the threat or mitigating the effects of the threat" (Carter & Carter, 2009, p. 8). Seguindo a lógica dos autores, e partindo duma abordagem holística, perspetivam o POI como um modelo capaz de conciliar as experiências adquiridas pelos polícias do policiamento comunitário e orientado para os problemas, repositórios essenciais do conhecimento das comunidades, e, dessa forma, potenciais coletores de informação para o ciclo da inteligência, permitindo definir os parâmetros dos problemas da comunidade.

A aplicação de modelos híbridos é, de igual forma, defendida por Elias (2011, p. 92) sustentando que "um dos principais vectores da nova governação da segurança parece efetivar-se através da implementação de modelos dinâmicos e multidimensionais de policiamento de proximidade". Essa mesma linha de pensamento é corroborada por Fernandes (2014, p. 194) ao defender que a multidisciplinariedade "é aquela que apresenta melhores resultados na redução da criminalidade e do sentimento de insegurança".

Com base nesta perspetiva integral e sistémica, Carter e Carter (2009, p. 11) propõem uma definição operacional para caracterizar o POI:

> The collection and analysis of information related to crime and conditions that contribute to crime, resulting in an actionable intelligence product intended to aid law enforcement in developing tactical responses to threats and/or strategic planning related to emerging or changing threats.

Embora divergentes na abordagem ao conceito, parece-nos pacífico afirmar que na lógica deste modelo de policiamento, a inteligência resultante do processo de análise de informação fundamentará as decisões dos Comandantes a compreender o ambiente criminal, identificar padrões, prever tendências e, consequentemente, tomar decisões mais céleres, assertivas e informadas, quer na gestão dos recursos disponíveis, quer na definição das estratégias. Assume-se assim "como uma modelo de gestão da segurança e ordem públicas que tem o seu centro de gravidade na inteligência, a qual orienta a estratégia da organização aos vários níveis hierárquicos e, sobretudo, a continuidade das operações" (Fernandes, 2014, p. 191).

3. Definição de grande evento

No cenário contemporâneo de crescente globalização "as Organizações Internacionais, os Estados e os setores público e privado procuram captar a realização de grandes eventos, como forma de afirmação nacional, regional ou local" (Elias, 2022, p. 407) visando, por um lado, a atração de investimento económico e, por outro, a obtenção de visibilidade e reconhecimento para as temáticas que procuram promover[2].

Não sendo um conceito que reúna consenso, a tentativa de definição de Grande Evento (GE) gera algumas inconformidades. De acordo com Allen, O'Toole, McDonnell e Harris (2002), citada por Oliveira (2019, p. 16), GE são "aqueles que, pela sua escala e interesse mediático, são capazes de atrair um número significativo de visitantes, cobertura mediática e benefícios económicos".

Com base na doutrina desenvolvida pelo projeto EU-SEC II (*Coordinating National Research Programmes on Security during Major Events in Europe*) no âmbito do *International Permanent Observatory* (IPO) da *United Nations Interregional Crime and Justice Research* (UNICRI) foi estabelecido um modelo de planeamento de segurança direcionado para GE. No âmbito desse projeto, e na ausência duma definição operacional concetual, considerámos o conceito apontado pela UNICRI, definindo como GE um acontecimento previsível que exige, para a elaboração do seu modelo de planeamento, a ativação de mecanismos de cooperação internacional (UNICRI, 2011), devendo observar uma das seguintes características:

1. Grande presença de VIP e ou altas entidades (políticos, atletas, artistas);
2. Grande cobertura mediática;
3. Grande número de pessoas;
4. Dispersão / concentração ou outros eventos durante o grande evento;
5. Risco de alterações de ordem pública (adeptos / manifestantes);
6. Significado histórico ou político e popularidade;
7. Grande número de profissionais da segurança empenhados (polícias, proteção civil, seguranças privados);

[2] Podem assim assumir diversa natureza, nomeadamente, política (p.ex. cimeiras internacionais ou visitas de Estado), cultural (p.ex. concertos musicais ou festivais), desportiva (p.ex. organização de fases finais de campeonatos da europa, finais de liga dos campeões de futebol ou Jogos Olímpicos), científica ou económica (p.ex. conferências), religiosa (jornada mundial da juventude), entre outras.

8. Elevado número de cidadãos nacionais e, em muitos casos, estrangeiros;

9. Cooperação policial internacional e eventual assistência técnica;

10. Riscos diversos (álcool, drogas, falsificações, carteiristas, entre outros);

11. Ameaças e riscos transnacionais (terrorismo, criminalidade organizada, criminalidade violenta, cibercriminalidade, entre outros). (Elias, 2022, p. 408)

A organização de um GE requer, assim, por parte dos responsáveis de segurança, uma mudança de paradigma na atuação policial, forçando uma transição dum modelo reativo para um modelo proativo, estratégico e baseado em *intelligence*, exigindo "uma resposta extraordinária, planeada e executada através de um modelo de gestão, muitas vezes, com base na inteligência policial e trabalhando com limitações quantificáveis e uma capacidade disponível" (Elias, 2022, p. 408).

PERSPETIVAS

1. Planeamento operacional dum grande evento

O planeamento de segurança dum GE é um processo complexo, que se inicia com a definição de linhas estratégias orientadoras por parte da Direcção Nacional da PSP, passando posteriormente para uma fase de elaboração de planos de ação setoriais, ao nível operacional dos Comandos Metropolitanos, Regionais ou Distritais (Alves, 2015; Gomes, 2018; Gonçalves, 2014).

Na base do processo de definição das opções estratégicas, operacionais e táticas, estará, ao seu nível decisório, uma avaliação criteriosa da missão a desenvolver, com a necessária análise de risco inerente ao evento. No planeamento de grandes eventos, o processo decisório é corporalizado através da elaboração de uma ordem de operações que, conforme evidencia Moura (2009, p. 27), "contém medidas de coordenação necessárias para sincronizar a operação, que oriente a preparação de atividades, que permita distribuir recursos e que estabeleça a fita do tempo e as condições para a sua execução".

Torna-se assim nuclear que o decisor policial não efetue o planeamento "baseado no curso dos acontecimentos considerado mais expetáveis", mas sim apoiado numa "lógica contingencial, suportada no processo de gestão dos riscos e em que é crucial a elaboração de "cenários", que permitam definir, ponderar e validar um conjunto de opções decisórias (GODIAC, 2013; UNICRI-IPO, 2007; Oliveira, 2015; Ramos, 2005; Ribeiro, 2009; Torres, 2015a, 2015b)" (Carvalho, 2016, p. 14).

É precisamente da necessidade de "recolha, tratamento e difusão de informações com relevância para a segurança e ordem públicas" que os NIP concentram a sua atividade, afigurando-se fundamentais para o planeamento e execução de operações policiais, "na medida em que fornecem aos decisores o conhecimento necessário sobre as ameaças e os riscos" (Reis, 2017, p. 55).

Sendo unânime na literatura especializada (Carvalho, 2015, 2016; Elias, 2011; Fernandes, 2014; Moura, 2009; Torres, 2015a, 2015b, 2024; Rodrigues, 2024) que, independentemente do planeamento, "o risco é um aspeto inerente às operações policiais" (Moura, 2009, p. 29), o planeamento operacional tornar-se-á tão ou mais completo se o trabalho da INTELPOL for dotado de metodologias que permitam maior eficácia na avaliação do risco e subsequente geração de cenários, estabelecendo assim "ações que permitam reduzir o risco" (Moura, 2009, p. 29). É assim a base do planeamento operacional pois a "recolha, análise e difusão de informações permitem conhecer a ameaça, o terreno e as nossas próprias forças" (Oliveira, 2019, p. 74).

2. Otimização do processo de gestão do risco

Para uma organização policial, a adoção de metodologias de gestão do risco afigura-se fulcral para, com objetividade e adoção de procedimentos uniformes, capacitar os Comandantes com informação necessária para fundamentar, de forma racional e consciente, a tomada de decisão em todos os níveis hierárquicos (estratégico, operacional e tático), e, assim, aumentar a eficiência das suas operações.

No domínio da segurança, e com maior perspetivação na segurança pública, a gestão do risco poderá ser entendida como um processo estruturado e sistemático, que visa identificar, analisar e classificar os riscos, considerando o seu impacto nos objetivos estratégicos e na missão da organização nos casos concretos (Rodrigues, 2024; Torres, 2015a, 2024).

De acordo com a norma internacional ISO/FDIS 31000:2018, este processo é cíclico e contínuo, compreendendo quatro fases essenciais: 1) o estabelecimento do contexto; 2) a avaliação do risco; 3) o tratamento do risco e, por fim; 4) a monitorização e revisão de todo o ciclo. (Rodrigues, 2024)

2.1. Definição do contexto

O ponto de partida para qualquer processo de gestão do risco é, precisamente, a definição do seu contexto, que passa por efetuar uma análise profunda: ao ambiente interno (recursos, estrutura, cultura organizacional); ao ambiente externo (ambiente social, político, relação

com a comunidade); e ao contexto da própria gestão do risco (estratégia e protocolos que suportam todo o processo) (Hopkin, 2018, citado por Rodrigues, 2024).

Tendo como referência Torres (2015a, 2024), para a definição do contexto deverá o analista[3] "desenvolver um profundo estudo prévio sobre o setor de atividade e o ambiente socioeconómico que envolve a realidade em estudo…obtendo o máximo de informação possível, quer de fontes oficiais e oficiosas quer de partes interessadas"[4] (Torres, 2024, p. 27).

A definição do contexto é assim determinante, pois permite definir a relevância e a perceção dos riscos, na lógica de que um risco considerado inaceitável numa determinada sociedade ou evento poderá ser tolerado noutra, devendo ser tido em consideração durante todas as fases do processo (Rodrigues, 2024; Torres, 2015a, 2024).

2.2. Avaliação do risco

Posteriormente, avançamos para a "fase de charneira do processo de gestão do risco" (Torres, 2015, p. 45)" - a avaliação do risco - sendo a fase "que permite identificar de que forma os objetivos da entidade ou organização podem ser afetados, promovendo a análise do risco, estimando a probabilidade da sua concretização e as respetivas consequências" (Rodrigues, 2024, p. 19). Afigura-se assim um exercício de inteligência por excelência, que envolve:

> "O levantamento de vulnerabilidades dos ativos críticos, atribuição de um grau de probabilidade à concretização da ameaça e, sobretudo, à identificação dos impactos da concretização da ameaça. Este exercício revela-se como algo complexo e detalhado porquanto implica que seja efetuada uma análise interna – levantamento de vulnerabilidades – uma análise externa – aferição da probabilidade da concretização de ameaça – e uma conjunção de ambos, com a previsão das consequências, isto é, dos danos potencialmente resultantes da concretização da ameaça." (Rodrigues, 2024, p. 20)

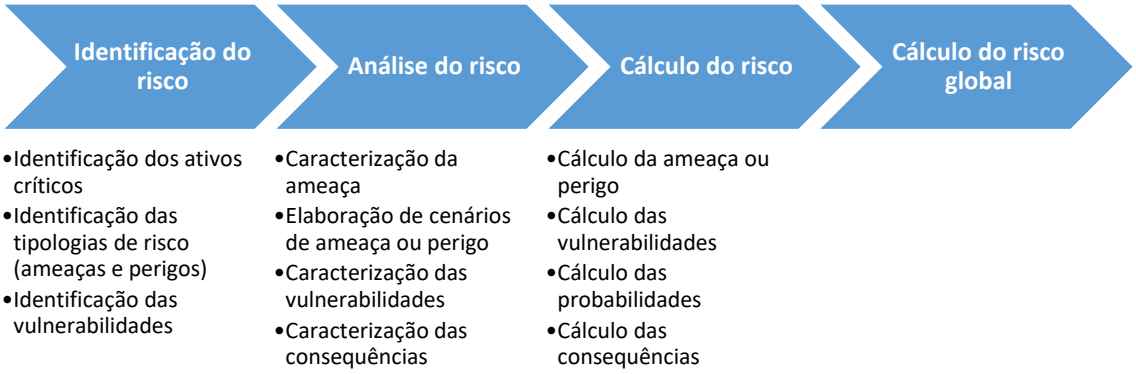
[3] O analista de informações é o Polícia que, pertencente ao Núcleo de Informações Policiais, tem como principal função a produção e difusão de produtos de inteligência policial operacional.

[4] Poderá, para tal, proceder a uma análise SWOT, correspondendo as Forças (S – strenghts) e as Fraquezas (W – weaknesses) ao contexto interno, e as Ameaças (T – threats) as Oportunidades (O – opportunities) ao contexto externo. (Torres, 2015a)

Sistematizado no estudo de Rodrigues (2024), a principal literatura dedicada à gestão dos riscos enumera três etapas a cumprir durante a fase da avaliação de risco: identificação do risco, análise do risco e cálculo do risco.

Tabela 1

Modelo de avaliação do risco



Nota: Adaptado de Rodrigues, 2024, p. 92

Seguidamente tentaremos refletir sobre cada fase da avaliação do risco, e de que forma pode o processo ser otimizado nos NIP, tendo em consideração os objetivos definidos para a presente investigação.

2.2.1. Identificação do risco

Torres (2015ª, p. 24) afirma que "para planear segurança há que ter a exata ideia do que é preciso proteger e/ou salvaguardar", e não podíamos estar mais de acordo.

Nesse sentido, a fase de identificação do risco deverá começar pela identificação e hierarquização dos ativos críticos suscetíveis de serem comprometidos, identificando sobre "o quê ou quem recai a ameaça" (Rodrigues, 2024, p. 23). Referente aos estudos de segurança, Torres (2015a) identifica seis grupos possíveis no campo dos ativos críticos, nomeadamente: pessoas; infraestruturas; equipamentos; informação; atividades e operações; e reputação. É nesta fase que o "o papel dos administradores de topo é absolutamente crucial", pois, apenas os próprios, juntamente com "outro pessoal qualificado e especializado, poderão dizer com propriedade os ativos mais importantes para as suas instituições" (Torres, 2024, p. 27) devendo, em coordenação com os analistas de informações: 1) elencar todos os ativos considerados críticos; 2) identificar os eventos indesejáveis e os impactos expectáveis; 3) valorar e graduar os ativos críticos tendo como base a sua eventual perda, total e/ou parcial.

Tabela 2

Tabela auxiliar de seleção/valoração de ativos críticos

Ativos Críticos		Valoração dos ativos					
		Importância para a missão	Dificuldade de substituição/perda de produtividade	Importância para a posição de liderança	Diferenciação tecnológica	Importância global	(…)
Pessoas	Ativo 1						
	Ativo 2						
	Ativo n						
Infraestruturas	(…)						
Equipamentos	(…)						
Informação	(…)						
Atividades	(…)						
Reputação	(…)						

Nota. Adaptado de Torres, 2024, p. 27

Na tabela auxiliar proposta (tabela 2), cada ativo dever ser assim qualificado numa escala de cinco graduações, que começa com o nível de "irrelevante", passando por "reduzida", "moderada", "elevada" e acabando no nível "crítico".

De seguida, após o minucioso levantamento dos ativos críticos a proteger, surge a etapa referente à identificação das ameaças (de origem humana e que subentende intencionalidade) e dos perigos (de origem natural ou acidental, sem intencionalidade) (Torres, 2015a, 2024), "realistas ou plausíveis" (Rodrigues, 2024, p. 25), com o propósito de "identificar a sua origem e tipologia, através do levantamento dos indicadores do risco que impendem sobre os ativos críticos" (Rodrigues, 2024, p. 25).

Numa lógica de facilitação do processo posterior de análise, a tabela 3 incorpora algumas fontes de ameaça (sendo uma tabela dinâmica, deverá ser adaptada à particularidade de cada evento) com os ativos críticos aos quais podem provocar danos, devendo o analista assinalar, para cada fonte de risco, os ativos que poderão ser afetados.

Tabela 3

Fontes de risco e ativos críticos

Fontes de risco / Ativos Críticos	Ativo 1	Ativo 2	Ativo 3	Ativo 4	Ativo 5	Ativo n
Multidão	X		X			X
Desastres naturias		X		X	X	
Incêndios			X			
Saúde Pública						
Protestos	X	X				
Terrorismo	X	X	X	X	X	X
Crminialidade			X		X	
Imagem Institucional		X				
(…)						

Nota. Adaptado de Rodrigues, 2024, p. 95

A terceira, e última, etapa da fase adstrita à identificação do risco procederá ao levantamento das vulnerabilidades dos ativos críticos, tendo em consideração as ameaças e perigos apurados nas etapas anteriores. Tomando como referência Rodrigues (2024, p. 25), as vulnerabilidades "correspondem ao grau de resistência ou resiliência ao evento com potencial para prejudicar o ativo em questão, criado pela ameaça, sendo que quanto maior for a vulnerabilidade, menor será a resistência ou resiliência".

Na sua análise, Torres (2015a, p. 40) distingue quatro eixos fundamentais de vulnerabilidade: 1) físicas - fragilidades nas infraestruturas físicas que falham em proteger os ativos; 2) tecnológicas - inexistência de meios tecnológicos adequados para detetar ou resistir a ameaças; 3) operacionais - erros pontuais na execução de procedimentos e protocolos, diretamente ligados ao fator humano; e 4) estruturais - falhas sistémicas relacionadas com uma "mentalidade e cultura de segurança" perene e difícil de alterar, como a falta de compromisso da organização com as normas de segurança.

Nesta etapa, competirá então ao NIP identificar e avaliar as vulnerabilidades considerando, genericamente: "1) número de fraquezas do sistema de segurança que estão na sua origem, 2) grau de dificuldade em serem exploradas e 3) eficácia das atuais contramedidas de segurança de que são alvo" (Torres, 2024, p. 43).

2.2.2. A análise do risco

Após a fase onde se identificaram os riscos, a análise dos mesmos aprofunda o conhecimento sobre cada elemento elencado. Segundo as normas ISO 31010:2009, a análise do risco "tem como objetivo desenvolver um conhecimento aprofundado do risco, criando as condições para que, na fase seguinte, o risco possa ser calculado" (Rodrigues, 2024, p. 27). É nesta fase que os analistas se irão debruçar na valoração das ameaças e na identificação da sua

capacidade em explorar as vulnerabilidades existentes (Fernandes, 2014; Rodrigues, 2024; Torres, 2015).

No contexto da INTELPOL, a análise das ameaças é um exercício minucioso que se foca em três vetores (Fernandes, 2014):

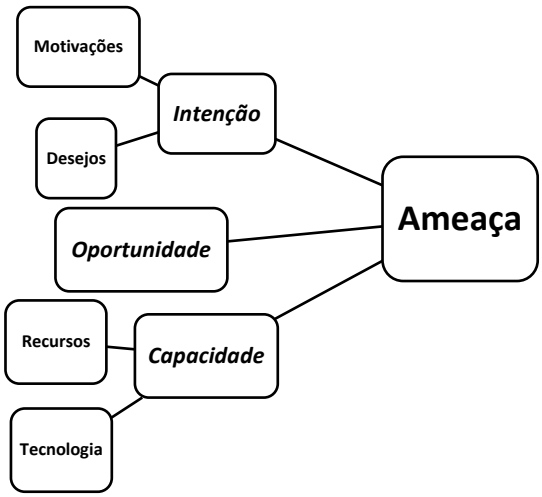
1) Intenção: as motivações, desejos e objetivos do agente da ameaça, pois "será a intenção que provocará no agente da ameaça o ímpeto de potenciar o evento que pretenderá causar danos ao ativo crítico" (Rodrigues, 2024, p. 29);

2) Capacidade: os recursos, meios e conhecimentos que o agente possui e que lhe permitirão concretizar o evento danoso;

3) Oportunidade: as circunstâncias externas que favorecem a ação do agente.

Figura 1

Componentes da Ameaça



Nota. Adaptado de Torres, 2024, p. 32

Consequentemente, a fase referente à análise das ameaças e dos perigos deverá ser um exercício atento e estruturado, com debate de ideias entre analistas experientes, devendo, para objetivar a caracterização das fontes do risco e a forma como poderão concretizar danos aos ativos críticos, auxiliar-se duma lista de questões genéricas. Deverão, assim, num *brainstorming* coletivo, integrar informações específicas

> que resultam da recolha, tratamento e análise dos dados e notícias relativos ao evento, em específico, considerando o seu contexto atual, ou seja, informações que de algum

> modo se afastem da caraterização efetuada, mas que possam contribuir para alterar as forças motrizes, podendo resultar de fatores aleatórios, o que poderá significar, ou não, o reforço de a hipótese da ameaça se verificar. (Rodrigues, 2024, p. 98)

Para finalizar a etapa referente à análise das ameaças ou perigos, os analistas, num exercício preditivo, deverão "recolher as ideias apresentadas sobre cenários de ameaças plausíveis, considerando os ativos críticos a proteger" (Rodrigues, 2024, p. 101) com o objetivo de identificar as situações que exigirão a tomada de medidas.

Simultaneamente à análise das ameaças, deverá ser levado a cabo a análise das vulnerabilidades, "devendo ser efetuada com as ameaças já identificadas e avaliadas" (Rodrigues, 2024, p. 30), pois uma vulnerabilidade só se torna relevante se puder ser explorada por uma ameaça plausível. Importa nesta fase ter presente que uma medida implementada para reduzir o risco inerente a uma determinada ameaça poderá, ela mesmo, constituir-se como uma vulnerabilidade para um outro tipo de ameaça ou perigo.

Nesta etapa, o analista deverá examinar as vulnerabilidades, permitindo que, a nível estratégico-operacional, seja facilmente percecionada "a ordenação das vulnerabilidades face à sua exposição perante os diferentes cenários de ameaça e perigo, apresentando-se como um bom ponto de partida para início da análise das vulnerabilidades" (Rodrigues, 2024, p. 103). A tabela seguinte, adaptada de Rodrigues (2024), sistematiza algumas vulnerabilidades possíveis num GE, face a possíveis ameaças, sendo meramente ilustrativo da metodologia que deverá ser adotada pelo analista de informações.

Tabela 4

Quadro de ameaças e vulnerabilidades

Vulnerabilidades/Ameaças	Confrontos com a polícia	Invasão de áreas restritas	Interrupção do evento	Confrontos entre grupos rivais	(…)
Falhas na monitorização dos sistemas de segurança	X	X	X	X	
Adequabilidade dos planos de segurança		X	X		
Capacidade de escoamento da multidão	X			X	
Existência de outras atividades perto do recinto do evento	X	X	X	X	
Acessibilidade/circulação no interior do recinto	X	X	X	X	
(…)					

Nota: Adaptado de Rodrigues, 2024, p.31

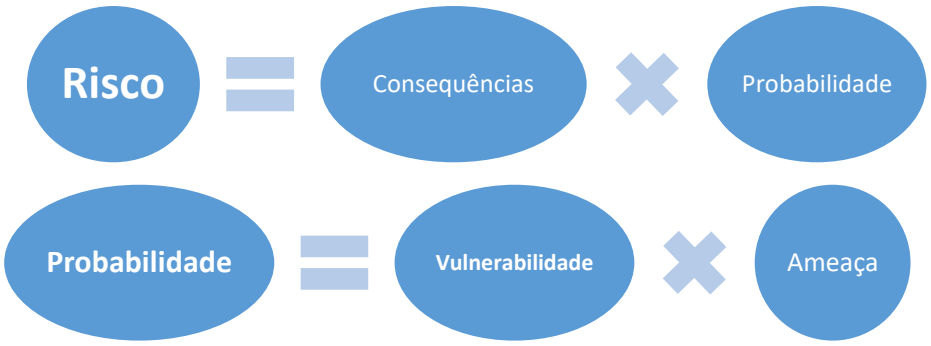
A fase referente à análise do risco culmina com a análise das consequências, ou impactos (Torres, 2024), que estima, mediante a exploração das vulnerabilidades, o dano potencialmente provocado nos ativos críticos pela concretização da ameaça (Rodrigues, 2024; Torres, 2015a), não apenas em termos materiais, mas também em custos de reparação, perda de produtividade e, crucialmente para a polícia, danos intangíveis como a reputação institucional e a confiança pública. Deverá então o analista, listar, para cada cenário de ameaça identificado, o conjunto de consequências ou impacto que a concretização do risco provocará, ou seja, que danos poderão ocorrer e com que gravidade. O estudo das consequências será particularmente relevante, "dado que será o vetor em análise com maior relevância para o decisor, a quem competirá, no âmbito do tratamento do risco, tomar opções e investir em medidas que devam fazer face às ameaças" (Rodrigues, 2024, p. 31).

2.2.3. Cálculo do risco

A última fase referente à avaliação do risco é precisamente o cálculo do risco, tendo este o objetivo de identificar se o risco que impede sobre o evento "se encontra dentro de limites considerados aceitáveis ou se, por outro lado, não é aceitável, e como tal, se se exige a tomada de medidas atinentes para que este nível se situe dentro dos parâmetros considerados adequados" (Rodrigues, 2024, p. 32). Dessa forma, será apurado o nível do risco, através da multiplicação do fator probabilidade, resultante da conjugação das ameaças com as vulnerabilidades, e o fator consequências (Fernandes, 2014; Rodrigues, 2024; Torres, 2015a, 2024). É precisamente da conjugação entre a ameaça e a vulnerabilidade que resulta a probabilidade de ocorrência de um evento adverso, a qual, "ao ser conjugada com as consequências na fase do cálculo do risco, irá resultar o nível de risco" (Rodrigues, 2024, p. 31)

Figura 2

Cálculo do risco e da probabilidade



Como modelo de otimização do processo de cálculo do risco numa SO/SINTEL, propomos a adoção duma escala de graduação de 5 níveis (muito baixo; baixo; médio; alto e muito alto), representada numa matriz de risco 5x5 (Rodrigues, 2024), adequando-se a uma forma mais resumida e intuitiva na amostragem dos resultados obtidos, facilitando o processo de tomada de decisão.

Tabela 5

Matriz de Risco

FATOR A	FATOR B					
	5º grau	5	10	15	20	25
	4º grau	4	8	12	16	20
	3º grau	3	6	9	12	15
	2º grau	2	4	6	8	10
	1º grau	1	2	3	4	5
		1º grau	2º grau	3º grau	4º grau	5º grau

Nota: Adaptado de Rodrigues, 2024, p. 107

Cálculo da Probabilidade

Conforme já exposto, o fator probabilidade resulta da multiplicação entre a ameaça e vulnerabilidade, pelo que deverá o analista, de forma isolada, obter os graus para cada um dos fatores em equação. Segundo Rodrigues (2024), numa lógica de facilitação na obtenção dum resultado entre 1 e 5, cada fator (ameaça e vulnerabilidade) será equacionado tendo em consideração cinco subfactores, propostas na tabela 6, cuja resposta binária permitirá o cálculo dentro do intervalo esperado. Adotando o algoritmo de cálculo de Rodrigues (2024), por o considerarmos adequado, tomaremos: o valor "1" para nenhuma resposta positiva; o valor "2" para uma resposta positiva; o valor "3" para duas respostas positivas; o valor "4" para três respostas positivas; e o valor "5" para quatro ou cinco respostas positivas.

Tabela 6

Cálculo do cenário da ameaça e das vulnerabilidades

Cálculo do cenário de ameaça
Existe intenção por parte do agente de ameaça em concretizar este cenário?
É reconhecida capacidade ao agente da ameaça ou ao perigo para concretizar este cenário?
Existe alguma circunstância específica que poderá representar uma janela de oportunidade para a concretização da ameaça ou do perigo?
Existe histórico de se ter verificado a ocorrência do cenário de ameaça ou perigo?
Foram recolhidas informações específicas que reforcem a hipótese de vir a ser concretizada o cenário de ameaça?
Cálculo das vulnerabilidades
A vulnerabilidade está assente em várias fragilidades?
A vulnerabilidade é de difícil correção?
As medidas existentes para reduzir as vulnerabilidades são ineficazes?
A vulnerabilidade é facilmente explorada pelos agentes de ameaça?
Em caso de sucesso na exploração da vulnerabilidade, não existem mais vulnerabilidades que o agente de ameaça necessite de explorar?

Nota: Adaptado de Rodrigues, 2024, p. 108

Desta forma, empregando o modelo a cada cenário, é possível obter o produto entre a ameaça e as vulnerabilidades a ela sujeitas, obtendo um valor variável entre 1 e 25. Aplicando a matriz de risco (tabela 5), obtemos um resultado de natureza qualitativa que variará entre: muito improvável; improvável; pouco provável; provável; e muito provável. (Rodrigues, 2024)

Cálculo das Consequências

A determinação do risco requer, fundamentalmente, que, à semelhança do fator probabilidade, as consequências associadas a uma ameaça sejam calculadas. Tal desiderato impõe a necessidade de traduzir os diferentes graus de consequências, numa escala numérica, seguindo o mesmo modelo da matriz do risco.

Dessa forma, cada cenário de ameaça deverá "ser avaliado quanto aos seus impactes potenciais multivetoriais" (Torres, 2015a, p. 61), equacionando "os impactes na entidade, organização, região/nação, projeto ou atividade, perante a concretização da ameaça em causa" (Torres, 2024, p. 68). Deve o analista "assumir um quadro de referência bastante alargado" (Torres, 2024, p. 68), tais como impactos financeiros/monetários, danos patrimoniais, perigo para a vida ou integridade física ou reputação institucional.

O procedimento de cálculo das consequências, conforme proposto na tabela 7, consistirá então na atribuição de valor aos múltiplos efeitos que advêm da materialização da referida ameaça, criando hipóteses de impacto transpostos para um resultado de natureza qualitativa: irrelevante; reduzida; moderado; elevado; crítico. (Rodrigues, 2024)

Tabela 7

Modelo para graduação das consequências dos cenários de ameaça

	Consequências Descritivas
5 - Crítico	Paralisação absoluta do evento, inoperacionalizando o funcionamento das instituições; grave impacto na integridade física das pessoas e perigo de morte; grave impacto na reputação das instituições, nacional e internacionalmente
4 - Elevado	Grave prejuízo em termos de capacidade de cumprimento da missão/objetivos, com impacto grave no desenrolar do evento que leve ao seu cancelamento e ocorrência de ferimentos graves nos participantes; grave impacto na reputação das instituições, nacional e internacionalmente
3 - Moderado	Redução apreciável, mas tolerável, na capacidade de cumprimento da missão/objetivos, com perturbação no desenrolar do evento e ocorrência de ferimentos ligeiros nos participantes; impacto na reputação das instituições a nível nacional
2 - Reduzido	Redução apreciável, mas tolerável, na capacidade de cumprimento da missão/objetivos, com perturbação no desenrolar do evento e ocorrência de ferimentos ligeiros nos participantes; impacto na reputação das instituições a nível local
1 - Irrelevante	Pequena perturbação do evento; sofrimento reduzido e sem gravidade para um número reduzido de pessoas; pequeno impacto na reputação das instituições, circunscrito ao local do evento.

Nota: Adaptado de Torres, 2024, p. 64

Cálculo do Risco Final

Conforme afirma Rodrigues (2024, p. 34), mais do que se cingir à apresentação dum mero resultado final, o cálculo do risco deverá, acima de tudo, "apresentar o contexto mais abrangente do risco, nomeadamente os riscos identificados que carecem de tratamento prioritário e que justifiquem maior investimento, bem como apresentar as considerações relativas ao impacto que este tratamento do risco possa ter, considerando os *stakeholders*", permitindo assim ao decisor poder interpretar os resultados do processo de gestão e, dessa forma, tomar decisões relativas à melhor forma de colmatar os riscos.

Para determinar o risco global, é essencial calcular previamente o risco associado a cada cenário de ameaça, individualmente. Esta abordagem granular é fundamental para a tomada de decisão e para a implementação de contramedidas eficazes e distintas, adequadas à natureza específica de cada vulnerabilidade explorada (Torres, 2024). Seguindo o mesmo modelo de quantificação das diversas análises efetuadas, propomos a utilização da seguinte escala numérica discreta para classificar os diferentes graus de probabilidade e consequência previamente apurados: 1 - muito baixo; 2 – baixo; 3 - médio; 4 – alto; e 5 - muito alto (Rodrigues, 2024).

Na tabela 8, exemplificamos um quadro-modelo de cálculo do risco dos cenários de ameaça, que, pela simplicidade de apresentação do processo de gestão do risco, permitirá aos Comandantes do policiamento aferir de forma intuitiva os cenários de ameaça que oferecem maior preocupação, bem como a interdependência entre eles e o seu impacto no policiamento.

Tabela 8

Cálculo do risco dos cenários de ameaça

Cenário	Probabilidade	Consequências	Risco
A - Confrontos com a polícia	Pouco provável	Elevadas	Alto
B -Invasão de áreas restritas	Improvável	Moderadas	Médio
C - Interrupção do evento	Improvável	Moderadas	Médio
D - Confrontos entre grupos rivais	Provável	Elevadas	Muito alto
(…)	**(…)**	**(…)**	**(…)**

A aferição do risco global, embora meramente indicativo para caracterizar na globalidade o evento, requer uma abordagem que transcenda a aplicação de fórmulas matemáticas convencionais. Para assegurar o “realismo e pragmatismo” (Rodrigues, 2024, p. 114) necessário, o presente estudo adota uma abordagem qualitativa, fundamentada no algoritmo desenvolvido por Rodrigues (2024), que se baseia num conjunto de regras de precedência. Neste modelo, a classificação do cenário mais grave tem um peso determinante: a ocorrência de um ou mais cenários de risco "muito alto", ou de dois cenários "alto", eleva o risco global para o nível máximo. De igual modo: um cenário "alto" ou três cenários "médio" são suficientes para definir o risco global como "alto"; a verificação de dois cenários “médio” resultarão num risco global “médio”; a verificação de todos os cenários risco “muito baixo” ou todos as restantes combinações não previstas anteriormente, resultarão num risco global

"muito baixo". Desta forma, acreditamos que o resultado final será sempre um reflexo realista e prudente das vulnerabilidades identificadas.

2.3. Tratamento do risco

Findo o processo de avaliação do risco, segue-se o tratamento do risco, a fase em que a análise se transforma em ação. Num trabalho de estreita colaboração entre os analistas e os Comandantes envolvidos na operação policial, enquanto decisores máximos das opções estratégico-operacionais a adotar, são escolhidas as opções mais adequadas para lidar com os riscos calculados. Esta decisão deve ser transparente e fundamentada na melhor informação disponível, considerando sempre a relação custo/benefício de cada contramedida (Torres, 2024).

Hopkin (2018), citado por Rodrigues (2024), identifica quatro estratégias fundamentais para o tratamento do risco:

1) aceitar o risco – de forma informada e consciente o risco não justifica o investimento em contramedidas, sendo adequada para riscos de nível baixo, onde a probabilidade e as consequências são reduzidas;

2) transferir o risco – através da externalização de parte da responsabilidade do risco para outra entidade, muito frequente através da articulação com empresas de segurança privada, assumindo as forças de segurança funções específicas de supervisão e controlo;

3) reduzir o risco - é a estratégia mais comum, que implica a adoção de contramedidas para diminuir a probabilidade de um evento ocorrer ou para mitigar as suas consequências (ex.: policiamento dissuasor, controlo de acessos);

4) eliminar o risco - A abordagem mais adequada para fazer face a riscos muito elevados. Pode envolver uma atuação diretamente no ativo crítico a proteger, com a cessação da atividade que gera o risco (ex: cancelamento do evento), a neutralização da fonte da ameaça (ex: detenção de suspeitos), ou uma abordagem sobre as consequências, criando condições para reduzir o impacto da materialização da ameaça (ex.: sistema de redundância das fontes de energia, por forma a colmatar a falha do sistema de energia principal).

Não obstante, importa ter presente que o risco nunca será erradicado na sua totalidade, considerando a existência dum risco residual, compreendendo os riscos que "subsistem após o tratamento e que, em alguns casos, não são sequer conhecidos pelo gestor de risco" (Rodrigues, 2024, p. 43).

3. Geração de cenários

Uma das mais valiosas ferramentas da INTELPOL é a geração de cenários que, interligada de forma umbilical com o processo de gestão do risco, constitui a sua aplicação prática (Carvalho, 2016). Longe de serem meras hipóteses ou suposições, os cenários são "narrativas estruturadas representativas de futuros possíveis" (Carvalho, 2016, p. 16), que descrevem sequências plausíveis de acontecimentos, sendo um processo metodológico que obriga a uma reflexão disciplinada, longe dum mero exercício de adivinhação.

O objetivo da projeção de cenários não é o de prever qual deles irá efetivamente ocorrer, mas sim preparar a força de segurança para um conjunto de eventualidades. Como sublinha Torres (2015b, p. 150), esta lógica contingencial é crucial para a elaboração de "cenários realistas com respostas ajustadas", permitindo a preparação prévia de planos de contingência.

Relativamente à metodologia para a criação de cenários, podemos considerar que a mesma é uma atividade de natureza colaborativa, que deve envolver não apenas os analistas de informações, mas também os destinatários finais dos cenários, como os Comandantes operacionais, para garantir a sua pertinência e utilidade (Carvalho, 2016; Torres, 2015b).

De forma a explorar um leque representativo de futuros plausíveis, sem sobrecarregar, contudo, o processo de decisão, concordamos com Carvalho (2016, p. 22) que aponta para a elaboração “entre 3 e 5 cenários", e que descreve as etapas típicas e sequenciais que compõem o processo metodológico da geração de cenários:

1) Definição do contexto e dos objetivos: é a fase inicial e fundamental do processo, sendo definida, com clareza, a situação ou problema a ser analisado, os principais objetivos a alcançar com os cenários, o horizonte temporal de referência e quem são os intervenientes e destinatários do processo.

2) Análise de perceções e pressupostos: nesta etapa, o objetivo é explorar e desafiar as crenças e pressupostos existentes sobre a situação em estudo, procurando-se identificar possíveis enviesamentos cognitivos e os "quadros-mentais" que podem limitar a análise, não se limitando a projetar o passado no futuro, mas explorando um leque verdadeiramente diversificado de futuros plausíveis.

3) Identificação e análise dos elementos essenciais: identificam-se os elementos-chave que influenciarão o futuro, como tendências, comportamentos de atores e eventos significativos, recaindo o foco sobre as "incertezas críticas" que, além de manifestamente imprevisíveis, possuem maior potencial de impacto.

4) Construção dos cenários: com base nas incertezas críticas, procede-se à construção de um número limitado de cenários, devendo adotar uma narrativa estruturada, coerente e plausível, que descreve uma sequência de acontecimentos que conduzem a um futuro possível e distintos entre os vários cenários projetados.

5) Análise das implicações dos cenários: uma vez construídos os cenários, esta etapa foca-se na análise das suas potenciais consequências estratégicas, aferindo a robustez dos planos existentes, e delineando novas opções estratégicas com base na definição de respostas flexíveis.

6) Seleção e monitorização de indicadores: a etapa final consiste em selecionar um conjunto de indicadores a partir dos cenários elaborados. Estes indicadores funcionam como 'sinais' ou "*early warnings* que permitam alertar oportunamente o decisor face aos primeiros sinais de mudanças ou descontinuidades iminentes, minimizando as hipóteses de surpresas estratégicas" (Carvalho, 2016, p. 23).

Conforme afirma Oliveira (2015), citado por Carvalho (2016, p. 14), um planeamento que considere a informação obtida através da análise e avaliação do risco, e materializada na projeção de cenários plausíveis, "permitirá dotar o Comandante do policiamento de um excelente instrumento de apoio à tomada de decisão (…). Revelará principalmente, as várias opções disponíveis para lidar com os problemas que possam surgir a cada momento e as suas potenciais consequências".

CONCLUSÃO

O presente trabalho de investigação debruçou-se sobre a otimização da Inteligência Policial Operacional no planeamento de grandes eventos, partindo da questão central: "Que processos metodológicos devem ser adotados pelos NIP para transformar a análise de risco e a geração de cenários numa ferramenta eficaz de apoio ao planeamento operacional de grandes eventos?" e desdobrando-se numa breve análise teórica acerca da importância da INTELPOL e do POI, assim como, de forma exaustiva, na relevância da inteligência operacional para o planeamento de grandes eventos.

Ao longo do trabalho esforçámo-nos por demonstrar a inegável pertinência deste tema no atual contexto de globalização e de ameaças complexas, exigindo os "grandes eventos", pela sua natureza e exposição mediática, novas formas de atuação por parte das forças de segurança, que transcendam os modelos de policiamento mais reativos (Elias, 2022). Evidenciamos assim que a Inteligência Policial Operacional se apresenta como um pilar fundamental de um planeamento proactivo, capacitando os Comandantes a antecipar

ameaças, a compreender as vulnerabilidades e a alocar recursos de forma mais eficiente e eficaz. Conforme evidenciado por Torres (2015a, 2024), a sua função é a de transformar a incerteza num risco calculado, alicerçando a tomada de decisão em conhecimento fundamentado e não em meras suposições.

Não obstante, a aplicação deste princípio nem sempre se verifica na prática. Esta falha metodológica é frequentemente uma consequência de rotinas institucionais e de uma insuficiência nas informações que suportam o processo de decisão:

> "Os decisores são tentados a elaborar planos de ação baseados num único cenário - o mais expetável face ao histórico - ou, frequentemente, o que lhes convém mais por força das teses em que acreditam, das competências que dominam ou até das suas intuições. Ou, simplesmente, deixam-se vencer pela rotina, preparando-se automaticamente sempre do mesmo modo" (Torres, 2015b, p. 142).

Contudo, importa ter presente que a implementação do POI acarreta uma profunda mudança cultural e organizacional dentro das próprias forças de segurança (Carter & Carter, 2009; Ratcliffe, 2016), sendo necessário fomentar uma cultura de partilha de informação entre diferentes unidades e níveis hierárquicos, quebrando as tradicionais 'quintinhas' de conhecimento e exigindo que os Comandantes comuniquem claramente as suas necessidades de informação, assim como os analistas, por sua vez, produzam conhecimento relevante, oportuno e que possa influenciar diretamente o planeamento e a execução das operações (Fernandes, 2014).

A superação deste desafio exige uma aposta forte, e inequívoca, por parte das instituições policiais, materializadas num investimento sustentado em recursos humanos e tecnológicos (fundamental para a recolha, processamento e análise de grandes volumes de dados). Acreditamos também que a capacidade de desenvolver um planeamento de segurança que se adapte e resista às adversidades, assenta, com bastante veemência, na preparação e formação de analistas tecnicamente qualificados, com competências avançadas no processo de gestão do risco e na geração de cenários.

Por fim, podemos conclui que a eficácia da INTELPOL, nomeadamente no nível da Inteligência Operacional é a garantia final para a eficácia da segurança a grandes eventos, refletindo-se, de forma crescente, como uma montra da modernidade e da capacidade organizativa da instituição policial e do próprio Estado.

REFERÊNCIAS

Acosta, J., Merino, W., & Zometa, D. (2015). El impacto de la Inteligencia Policial en la toma de decisiones estratégicas, operativas y tácticas en la Policía Nacional Civil de El Salvador. *Policía y seguridad pública, Vol. 2, Nº 5*, 351-414. https://dialnet.unirioja.es/servlet/articulo?codigo=6522954

Alves, F. (2015). *Planeamento de operações policiais: Protocolo/Procedimentos de actuação em cenários de risco. Caso prático - manifestações no COMETLIS* [Trabalho individual final no âmbito do 1º CCDP, ICSPSI]. Repositório Comum. http://hdl.handle.net/10400.26/34790

Araújo, A. (2019). *O policiamento e as informações na divisão policial de Sintra: Entre a realidade e a utopia* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/30330

Barradas, J. (2015). *Da intercepção de comunicações, acções encobertas e serviços de informações: Os meios essenciais na recolha de intelligence* [Dissertação de mestrado, Faculdade de Direito da Universidade Nova de Lisboa]. Repositório Comum. http://hdl.handle.net/10362/16424

Brandão, A. P. (2004). Segurança: um conceito contestado em debate. *Informações e segurança: Estudos em honra do General Pedro Cardoso,* 37-54. Prefácio - Edições de Livros e Revistas, Lda.

Bravo, R. (2011). *Contributo para os estudos de intelligence sobre os sete espaços de conflito - Por um modelo holístico de análise.* Obtido de https://www.academia.edu/699210/CONTRIBUTO_PARA_ESTUDOS_DE_INTELLIGENCE_SOBRE_OS_SETE_ESPA%C3%87OS_DE_CONFLITO_POR_UM_MODELO_HOL%C3%8DSTICO_DE_AN%C3%81LISE

Camacho, J. (2015). *A mobilidade da informação na Polícia de Segurança Pública. Uma estratégia para a gestão operacional* [Dissertação de mestrado, ISCSP/UL]. Repositório Comum. http://hdl.handle.net/10400.5/11546

Carter, D. (2009). *Law enforcement intelligence: A guide for state, local and tribal enforcement agencies* (second edition). U. S. Department of Justice. Obtido de https://irp.fas.org/agency/doj/lei.pdf

Carter, D. L., & Carter, J. G. (2009). Intelligence-led policing: conceptual and functional considerations for public policy. *Criminal justice policy review, 20(3),* 310-325. doi:https://doi.org/10.1177/0887403408327381

Carvalho, J. (2009). Segurança nacional, serviços de informações e as forças armadas. *Segurança e Defesa nº 11 (Setembro-Novembro)*, 16-28.

Carvalho, J. (2015). *Prospetiva e intelligence policial. Estudo da utilidade da geração de cenários* [Dissertação de Mestrado, ISCSP/UL].

Carvalho, J. (2016). *A Geração de cenário no planeamento de operações policiais. Uma reflexão metodológica* [Trabalho individual final no âmbito do 2º CCDP, ICSPSI]. Repositório Comum. http://hdl.handle.net/10400.26/35324

Cavaleiro, R. (2016). *Modelo integrado de segurança em eventos desportivos. Portugal e a nova conceção europeia* [Trabalho individual final no âmbito do 2º CCDP, ICSPSI]. Repositório Comum. http://hdl.handle.net/10400.26/35330

Clemente, P. (1996). *Da polícia em ordem pública.* Governo Civil do Distrito de Lisboa.

Clemente, P. (2009). A ordem em público. *Reuniões e manifestações - Actuação policial,* 119-139. Almedina.

Clemente, P. (2010). Polícia e segurança – Breves notas. *Política internacional e segurança, n.º 4*, 139-169. Lusíada.

Clemente, P. (2015). *Cidadania, polícia e segurança.* Instituto Superior de Ciências Policiais e Segurança Interna.

Costa, D. (2011). *Policing diversity. A atuação policial proativa perante a diversidade de grupos minoritários. Estudo exploratório na área da 34.ª Esquadra - Olivais* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/24490

Costa, P. (2015). *A inteligência policial. Análise do modelo de funcionamento das unidades de informações desportivas.* [Trabalho individual final no âmbito do 1º CCDP, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/34626

Costa, R. (2017). *Inteligência Policial Judiciária: Os limites doutrinários e legais na assessoria eficaz à repressão ao crime organizado* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/25370

Costa, T. (2018). *Comportamentos de risco associados ao futebol. Um estudo exploratório* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/25022

DHS. (April de 2011). *Risk management fundamentals. Homeland security risk management doctrine.* U.S. Department of Homeland Security. Obtido de https://www.dhs.gov/publication/risk-management-fundamentals

Dias, H. V. (2011). Breve contributo para uma teoria dos serviços de informações. *Politeia - Ano VIII*, 51-83.

Dias, H. V. (2015). Os serviços de informações: atividade, organização, poder e controlo. *Politeia - Ano X-XI-XII*, 155-183.

Elias, L. (2011). *Segurança na contemporaneidade - Internacionalização e comunitarização* [Tese de doutoramento, FCSH/UNL]. Repositório da Universisade Nova de Lisboa. http://hdl.handle.net/10362/14011

Elias, L. (2022). *Ciências policiais e segurança interna. Desafios e prospetiva (2ª Edição).* Instituto Superior de Ciências Policiais e Segurança Interna.

Fernandes, L. F. (2014). *Intelligence e segurança interna.* Instituto Superior de Ciências Policiais e Segurança Interna.

Ferreira, N. (2011). *Predictive policing. Uma técnica complementar ao serviço do PIPP* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/24519

Fortes, A. (2020). *Informações de segurança versus informações policiais: Complementaridade ou sobreposição?* [Trabalho individual final do curso de Estado-Maior conjunto, IUM]. Repositório Comum http://hdl.handle.net/10400.26/33127

Gill, P., & Phythian, M. (January de 2016). What is intelligence studies?. *The international journal of intelligence security and public affairs, 18*, 5-19. doi:10.1080/23800992.2016.1150679

Gomes, J. (2018). *A decisão policial em grandes eventos desportivos. Um estudo naturalista* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/25698

Gonçalves, A. (2014). *A tomada de decisão policial nos grandes eventos desportivos* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/15106

Goulão, J. (2016). *Avaliação do risco: Métodos quantitativos aplicados a eventos de ordem pública* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/21078

Guimarães, M. (2022). O risco e a segurança no NITTO ATP FINALS 2021. Estudo de caso [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/41470

Guinote, H. (Janeiro/Junho de 2006). O sentimento de insegurança e os diversos poderes. *Politeia: Ano III*, 29-62.

Hoggett, J., & Stott, C. (June de 2010). Crowd psychology & public order policing: An overview of scientific theory and evidence. *Policing-an international journal of police strategies & management – policing, 33*, 218-235. doi:10.1108/13639511011044858

James, A. (2013). *Examining intelligence-led policing. Developments in research, policy and practice.* Palgrave Macmillan. doi:10.1057/9781137307378

Marta, R. (2023). *Subsídios para a construção de um modelo estratégico de segurança nos grandes eventos desportivos* [Trabalho individual final no âmbito do 5º CCDP, ICSPSI]. Repositório Comum. http://hdl.handle.net/10400.26/45944

Moura, P. (2009). *A análise do risco no planeamento operacional* [Trabalho individual final no âmbito do 3º CDEP, ICSPSI]. ISCPSI.

Oliveira, C. (2019). *Planeamento de segurança de grandes eventos. Estudo de caso: Web Summit 2018* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/31637

Peña, J. (2012). Inteligencia táctica. *UNISCI discussion papers, Nº 28 (Enero / January)*, 213-232. Obtido de https://www.unisci.es/journal-uniscirevista-unisci-no-28-enero-2012-asia-central-ee-uu-asia-pacifico-pacifismo-terrorismo-y-derechos-humanos-inteligencia-santa-sede/

Pereira, A. (2020). *Do modelo de policiamento tradicional ao modelo de intelligence-led policing: Estudo comparativo* [Dissertação de mestrado, Academia Militar]. Repositório Comum. http://hdl.handle.net/10400.26/34624

Pinheiro, A. (2017). *Um estudo sobre a decisão policial no contexto dos grandes eventos desportivos* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/19933

Pinto, F. (2017). *Gestão de grandes eventos. A herança do Euro 2004: Planeamento e comando do policiamento a um grande evento desportivo nacional de risco elevado.* [Trabalho individual final no âmbito do 4º CDEP, ICSPSI]. Repositório Comum. Obtido de http://hdl.handle.net/10400.26/35145

Quivy, R., & Campenhoudt, L. (1998). *Manual de investigação em ciências sociais* (2.ª ed.). Trajetos.

Ratcliffe, J. (2016). *Intelligence-led policing* (Second Edition ed.). Routledge.

Reis, P. (2017). *A tomada de decisão dos comandantes de polícia em grandes eventos políticos* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/19930

Rodrigues, I. (2024). *Avaliação do risco em grandes eventos desportivos* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/58160

Rodrigues, J. (2025). *As informações e o modelo de policiamento de proximidade: Potencialidades de articulação* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/58428

Santos, R. (2015). *Dialogue policing: Uma nova abordagem à gestão de multidões* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/32239

Silva, C. R. (2017). *Inteligência criminal e investigação criminal prospetiva: Estudo de caso do fenómeno de criminalidade itinerante. Lanzas internacionales em Portugal* [Trabalho individual final no âmbito do 4º CDEP, ICSPSI]. Repositório Comum. http://hdl.handle.net/10400.26/35125

Silva, S. (2014). *Policiamento de proximidade e intelligence-led policing: A necessidade da partilha de informação para um melhor desempenho policial* [Dissertação de mestrado, ISCPSI]. Repositório Comum. http://hdl.handle.net/10400.26/15391

Spiller, S. (2006). The FBI's field intelligence groups and police. Joining forces. *FBI law enforcement bulletin. Volume 75*, 1-6. Obtido de https://www.ojp.gov/ncjrs/virtual-library/abstracts/fbis-field-intelligence-groups-and-police-joining-forces

Torres, B. (2019). Segurança interna - (Des)centralização de competências. *Janus 2018-2019*, 112-113.

Torres, J. (2011). Segurança "just-in-time": abandonar de vez o paradigma da mão-de-obra intensiva. *Politeia - Ano VIII*, 235-247.

Torres, J. (2015a). *Gestão de riscos no planeamento, execução e auditoria de segurança.* ISCPSI-ICPOL.

Torres, J. (2015b). Gestão contingencial de cenários de risco para a segurança pública. in M. M. Valente, *Ciências policiais e política criminal. Justiça e segurança: um discurso de liberdade democrática* (pp. 141-165). ISCPSI.

Torres, J. (2018). Terrorismo do séc. XXI: Lidar com o risco ou com a incerteza?. *Segurança e Defesa n.º38 (janeiro - Março)*, 14-31.

Torres, J. (2024). *Manuel de Gestão do Risco e da Incerteza.* ISCPSI-ICPOL.

Toscano, R. (2022). *Inteligência tática: Informações just-in-time* [Trabalho individual final no âmbito do 5º CCDP, ICSPSI]. Repositório Comum. http://hdl.handle.net/10400.26/46004

UNICRI. (2007). *IPO modelo de planeamento da segurança.* (ISCPSI, Trad.)

UNICRI. (2011). *Foundations of the european house of major events security. A manual for the international coordination os major events security research in Europe.* UNICRI

- United Nations Interregional Crime and Justice Research Institute. Obtido de https://unicri.org/sites/default/files/2019-11/EU-Sec%20II%20Manual.pdf

UNICRI. (2014). *The european house of major events security: A user guide for police security planners and policy makers*. UNICRI - United Nations Interregional Crime and Justice Research Institute. Obtido de https://unicri.org/european-house-major-events-security-user-guide-police-security-planners-and-policy-makers

UNODC. (2006). *Policing. Police information and intelligence systems. Criminal justice assessment toolkit.* United Nations.

UNODC. (2020). *Criminal intelligence. Manual for front-line law enforcement*. United Nations.

Warner, M. (2002). Wanted: a definition of "intelligence". Understanding our craft. *Studies in intelligence Vol. 46 No. 3*. Obtido de https://www.cia.gov/resources/csi/studies-in-intelligence/volume-46-no-3/

Weisburd, D. a. (2004). What can police do to reduce crime, disorder, and fear?. *The ANNALS of the american academy of political and social science, 593*, 42-65. doi:https://doi.org/10.1177/0002716203262548