RBI

Revista Brasileira de Inteligência

Número 14
Dezembro 2019
ISSN Online 2595-4717
ISSN Impressa 1809-2632

ABIN 20 Anos

PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Revista Brasileira de Inteligência

ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online

dro Nogueira Gonçalves Diogo, Rodrigo Cerveira Cittadino, Roniere Ribeiro do Amaral, Ryan de Sousa Oliveira, Uver Oliveira Cabral.

Capa
Helen Santos Rigaud.

Editoração Gráfica
Luciano Daniel da Silva.

Revisão
Ana Beatriz Vieira Coelho Pereira, Caio Márcio Pereira Lyrio, Cláudia Suzano de Almeida, Eva Maria Dias Allam, Luiza da Silva, Sandra Mara Santa Barba Miranda, Uver Oliveira Cabral.

Catalogação bibliográfica internacional, normalização e editoração
Centro de Fontes Abertas - CFA/CGPAS/ESINT.

Disponível em
http://www.abin.gov.br

Contato
SPO Área 5, quadra 1, bloco D
CEP: 70610-905 – Brasília/DF
E-mail: revista@abin.gov.br

Tiragem desta edição
500 exemplares.

Impressão
Gráfica - Abin.

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência.
– n. 14 (dez. 2019) – Brasília: Abin, 2005 –
126 p.
Anual
ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online
1. Atividade de Inteligência – Periódicos 1. Agência Brasileira de Inteligência.

CDU: 355.40(81)(051)

SUMÁRIO

Editorial

A Agência Brasileira de Inteligência (ABIN), criada em 7 de dezembro de 1999, por meio da Lei nº 9.883/99, chancela o compromisso do Estado brasileiro com a consolidação de uma Inteligência compatível com a grandeza do País e comprometida com a inafastável observância dos ditames constitucionais enfeixados no instituto do Estado Democrático de Direito.

Neste cenário, a Revista Brasileira de Inteligência (RBI), em suas sucessivas edições, consagra-se como um relevante canal de diálogo entre a comunidade de Inteligência e a sociedade nacional. Revista de amplo acesso público, publicada nos formatos impresso e digital, a RBI celebra, nesta 14ª edição, os 20 anos de nossa respeitável ABIN, instituição responsável pela revista.

O aperfeiçoamento contínuo da RBI reafirma sua vocação para o fomento de debates e reflexões acadêmicas voltadas ao aprimoramento da cultura de Inteligência, bem como ao avanço científico nesta área do conhecimento tão imprescindível e instigante.

Boa leitura!

Gibran Ayupe Mota
Diretor da Escola de Inteligência

VIESES COGNITIVOS NA ATIVIDADE DE INTELIGÊNCIA: CONCEITOS, CATEGORIAS E MÉTODOS DE MITIGAÇÃO

Christiano Ambros *
Daniel Lodetti **

Resumo

Desde que comissões congressuais dos Estados Unidos da América avaliaram que parte das falhas da Inteligência nacional nos atentados terroristas de setembro de 2001 e na Guerra do Iraque de 2003 originaram-se na análise, o debate sobre erros analíticos advindos de vieses cognitivos e técnicas para mitigá-los vem crescendo significativamente. Vieses cognitivos são erros sistemáticos que ocorrem como uma estratégia de simplificação no processamento da informação e que se repetem de forma previsível em circunstâncias particulares. Na Atividade de Inteligência, essas estratégias mentais representam risco para uma exitosa análise de Inteligência. Profissionais de Inteligência são treinados a desenvolver capacidades variadas, mas, muitas vezes, não são ensinados a ter consciência de seus modelos mentais, a analisar seu próprio processamento de informações e a questionar seus pressupostos analíticos. Portanto, estão vulneráveis a cometer erros de análise oriundos de vieses cognitivos. O presente artigo objetiva discutir, de forma clara, prática e objetiva, o conceito de vieses cognitivos, apresentar os vieses cognitivos que mais afetam a Atividade de Inteligência e debater técnicas de análise estruturada, consideradas ferramentas que podem mitigar o impacto negativo dos vieses cognitivos na Inteligência.

Palavras-chaves: viés cognitivo, técnicas de análise estruturada, análise de Inteligência, falhas de Inteligência.

COGNITIVE BIASES IN THE INTELLIGENCE ACTIVITY: CONCEPTS, CATEGORIES AND MITIGATION METHODS

Abstract

Since US Congressional Committees have assessed that part of the failures of National Intelligence in the September 2001 terrorist attacks and the 2003 Iraq War originated in the analysis, the debate over analytical errors stemming from cognitive biases and techniques to mitigate them has been growing significantly. Cognitive biases are systematic errors that occur as a simplification strategy in information processing and they are predictably repeated under particular circumstances. In the Intelligence Activity, these mental strategies pose a risk for successful Intelligence analysis. Intelligence professionals are trained to develop varied skills, but often are not taught to be aware of their mental models, to analyze their own information processing, and to question their analytical assumptions. Therefore, they are vulnerable to making analysis errors arising from cognitive biases. This article aims to discuss, straightforwardly, comprehensively and objectively, the concept of cognitive biases, to present the cognitive biases that most affect the Intelligence Activity, and to discuss techniques of structured analysis, tools that can mitigate the negative impact of cognitive biases on intelligence.

Keywords: *cognitive bias, structured analytic techniques, Intelligence analysis, intelligence failures.*

* Doutor em Ciência Política pela Universidade Federal do Rio Grande do Sul (UFRGS). Pesquisador associado do Centro de Estudos sobre Governo (CEGOV) da UFRGS

** Bacharel em Economia pela Universidade Federal de Santa Catarina (UFSC)

Introdução

A extensa literatura sobre falhas de Inteligência e surpresa estratégica costuma focar em aspectos como o desenho institucional das agências e os sistemas de obtenção de informações, mas negligencia os erros na análise de Inteligência e os aspectos cognitivos dos analistas (HANDEL, 1984; ZEGART, 1999; BRUNEAU & BORAZ, 2007; GILL, 2007). Betts (2009b, 91) afirma que as avaliações das falhas de Inteligência, até o início dos anos 2000, preocupavam-se em como aperfeiçoar a coleta de Inteligência, mas marginalizavam a melhora dos procedimentos analíticos.

Desde os atentados de 11 de setembro de 2001 e, com mais ênfase, desde as falhas da Inteligência estadunidense na Guerra do Iraque de 2003, o debate sobre erros analíticos e técnicas para o aperfeiçoamento da análise vem crescendo significativamente (GEORGE & BRUCE, 2008; PHYTIAN, 2009; KERBBELL *et alii*, 2010). A lógica desse debate é clara: tendo em vista que as falhas de Inteligência decorrem de falhas humanas, ao melhorar a qualidade da análise de Inteligência, é provável que se reduza a probabilidade de estimativas erradas (BAR-JOSEPH, 2008, p. 134).

Os erros de análise podem ocorrer em diferentes etapas no trabalho da Inteligência. Esses erros têm origem em causas diversas, como pressupostos falsos, escassez de tempo, orientação ao consenso entre os analistas, disfunções nas organizações, interpretações motivadas (JORDAN, 2011) e problemas relacionados à própria coleta de informações. Se considerarmos os aspectos cognitivos individuais do analista, poderíamos identificar quatro dimensões subconscientes – ou conscientes em determinado grau – que influenciam o modo de percepção e avaliação de informações: a dimensão ambiental e sistêmica[1], a dimensão ideológica[2], a dimensão emocional[3] e a dimensão cognitiva.

A dimensão cognitiva é a mais universal delas, na medida em que resulta do desenvolvimento neurológico do cérebro humano e afeta todos de maneira muito similar, diferentemente das outras dimensões, que são idiossincráticas. A dimensão cognitiva refere-se aos procedimentos mentais subconscientes, aos atalhos cognitivos automáticos e às estratégias simplificadoras que possibilitam ao cérebro lidar com o volume e a complexidade de informações que recebe. Esses mecanismos de simplificação estratégica do processamento de informações, apesar de

1 Esta dimensão se relaciona aos modelos mentais e esquemas cognitivos que internalizamos a partir da adaptação ao ambiente em que estamos inseridos; em função disso, reproduzimos percepções, julgamentos e comportamentos de forma automática e inconsciente, e consideramos como naturais padrões que são sistêmicos. Para uma abordagem teórica sobre esta dimensão na Ciência Política, ver Neoinstitucionalismo Histórico Sociológico em Hall e Taylor, 1996, p.18.

2 Na dimensão ideológica, nossos esquemas mentais e modelos cognitivos são impactados por crenças, conceitos gerais, regras e estereótipos obtidos durante nossa vida de acordo com nossas experiências e nossa interpretação passada da realidade. Para uma interpretação do papel da dimensão ideológica na política externa e relações internacionais, ver Herz (1994).

3 Ainda que o papel das emoções no processamento de informações seja muito debatido, uma série de descobertas atuais da neurociência, que utiliza tecnologias de ponta da tomografia digital, evidenciam a dimensão emocional como fundamental para percepção, julgamento e tomada de decisão dos indivíduos. Para abordagens nos âmbitos da sociologia e da ciência política, ver Elster (1994) e Mintz & DeRouen (2010). No campo da neurociência, ver Pinker (1999) e Damacio (1994).

ser uma bem-sucedida adaptação evolutiva do cérebro, também criam armadilhas cognitivas, chamadas de heurísticas ou de vieses cognitivos.

No contexto da Atividade de Inteligência, vieses cognitivos são uma grande ameaça para uma exitosa análise de Inteligência. Profissionais de Inteligência são treinados a desenvolver capacidades variadas. No entanto, muitas vezes, eles não são ensinados a saber qual a forma mais adequada de pensar e raciocinar em relação a uma questão específica. Portanto, estão vulneráveis a cometer erros de pensamento oriundos de vieses cognitivos.

O presente artigo busca apresentar, de forma clara, prática e objetiva, os principais vieses cognitivos que afetam negativamente o trabalho do profissional de Inteligência e sugerir formas de mitigá-los. A importância dada ao tema de vieses cognitivos nos Estudos de Inteligência é crescente, especialmente nos Estados Unidos da América (EUA) e em países da União Europeia (UE), inclusive com financiamento oriundo das comunidades de Inteligência para pesquisas relacionadas ao tema nas universidades. Entretanto, na América do Sul, e especificamente no Brasil, o assunto ainda é pouco estudado de forma sistemática; há alguns trabalhos relevantes na área (AFONSO, 2009; AMBROS, 2011; MACHADO, 2018), mas ainda sem massa crítica suficiente. Nesse sentido, buscamos fomentar o debate e estimular outros trabalhos com esta temática, com o propósito de contribuir para o aprimoramento da qualidade analítica e operacional da Inteligência no Brasil.

Além de introdução e conclusão, este artigo contém três seções principais: a primeira discute o conceito de vieses cognitivos; a segunda apresenta os vieses cognitivos que mais afetam a Atividade de Inteligência; e a terceira debate as técnicas de análise estruturada, consideradas uma das possíveis formas para mitigar o impacto negativo dos vieses cognitivos na Inteligência.

Vieses Cognitivos

Vieses são erros sistemáticos no processamento da informação que se repetem de forma previsível em circunstâncias particulares (KAHNEMAN, 2011). Existem diversos tipos de vieses que impactam o processo mental do indivíduo, como vieses culturais, organizacionais, emocionais e automotivados. Vieses cognitivos são um tipo específico de viés. De acordo com Machado (2018), são erros de raciocínio causados por estratégias mentais de simplificação, geradas no esforço de processamento de informações. Trata-se do fenômeno da heurística intuitiva, atalhos mentais que simplificam procedimentos complexos que frequentemente acarretam erros de análise (KAHNEMAN, 2011).

Psicólogos evolucionistas demonstram que vieses cognitivos são uma adaptação biológica do cérebro humano para lidar com problemas específicos de forma ágil e eficiente em um ambiente informacional ambíguo e complexo (HASELTON *et alii*, 2016). Dessa forma, são atalhos mentais naturais e universais no cérebro humano, que agem automaticamente e inconscientemente, e, por isso, são consistentes e previsíveis. Embora esses atalhos cognitivos simplificadores muitas

vezes nos ajudem a lidar com a sobrecarga informacional de situações cotidianas e a garantir nossa capacidade de processamento em ambientes complexos sem sobrecarregar o nível consciente do cérebro, eles também criam armadilhas persistentes e erros sistemáticos de percepção e avaliação. É nesse sentido que Heuer (1999) aponta que "vieses cognitivos são similares a ilusões de ótica, pois o erro persiste mesmo quando se está completamente consciente de sua natureza". A consciência do viés, por si só, não produz uma percepção mais acurada. Portanto, devido a sua origem biológica, vieses cognitivos são inevitáveis e não são completamente superáveis. É possível, contudo, criar estratégias para mitigá-los.

O campo de pesquisa sobre vieses cognitivos iniciou-se na década de 1970, quando psicólogos começaram a estudar os erros no raciocínio humano que acreditavam ser consequência do uso de heurísticas. Amos Tversky e Daniel Kahneman foram os primeiros a estruturar os estudos existentes sobre o assunto em um programa de pesquisa sobre heurísticas e vieses, na obra seminal *The Psychology of Intuitive Judgment: Heuristics and Biases*, de 1982. Esses estudos tiveram grande influência em parte significativa da comunidade científica, com impactos não só na psicologia, mas também nos mais variados campos, como direito, medicina, economia, computação, ciência forense, ciência política e marketing. Foram a base, inclusive, para novas disciplinas, como a economia comportamental. Em 2002, Daniel Kahneman foi laureado com o Prêmio Nobel de Economia por suas contribuições basilares para a economia comportamental[4].

Diversas classificações e descrições dos tipos de vieses cognitivos podem ser encontradas na literatura especializada, que aborda especialmente os processos cognitivos nas tarefas de inferência, categorização, avaliação e comparação. O aumento das linhas de pesquisa que se dedicam aos vieses cognitivos gerou tanto o aumento dos modelos normativos para o estudo empírico dos vieses quanto a extensão do próprio conceito; logo, tornou-se muito difícil agregar numa mesma definição o fenômeno daquilo que frequentemente é classificado como um viés cognitivo (CaVERNI *et alii*, 1990). Tversky e Kahneman (1982) iniciaram o programa de pesquisa com aqueles vieses que afetam o julgamento probabilístico. Gingerenzer (1991) introduz a ideia das heurísticas rápidas e frugais, que são aprofundadas por Kahneman em "Rápido e Devagar: duas formas de pensar" (2011). Pohl (2004) categoriza os vieses cognitivos em três: de pensamento, de julgamento e de memória. Dessa forma, segundo Machado (2018, p. 3), os conceitos de vieses cognitivos têm em comum, independentemente da categoria em que se encontram, a "propriedade de impedir a ampliação da capacidade lógica de produzir julgamentos distantes do modelo mental a

4 Em 2011, Kahneman lançou o *best seller* "Rápido e Devagar: duas formas de pensar", em que explica o raciocínio intuitivo por meio de dois sistemas psicológicos que, muitas vezes, estão em conflito: o sistema 1, que opera automática e rapidamente, com pouco ou nenhum esforço e nenhuma percepção de controle voluntário, e que tem suas capacidades baseadas em habilidades instintivas e involuntárias; e o sistema 2, que opera em atividades mentais difíceis, exigindo atenção, escolha e concentração.

que o intelecto está habituado"[5].

Apesar das diferentes linhas de pesquisa e distintas conceitualizações e categorizações, existem heurísticas e vieses que são mais frequentemente abordados nos estudos das diferentes áreas. Entre eles, destacam-se o viés da representatividade; o do *status quo*; o de ancoragem e ajustamento; o da confirmação; o da disponibilidade; o de espelhamento de imagem; e o de atribuição.

O viés da representatividade (*representativeness heuristic*) é um atalho mental que permite que julgamentos sobre pessoas e eventos sejam feitos baseados em similaridades a um grupo ou evento particular conhecido, de acordo com esquemas mentais já internalizados no indivíduo, em uma lógica de categorização de atributos e inferência de julgamentos.

O viés do *status quo* está relacionado com a tendência dos indivíduos a preferirem manter seu estado atual, mesmo que uma alteração da situação pudesse proporcionar uma mudança positiva a ele. Assim, o viés do *status quo* está intimamente relacionado com o conceito de aversão a perdas. Dessa forma, esse viés estimula o indivíduo a permanecer no padrão de referência atual. Quando em processo de estimativa de probabilidades, tendemos a pressupor que a situação continuará como está.

O viés de ancoragem e ajustamento (*anchoring and adjustment*) envolve a seleção de um ponto inicial (a âncora) no processo mental, que geralmente é a primeira informação que se recebe ou alguma experiência individual anterior, e vai gradualmente ajustando as novas informações de forma a serem compatíveis com a âncora. Ainda que mais tarde se descubra que as evidências que constituem a âncora estavam incorretas, a tendência é que haja grande dificuldade de mudar o marco cognitivo inicial, e que se mantenha, inercial e involuntariamente, o enfoque inicial.

Similar ao processo de ancoragem, o viés de confirmação estimula ou induz o analista a levar fortemente em consideração as informações que são consistentes às suas expectativas e hipóteses iniciais e ignore ou subestime evidências que as contradizem. Por sua vez, em função da heurística da disponibilidade, informações que podem rapidamente ser trazidas à mente ganhem maior proeminência do que outras evidências igualmente ou até mesmo mais válidas. Ou seja, geralmente é dado mais peso às evidências recentes do que seria justificável.

Finalmente, outro mecanismo mental automático é o Espelhamento de Imagem (*Mirror Imaging*), que é a projeção do modelo mental, esquema ou sistemas de crenças de uma pessoa na outra. Ocorre quando uma pessoa completa lacunas nas informações ou nos conhecimentos de um indivíduo ao assumir que ele se comportará como ela mesma se comportaria em determinada circunstância. Também relacionado ao julgamento do comportamento alheio, o viés de atribuição diz respeito à tendência a supervalorizar os fatores internos e a subestimar o impacto de fatores externos quando tentamos explicar o comportamento de outras pessoas. No entanto, ao justificarmos nosso próprio comportamento,

5 Hallinan (2010, p.3) também afirma que "o importante é que esses efeitos ocorrem largamente fora da nossa consciência; somos enviesados – nós somente não sabemos disso. Algumas dessas tendências são tão fortes que até mesmo quando nós sabemos sobre elas, nós achamos difícil de corrigi-las".

inclinamo-nos a fazer o oposto, dando maior peso às causas externas.

Relacionado especificamente à abordagem de vieses cognitivos nos Estudos de Inteligência, destacamos as obras dos acadêmicos Robert Jervis (1976; 2006; 2010) e Richard Betts (2008; 2009a; 2009b) e dos praticantes Jack Davis (1992; 1995; 2006) e Richard Heuer (1999; 2011). O ponto fundamental desses trabalhos é identificar e amenizar as estratégias inerentes ao processamento de informações dos analistas de Inteligência, no intuito de aumentar a eficácia das análises e diminuir o risco de falhas de Inteligência. Afinal, a maior parte dos erros cometidos pela comunidade de Inteligência estadunidense durante a década de 1990 esteve relacionada ao estágio da análise (LOWENTHAL, 2006). Na próxima seção, analisaremos os vieses cognitivos mais recorrentes na Atividade de Inteligência, essencialmente, os da categorização de Heuer (1999).

Vieses cognitivos recorrentes na atividade de Inteligência

Na Atividade de Inteligência, os vieses cognitivos decorrem de simplificações cognitivas que o profissional de Inteligência comete involuntariamente ao processar informações. O ambiente em que ocorre a Atividade de Inteligência, cuja principal razão de existência é o processamento eficiente de informações complexas, tende a deixar os envolvidos mais vulneráveis a esses mecanismos cerebrais simplificadores devido às pressões contextuais, como incerteza, ambiguidade, estresse e rápidas mudanças de objetivos[6]. Portanto, é importante que o profissional de Inteligência conheça o funcionamento de seu próprio processo mental e esteja alerta para os erros que pode cometer ao desenvolver sua análise.

Psychology of Intelligence Analysis (1999), de Richard J. Heuer, é um trabalho pioneiro em que o ex-analista da CIA explica como os vieses cognitivos impactam a análise de Inteligência. Ele sugere que os vieses cognitivos mais recorrentes na Atividade de Inteligência podem ser classificados em quatro categorias: vieses na avaliação de evidências; vieses na percepção de relação causa-efeito; vieses no cálculo de probabilidades; e vieses na avaliação retrospectiva da análise de Inteligência.

Vieses na avaliação de evidências

Na avaliação de evidências, há cinco vieses cognitivos principais que podem afetar o trabalho do profissional de Inteligência. O primeiro é atribuir excessivo peso estatístico a experiências pessoais, a relatos de pessoas próximas e a informações concretas. Conforme afirma Jordán (2011), um caso concreto relatado ao analista, p. ex., tende a ter maior impacto no seu raciocínio do que um conjunto de dados estatísticos, que é mais informativo, mas também mais abstrato ao seu pensamento. Nesse sentido, eventos vivenciados pessoalmente costumam ter maior peso na análise do que aqueles sobre os quais o profissional de Inteligência apenas

6 De acordo com Davis (1992), "as características essenciais dos modelos mentais no trabalho de analistas da Inteligência encarregados de produzir estimativas são subscritas por quatro elementos prevalentes no ambiente da inteligência: a complexidade dos assuntos, a ambiguidade presente, as pressões de tempo e a pressão para predizer" (tradução nossa).

leu. Além disso, palavras concretas são mais facilmente memorizadas do que palavras abstratas, do mesmo modo que palavras são mais facilmente memorizadas do que números e estatísticas. Nesse caso, quando uma teoria abstrata ou uma informação de segunda mão contradiz uma experiência pessoal de observação de um caso concreto, a última tende a prevalecer perante a primeira na maioria das circunstâncias.

Esse tipo de viés cognitivo ocorre, p. ex., na Inteligência de análise de conjuntura internacional. Suponha-se que um analista responsável por acompanhar a conjuntura política da Bolívia visitou Santa Cruz de la Sierra. Nessa região do país, o poder político é majoritariamente dominado pela elite branca local, formada, em sua maioria, por descendentes de europeus. Esse profissional ainda não visitou regiões do Ocidente Boliviano, onde descendentes de indígenas compõem a maioria da população e dominam boa parte do poder político local. Em razão de ter vivenciado experiências pessoais em apenas uma região do país, sua análise pode ser enviesada. Como resultado, o analista pode sobrevalorizar o peso da elite branca na conjuntura política nacional e diminuir o real peso do poder político de descendentes indígenas no país, ainda que fontes secundárias consistentes contradigam essa análise.

O segundo viés dessa categoria é não valorizar a ausência de evidências. Uma das principais características da análise de Inteligência é que, frequentemente, faltam informações essenciais. Idealmente, os profissionais de Inteligência deveriam ser capazes de reconhecer quais evidências relevantes estão ausentes, levar isso em consideração na análise e verificar qual variável essas evidências ausentes afetariam e seu impacto na construção de cenários. Entretanto, conforme Jordán (2011), um viés comum é que a informação que está fora de nossa vista também estará fora de nossos cálculos.

Robert Jervis (2010), em sua análise da falha de Inteligência estadunidense sobre as Armas de Destruição em Massa (ADMs) no Iraque em 2002, mostra que a tendência a não se valorizar a ausência de evidências como uma variável relevante na equação analítica foi um erro crucial. Devido à dificuldade de sistematização e atribuição de valor às variáveis em eventos complexos, a tendência é concentrar a análise nas evidências visíveis que corroborem determinada fração de conhecimento de uma variável. Frequentemente, o profissional de Inteligência desconsidera a ausência de evidência que sustenta uma variável essencial para que, de fato, o evento complexo ocorra. Por natureza, evidências positivas são muito mais contundentes do que a ausência delas e, por isso, evidências negativas e fatos que não ocorreram tendem a ser subestimados.

Na Atividade de Inteligência, a ausência de evidências pode ser erroneamente atribuída a ações de Contrainteligência do adversário que visam a ocultar fatos. Jervis (2010, p. 139), tratando do caso das ADMs, afirma que:

> O problema era que as comunidades de Inteligência britânica e americana tratavam a decepção (*deception*) e a negação (*denial*) (de informações pela Inteligência iraquiana) como dadas e não como hipóteses a serem testadas, e elas nunca se perguntavam qual informação poderia indicar que as atividades de desenvolvimento de ADMs não ocorriam

> e não que estavam sendo escondidas (...) a ironia aqui é que os Estados Unidos e o Reino Unido enganaram (*deceived*) eles mesmos ao acreditar que o Iraque estava engajado em um amplo esquema de decepção (*deception*).

O terceiro viés recorrente na avaliação de evidências é atribuir excessiva confiança a amostras reduzidas. Conforme afirmam Tversky e Kahneman (1974), a tendência de sobrevalorizar a representatividade de amostras reduzidas pode ser chamada de "lei dos pequenos números". Essa nomenclatura é uma paródia à lei dos grandes números, princípio estatístico segundo o qual amostras grandes serão mais representativas do universo populacional investigado do que amostras reduzidas. O viés cognitivo, portanto, é atribuir a amostras reduzidas a representatividade de amostras grandes, ou seja, generalizar equivocadamente as conclusões extraídas de uma amostra pouco representativa.

Esse tipo de viés pode ocorrer, p. ex., na área de Contraterrorismo, quando um analista toma como válido que um indivíduo terrorista tem perfil de homem, muçulmano, jovem e em situação vulnerável. Embora esse perfil seja recorrente em alguns atentados terroristas, não pode ser generalizado para todo o universo de ataques.

O quarto viés dessa categoria é dar como certo o caráter pouco seguro de algumas informações. Ao processar informações de confiabilidade e precisão duvidosas, profissionais de Inteligência tendem a fazer simples escolhas de sim ou não, ao agregar ou não aquele dado à sua análise. Quando rejeitam o dado, tendem a descartá-lo por completo, de modo que não terá mais nenhuma influência. Quando aceitam o dado, tendem a aceitá-lo como certo e a ignorar a natureza probabilística da confiabilidade e da precisão da informação. Segundo Heuer (1999), é comum que profissionais de Inteligência utilizem a estratégia de "melhor chute", que simplifica a integração de informações probabilísticas, mas ao custo de ignorar algum nível de incerteza. Por exemplo, se um analista tem informação sobre a qual tem 70% de certeza, tende a integrá-la como se tivesse 100% de certeza, enquanto informações, p. ex., com 20% de certeza serão descartadas por completo.

O quinto viés cognitivo frequente na avaliação de evidências é deixar-se influenciar pela impressão persistente de evidência desacreditada. As primeiras informações recebidas tendem a orientar o rumo do trabalho de Inteligência. Mesmo após descobrir que essas informações eram incorretas, o rumo inicial tende a permanecer. Segundo Heuer (1999), impressões iniciais tendem a se manter mesmo após a evidência que as legitimou ter sido desacreditada por completo. Para Jordán (2011), um exemplo desse tipo de viés cognitivo ocorreu na crença cega de alguns profissionais de Inteligência dos EUA na informação proporcionada pela fonte "Curveball" sobre suposta existência de laboratórios móveis de fabricação de armas biológicas no Iraque antes da invasão estadunidense em 2003. Mesmo após outras fontes terem desmentido essa informação, ela continuou persistente e determinante nos rumos tomados pela Inteligência estadunidense.

Vieses na percepção de relação causa-efeito

Devido à necessidade de se tentar compreender fenômenos complexos de maneira ordenada e causal, profissionais de Inteligência tendem a encontrar relação de causa e efeito em eventos que, na verdade, são acidentais e aleatórios. A necessidade do cérebro humano de compreender os fenômenos por meio de histórias consistentes pode gerar vieses de congruência, que ocorrem quando o analista distorce dados e evidências para que se encaixem em sua narrativa. Existem seis tipos de vieses na percepção de relação causa-efeito.

O primeiro deles é atribuir relação causal a fenômenos aleatórios e acidentais. A base deste fenômeno está na falácia do jogador, viés que atribui peso irreal de eventos passados em acontecimentos futuros que não estão relacionados de maneira causal, como um apostador que acredita que ele não tirará o número um nos dados porque o tirou na última rodada. Para Heuer (1999), a busca excessiva por coerência na narrativa da atividade de Inteligência gera a tendência de favorecer explicações causais mesmo quando elas não existem. Para haver coerência, é necessário ordem. Desse modo, os profissionais de Inteligência procuram padrões e relações de causalidade entre os dados disponíveis. Se nenhum padrão é encontrado, o primeiro pensamento do profissional é que lhe falta algum dado essencial ao entendimento do fenômeno; ele dificilmente considera a possibilidade de estar lidando com fenômenos aleatórios, sem nenhuma relação causal entre si[7].

Feller (1968) exemplifica esse viés cognitivo em acontecimento da Segunda Guerra Mundial, quando britânicos supostamente identificaram explicações causais para o padrão de bombardeio feito por aviões alemães em Londres. Essas explicações, muitas vezes, guiaram decisões de cidadãos londrinos de onde morariam ou onde teriam refúgio em momentos de bombardeio aéreo na cidade. Estudos pós-guerra demonstraram, contudo, que os bombardeios da Luftwaffe sobre Londres tinham padrão aleatório.

O segundo viés dessa categoria é imaginar uma centralização inexistente. Conforme afirma Jervis (1976), as pessoas têm dificuldade para perceber coincidências, causas acidentais e consequências não-intencionais. Na verdade, elas têm a tendência de enxergar ações coordenadas, planos e conspirações como supostamente advindos de planejamento racional e centralizado, o que nem sempre é verdadeiro. Para Jordán (2011), esse viés é muito comum quando a Inteligência analisa a política externa de outros países e percebe os outros Estados como atores unitários com planejamento e decisões centralizados e racionais. Na realidade, múltiplos indivíduos, grupos e organizações da sociedade civil participam na elaboração de qualquer política, com interesses frequentemente contraditórios. O mesmo erro pode ocorrer

7 Langer (1977) afirma que as pessoas dificilmente aceitam a possibilidade de um evento ser causado por aleatoriedade ou acaso. Segundo esse autor, até jogadores de dado acreditam que eles têm algum controle sobre o resultado do dado a ser lançado. Na Inteligência, os profissionais tendem a encontrar relações causais que muitas vezes não existem. Nesses casos, a Inteligência está erroneamente considerando que eventos aleatórios de um processo estocástico seriam parte de um processo supostamente determinístico.

quando se analisa a conduta de atores não-estatais, grupos insurgentes, organizações terroristas e grupos criminais. Portanto, esse viés é recorrente em diversas áreas da Inteligência, como na análise internacional e no Contraterrorismo.

O terceiro viés dessa categoria é equiparar a magnitude de causa e efeito. Essas inferências frequentemente são corretas em relação a propriedades físicas, como em observações de que objetos grandes fazem grandes ruídos, ou animais grandes deixam grandes pegadas. Contudo, o mesmo tipo de pensamento causa erros em realidades mais complexas em que se correlacionam diversas variáveis, como a do trabalho de Inteligência. Grandes acontecimentos nem sempre resultam de grandes causas. Heuer (1999) afirma que esse tipo de viés pode ocorrer com frequência na área de Inteligência Econômica, em que o analista pode assumir, p. ex., que grandes acontecimentos econômicos necessariamente geram consequências de mesma magnitude. Nessa área, também é comum, segundo Heuer, que se considere que eventos econômicos derivam de causas primariamente econômicas. Para Jordán (2011), esse viés ocorre também na direção oposta, pois causas pequenas podem gerar grandes consequências. Esse autor usa como exemplo o fato de um indivíduo solitário e sem importância como Lee Harvey Oswald ter marcado a história ao assassinar o presidente Kennedy.

O quarto viés é o chamado erro fundamental de atribuição, que ocorre quando se atribui excessivo peso a causas internas, em detrimento de causas externas. É comum que profissionais de Inteligência sobrevalorizem fatores internos e subestimem fatores externos na conduta de um líder político, um governo ou um ator não-estatal. Para além das características e intenções inerentes a cada indivíduo, deve-se considerar que os agentes atuam sempre dentro de algum contexto, o qual influencia sua conduta. Para Jordán (2011), um bom exemplo desse viés ocorre quando não se leva em conta os fatores que motivam o dilema de segurança[8].

O quinto viés dessa categoria é exagerar nossa própria capacidade de influenciar decisão alheia. Indivíduos e governos tendem a superestimar sua capacidade de influenciar comportamentos e decisões de outros atores. Para Heuer (1999), isso ocorre porque a própria pessoa sabe os esforços que fez para influenciar os outros indivíduos, mas é muito menos informada sobre outras variáveis que influenciaram a decisão alheia. Nesse sentido, profissionais de Inteligência tendem a superestimar a influência que o governo de seu país exerce sobre outras nações. Heuer (1999) mostra que esse viés gerou, p. ex., a falha da Inteligência dos EUA ao não anteciparem os testes nucleares da Índia na segunda metade da década de 1990. O novo governo indiano havia sido eleito com promessas de aumentar o arsenal nuclear do país. Contudo, para a maioria dos analistas de Inteligência dos EUA, essas promessas eram retóricas de campanha e,

8 No clássico dilema proposto por Herz (1950), a ocorrência de corridas armamentistas poderia ser explicada por fatores externos aos indivíduos. Ela ocorreria quando determinado ator, ao buscar melhorar sua capacidade bélica para ter maior segurança, faz com que seus vizinhos se sintam ameaçados e respondam aumentando suas defesas. Isto faria com que o primeiro interpretasse que estão aumentando seu estoque de armamento para atacá-lo e o faria investir ainda mais em sua capacidade bélica. Este ciclo, em última instância, geraria uma corrida armamentista.

por meio de pressão diplomática e ameaça de sanções econômicas, a Índia seria dissuadida da ideia de desenvolver armas nucleares. Os testes nucleares indianos mostraram que, na verdade, os analistas de Inteligência dos EUA superestimarem a capacidade de seu país de influenciar as decisões do país asiático.

O sexto viés refere-se às correlações ilusórias[9]. Esse viés ocorre quando o profissional de Inteligência percebe uma relação entre dois acontecimentos que, na verdade, não têm relação alguma. Ao analisar uma série de dados, os profissionais tendem a focar sua atenção em frações que sustentem a existência da relação, mas ignoram casos que mostram a não-existência dessa relação. Dessa forma, eles tendem a aplicar viés de confirmação para enxergar uma correlação que não existe. Consequentemente, essa correlação ilusória acarreta percepção incorreta de relação de causa e efeito e erro de análise.

Inúmeros experimentos já demonstraram que as pessoas não têm uma boa compreensão intuitiva de quais informações são realmente necessárias para comprovar uma correlação entre dois eventos ou duas variáveis. Conforme demonstra Jordán (2011), a ocorrência simultânea de dois fenômenos não significa que exista relação direta entre os dois acontecimentos, ou seja, a existência de simultaneidade não significa, necessariamente, existência de correlação.

Vieses no cálculo de probabilidades

Ao estimarem probabilidades, profissionais de Inteligência tendem a utilizar atalhos cognitivos que diminuem a complexidade do cálculo. No entanto, essas estratégias de simplificação do pensamento causam erros previsíveis e levam a probabilidades incorretas. Há cinco vieses frequentes nessa categoria.

O primeiro deles é julgar a probabilidade de um evento ocorrer com base na facilidade de se imaginar situações plausíveis em que esse evento ocorra ou de se lembrar do número de vezes em que ele já ocorreu. Para Kahneman (2011), essa confiança excessiva na facilidade em puxar da memória pode ser chamada de heurística da disponibilidade. Segundo Heuer (1999), a facilidade com que as lembranças vêm à mente é influenciada, muitas vezes, por fatores que não estão relacionados à probabilidade de o evento ocorrer, mais sim com o quão recente é o evento, se houve envolvimento pessoal do profissional de Inteligência, se o evento teve detalhes concretos mais facilmente recordáveis e quão importante ele foi à época em que ocorreu. Heuer afirma que esse viés ocorreu na Inteligência dos EUA pouco antes da entrada do país na Guerra do Vietnã. Ao imaginar os diversos cenários do que poderia acontecer com o envolvimento ou não de tropas estadunidenses no conflito, a Inteligência do país foi fortemente influenciada por dois acontecimentos até então recentes e que estavam bastante vivos na memória: a falha da política de apaziguamento no início da Segunda Guerra Mundial e o sucesso da intervenção na Guerra da Coreia.

O segundo viés dessa categoria é a ancoragem, que consiste no peso excessivo

9 Para mais sobre correlações ilusórias, ver Fiedler (in Pohl, 2004, p. 97).

das análises iniciais sobre a análise final. Segundo Heuer (1999), novas informações promovem um ajuste insuficiente da análise inicial, que tende a ancorar as demais análises. Para Jordán (2011), um exemplo desse viés acontece quando uma primeira análise de Inteligência fixa uma probabilidade e as seguintes modificações tendem a ancorar-se nesse ponto de partida. Por exemplo, se a probabilidade estabelecida inicialmente foi alta, as demais tendem a se manter em patamares elevados, mesmo com a adição de novas informações; se a probabilidade inicial foi baixa, as seguintes também tendem a ser consideradas baixas. Esse viés pode ocorrer em quase todas as áreas de Inteligência que trabalham com estimativas. Se, p. ex., inicia-se um novo trabalho com o pressuposto de que é alta a probabilidade de um líder estrangeiro ser deposto, mesmo que se encontrem evidências claras de que a probabilidade é baixa, o que ocorrerá será um ajustamento à âncora inicial da probabilidade alta que gerará uma estimativa mais alarmista do que as evidências realmente apontam.

O terceiro viés consiste no uso de expressões imprecisas e ambíguas para mostrar a probabilidade de um evento. Há duas formas de se expressar probabilidade, uma objetiva, com números, e outra subjetiva, com palavras. A forma subjetiva, com expressões como "possível", "provável" e "pouco provável", comumente gera interpretações incorretas. Isso ocorre porque as pessoas tendem a ver o que elas já esperavam ver, de modo que novas informações são assimiladas para se moldarem a crenças previamente estabelecidas. Isso é ainda mais forte na leitura de expressões subjetivas de probabilidade. Dessa forma, quando conclusões de Inteligência são expressas em termos imprecisos, a interpretação do leitor será enviesada em favor daquilo em que ele já acreditava antes. Segundo Heuer (1999), essa é uma das razões que levam alguns decisores a acreditarem que eles pouco aprendem com relatórios de Inteligência. Sherman Kent, o primeiro diretor do Escritório de Estimativas Nacionais da CIA, exemplificou esse viés em um experimento com 23 oficiais militares que tinham hábito de ler relatórios de Inteligência. No experimento, os oficiais tinham de ler um mesmo relatório de Inteligência e transformar expressões subjetivas de probabilidade em probabilidade numérica, que pode variar de 0% a 100%. A expressão "provável" foi classificada de forma bastante diferente pelos distintos leitores, variando entre 20% e 90%, o que demonstra o quão diversa pode ser a interpretação feita por cada leitor em relação a expressões subjetivas de probabilidade[10].

O quarto viés dessa categoria é calcular incorretamente a probabilidade de cenários. É a chamada falácia da conjunção[11], que ocorre quando não considera o caráter cumulativo da improbabilidade. Um cenário consiste em uma série de eventos interligados em uma narrativa descritiva. Dessa forma, para calcular corretamente a probabilidade de um cenário, deve-se multiplicar a probabilidade de cada evento individual. Contudo, segundo Jordán (2011), alguns profissionais enviesam sua análise ao usar uma média das probabilidades de

10 Sherman Kent, "Words of Estimated Probability", in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994).

11 Para mais sobre a falácia da conjunção, ver Tversky e Kahneman (IN Gilovich *et alii* 2002, p. 19-49).

cada evento para determinar a suposta probabilidade do cenário. Por exemplo, em um cenário previsível determinado por três eventos interligados com probabilidade de 70% para cada evento, é comum que alguns profissionais digam que o cenário tem 70% de chance de ocorrer, pois essa é a média entre as probabilidades dos três eventos. No entanto, o cálculo correto seria calcular a probabilidade composta dos três eventos (0,7 x 0,7 x 0,7 = 0,24), o que daria uma probabilidade baixa, de apenas 24%, para ocorrência do cenário.

O quinto viés consiste em desvalorizar probabilidades anteriores. Ao analisar um caso, um profissional de Inteligência geralmente trabalha com dois tipos de dados: específicos, que tratam do caso em análise, e genéricos, que resumem informações sobre diversos casos similares. Esse viés ocorre porque há tendência de que os dados específicos do caso sejam sobrevalorizados, e de que os dados genéricos sobre casos similares sejam ignorados.

Vieses na avaliação retrospectiva da análise de Inteligência

Três tipos de vieses sistemáticos costumam distorcer a avaliação baseada numa análise de Inteligência já concluída. Esses vieses têm em comum o fato de serem avaliações retrospectivas, que são beneficiadas pelo conhecimento prévio sobre o curso dos acontecimentos. Nesse sentido, fatores que antes eram considerados relevantes podem se tornar irrelevantes na análise retrospectiva, e fatores anteriormente considerados pouco relevantes podem se tornar determinantes. Para Heuer (1999), uma vez que a mente é reestruturada após absorver nova informação, é praticamente impossível reconstruir o estado de mente preexistente. Saber as consequências de uma situação já concluída torna mais difícil imaginar outros possíveis resultados que poderiam ter ocorrido.

O primeiro viés dessa categoria é a tendência de superestimar previsões de análises pretéritas. Quando eventos inesperados acontecem, analistas tendem a superestimar a expectativa que tinham de que esses eventos ocorreriam. Dessa forma, esses eventos parecem menos surpreendentes do que deveriam parecer e os analistas ficam menos surpresos do que deveriam estar com o desenrolar dos acontecimentos. Teovanovic *et alii* (2015) afirma que o viés de retrospectiva (*hindsight bias*) é geralmente apontado como uma consequência do processamento de informação e da memória difícil de evitar. A informação do resultado do evento muda irreversivelmente a representação do conhecimento, ou serve como uma âncora quando se tenta reconstruir estimativas esquecidas.

O segundo viés dessa categoria é a tendência de um decisor subestimar o quanto ele aprendeu após ter lido um relatório de Inteligência. As pessoas tendem a subestimar os aprendizados assimilados após a leitura de novas informações, de forma que pensam "eu já sabia disso". Na medida em que decisores que leem relatórios de Inteligência também manifestem esse viés, eles igualmente tenderão a subestimar o quanto aprenderam com o relatório lido. Este viés torna ainda mais difícil a relação entre a comunidade política e a comunidade de Inteligência. Logo, oficiais

de Inteligência estariam frequentemente envolvidos em disputas para justificar sua imprescindibilidade no processo de tomada de decisão[12].

O terceiro viés se dá com supervisores ou órgãos de controle que analisam falhas de Inteligência já ocorridas. Essas avaliações, feitas *a posteriori*, podem ser conduzidas, p. ex., pelo Congresso Nacional ou pelos próprios membros da comunidade de Inteligência. Algumas avaliações podem concluir que os eventos que ocorreram eram mais previsíveis do que realmente o eram, uma vez que essas análises se favorecem por serem retrospectivas. Segundo Heuer (1999), ao tentar reconstruir o passado, há forte tendência determinista sobre a inevitabilidade de um evento e sobre a previsibilidade das circunstâncias que levaram a esse evento. Nesse sentido, tende-se a julgar que analistas de Inteligência deveriam ter previsto certos fatos, mas, na verdade, em muitas ocasiões, esses fatos eram imprevisíveis em vista das informações disponíveis à época.

Há distintas maneiras de se tentar mitigar os vieses cognitivos dessas quatro categorias apresentadas acima. Uma dessas formas é a aplicação de ferramentas assessórias, p. ex., técnicas de análise estruturada. A utilização dessas técnicas auxilia analistas a lidarem com problemas perenes na atividade de Inteligência, como a complexidade dos fenômenos, as informações incompletas e ambíguas e as limitações inerentes da mente humana (US GOVERNMENT, 2009). Por isso, a próxima seção é dedicada a demonstrar os potenciais das técnicas estruturadas para a análise de Inteligência.

Técnicas de análise estruturada: formas de mitigar o impacto de vieses cognitivos na atividade de Inteligência

Desde a falha de Inteligência estadunidense no caso das armas de destruição em massa do Iraque em 2003, o debate sobre novos meios organizacionais para o compartilhamento de informações e métodos analíticos para mitigar vieses ganhou força (MARRIN, 2007). O *Intelligence Reform and Terrorism Prevention Act* (2004) nos EUA ordenou que a comunidade de Inteligência iniciasse um processo de revisão de seus métodos analíticos, para que enfatizassem a utilização de técnicas estruturadas (COULTHART, 2016). Desde então, a atividade de análise na comunidade de Inteligência estadunidense está em estágio de transformação de um modelo em que o analista processava individualmente a informação, de uma maneira intuitiva, para outro em que se incentiva a colaboração em grupo durante o processo analítico.

As motivações para essa mudança de paradigma na análise, segundo Heuer e Pherson (2011, p. 3), incluem: i) crescente complexidade nos assuntos internacionais e as exigências para subsídios informacionais multidisciplinares para grande parte dos produtos de análise; ii) a necessidade de compartilhar informações mais rapidamente através das divisões organizacionais; iii) a dispersão de *expertise*, especialmente devido à progressiva dificuldade em estabelecer

12 Sobre a relação entre a comunidade de Inteligência e a comunidade política, ver George e Bruce (2008, p. 71-91).

divisões entre analistas, coletores e operações; e iv) a necessidade de identificar e avaliar a validade de modelos mentais alternativos. Devido a essa mudança, "a comunidade de Inteligência passou a enfatizar fortemente o uso de técnicas de análise estruturada (*Structured Analytic Techniques – SATs*) para promover análises mais rigorosas, diminuir os riscos de falhas de Inteligência e fazer com que o raciocínio dos analistas seja mais transparente para os consumidores" (Artner *et alii*, 2017, p. 1).

As SATs são uma categoria entre diversas outras ferramentas de métodos analíticos aplicáveis à análise de Inteligência. Pesquisadores dos Estudos de Inteligência descrevem uma série de abordagens para os métodos de análise, dividindo-os frequentemente de forma binária (métodos qualitativos vs. quantitativos; dedutivos vs. indutivos; intuitivos vs. científicos) e trinária (intuitivo, estruturado e científico; intuitivo, estruturado e sistemático) (CLARK, 2007; KHALSA, 2009). É grande o debate entre as vantagens e desvantagens de cada um dos métodos na comunidade de Inteligência. Críticos dos métodos estruturados apontam que eles não dão conta dos reais problemas de Inteligência, que são complexos e com um infinito número de variáveis que consumiriam muito tempo para serem processadas por técnicas estruturadas. Críticos da abordagem intuitiva sustentam que esse tipo de método resulta sistematicamente em falhas analíticas e vieses cognitivos já comprovados empiricamente[13]. Enquanto aqueles imaginam a Inteligência como arte, estes vêem a Inteligência como ciência.

Heuer e Pherson (2011) sugerem uma taxonomia dividida em quatro categorias: i) julgamento especializado; ii) métodos quantitativos que utilizam dados qualitativos; iii) métodos quantitativos que utilizam dados empíricos; e iv) técnicas estruturadas. O julgamento especializado é o método tradicional com que a maior parte das análises de Inteligência é feita. Nele, o analista combina especialidade em determinado assunto com pensamento crítico e, muitas vezes, utiliza raciocínio baseado em evidências, métodos históricos, estudos de caso e raciocínio por analogia[14]. Os métodos quantitativos que utilizam dados qualitativos procuram quantificar os dados que advém do julgamento especializado, e utilizam principalmente, métodos de inferência bayesiana, modelagem dinâmica e simulação. Os métodos quantitativos com dados empíricos são utilizados para processar uma ampla gama de dados coletados de diversas formas e por diversos tipos de sensores, e são cada vez mais empregados por meio de análise de *Big Data*. Finalmente, as técnicas

13 Ver Sundri Khalsa (2009) e Stephen Marrin (2007).

14 Segundo Randy Pherson, ex-analista da Agência Central de Inteligência (CIA) e professor de métodos de análise, em relato descrito por Marrin (2007, p. 9) para explicar a abordagem intuitiva, ou julgamento especializado, "o método tradicional de análise da CIA envolve três fases: ler o tanto quanto você tem tempo para ler sobre o assunto no dia; pensar sobre o assunto e tirar uma resposta da cartola (*suck an aswer out your thumb*); escrever da maneira mais precisa possível (...) infelizmente, na CIA a maior parte da nossa energia e treinamento como analistas tradicionalmente foca na terceira fase – aprender como capturar a essência da nossa análise em um parágrafo ou página. Muitos recursos também foram destinados à primeira fase, mas nós continuamos lamentavelmente atrasados em relação ao que a tecnologia oferece. E, até recentemente, nós havíamos ignorado a necessidade (ou usado a desculpa de que nós não temos tempo) de desenvolver as habilidades necessárias para garantir mais rigor e método científico ao nosso processo analítico".

estruturadas são métodos de organizar e estimular o pensamento sobre problemas de Inteligência. Por meio delas, os processos mentais de raciocínio são externalizados de modo sistemático e possibilitam que sejam compartilhados, desenvolvidos em conjunto e facilmente verificáveis pelos outros. Nenhum desses métodos é melhor ou mais efetivo do que o outro. Todos são necessários em determinadas circunstâncias para aumentar as chances de se alcançar uma resposta apropriada a um problema. O uso de múltiplos métodos durante o desenvolvimento de uma análise de Inteligência deveria ser a norma, e não a exceção (HEUER e PHERSON, 2011, p. 23).

Os métodos estruturados têm por objetivo tornar o processo analítico mais consciente e transparente, e reduzir a probabilidade de erros que passam despercebidos em análises intuitivas. É possível identificar três dimensões principais em que as SATs impactam a função da análise de Inteligência: i) a individual, por meio da mitigação de determinados vieses cognitivos; ii) a organizacional, pois viabiliza maior colaboração entre analistas e influencia os processos da organização; e iii) a gerencial, devido à possibilidade de se avaliar o processo analítico de forma mais completa e integrada, e não somente o produto final da análise.

As SATs proveem ao analista uma orientação clara, passo-a-passo, para conduzir a análise dos problemas de Inteligência. A estruturação do processo analítico ajuda o profissional a tornar-se mais consciente de seus vieses cognitivos e a mitigá-los na medida do possível, o que reduz a subjetividade e aumenta o rigor e a transparência da análise (ARTNER *et alii*, 2017, p. 2). Heuer (1999) aponta que "ferramentas mentais (...) auxiliam o analista a manter a mente aberta, questionar suas suposições, ver diferentes perspectivas, desenvolver novas ideias e reconhecer quando é o momento de mudar seu pensamento" (HEUER, 1999, p. 65). Nesse sentido, as SATs são especificamente endereçadas para lidar com vieses cognitivos que são associados a falhas de Inteligência, como o viés de confirmação e o viés do *status quo* (ARTNER *et alii*, 2017, p. 3).

As técnicas estruturadas são o processo analítico pelo qual a viabilidade de colaboração se torna mais efetiva (HEUER, 2009). Elas têm sido frequentemente usadas em equipes colaborativas, em que cada passo do processo analítico expõe os analistas a perspectivas divergentes ou conflitantes (HEUER & PHERSON, 2011, p. 4). Dessa maneira, a transparência do processo ajuda a garantir que diferentes opiniões entre os analistas sejam ouvidas e seriamente consideradas, o que evita o pensamento de grupo e o fechamento cognitivo prematuro.

Cada técnica estruturada deixa rastros de seu processo, de forma que outros analistas e gerentes consigam avaliar as bases para o resultado analítico e aumentar o *accountability* da análise. Conforme aponta Stephen Marrin (2007), com uma auditoria do processo analítico, gerentes e analistas podem descobrir as origens dos erros e avaliar a utilização de novos métodos de análise ou novas aplicações para técnicas já utilizadas. Além disso, ao focar a avaliação gerencial mais no processo do que no produto final, novas métricas podem ser implementadas para mensurar a eficiência, a efetividade e

a eficácia da organização. Nesse sentido, o uso de SATs torna possível o avanço geral da análise de Inteligência, tanto no escopo metodológico quanto no gerencial, por meio da avaliação sistemática de acertos e erros.

Os métodos estruturados são chamados de "técnicas" porque geralmente guiam o analista mais a pensar sobre o problema do que a provê-lo com uma resposta definitiva, como se esperaria de uma metodologia. Por isso, o argumento de que as técnicas de análise estruturada engessariam demasiadamente o processo analítico e eliminariam o julgamento intuitivo do analista e seus *insights* é limitado[15]. As técnicas estruturadas são ferramentas aplicáveis ao processo de análise que não trazem respostas por si só. Em verdade, elas podem auxiliar o bom analista a ter mais *insights* e o analista mediano a fazer melhores análises. Conforme Heuer (1999, p. 82), "aprender técnicas de resolução criativa de problemas não impacta nos talentos naturais do analista, mas sim o ajuda a atingir seu potencial completo. A maior parte das pessoas tem a capacidade de ser mais inovativas do que elas imaginam" (sic).

De acordo com um guia não-classificado do governo estadunidense para a atividade de análise (EUA, 2009), as SATs podem ser classificadas em três categorias amplas: *técnicas diagnósticas*, que objetivam fazer com que as suposições e argumentos lógicos sejam mais transparentes; *técnicas de contradição*, que desafiam o pensamento corrente; e *técnicas de pensamento imaginativo*, que encorajam novas perspectivas, *insights* e cenários alternativos. Os passos metodológicos para a aplicação de cada técnica estruturada apontada podem ser encontrados no livro *Structured Analytic Techniques for Intelligence Analysis*, de Heuer e Pherson (2014). Abaixo, trazemos uma tabela (baseada em CHANG *et alii*, 2017) que sistematiza algumas das principais técnicas estruturadas, classificadas de acordo com a nomenclatura do documento oficial mencionado acima, e que aponta os vieses cognitivos que elas objetivam mitigar.

15 Para mais informações sobre o debate entre intuição e técnicas estruturadas, ver Khalsa (2009).

Quadro 1: Técnicas de Análise Estruturada e Vieses Cognitivos

TÉCNICA	CATEGORIA	DESCRIÇÃO	VIÉS COGNITIVO
Checagem de Suposições Chave	Técnicas Diagnósticas	Listar e revisar as suposições nas quais o argumento principal se fundamenta.	Viés do *Status quo*; viés de confirmação; viés da ancoragem; erro de atribuição.
Qualidade na verificação de informações	Técnicas Diagnósticas	Avaliar a integridade, a completude e a solidez das fontes de informação disponíveis.	Viés do *Status quo*; viés de confirmação.
Indicadores e marcadores de mudança	Técnicas Diagnósticas	Periodicamente, revisar tendências observáveis para rastrear eventos, monitorar alvos e perceber mudanças.	Viés do *Status quo*; Ancoragem e ajustamento.
Análise de Hipóteses Competitivas (AHC)	Técnicas Diagnósticas	Identificar explicações alternativas e avaliar evidências suportadas em hipóteses.	Viés do *Status quo*; viés da confirmação; erros de atribuição; viés da congruência; ancoragem e ajustamento; viés da disponibilidade
Advogado do Diabo	Técnicas de contradição	Desafiar consenso por meio da construção de casos robustos alternativos.	Viés do *Status quo*; viés da confirmação.
Time A/ Time B	Técnicas de contradição	Usar times analíticos separados que tenham visões contrastantes.	Viés do *Status quo*; viés da confirmação.
Análises alto-impacto/ baixo-impacto	Técnicas de contradição	Evidenciar eventos altamente improváveis com alto potencial de impacto.	Viés do *Status quo*
Análise "E se?"	Técnicas de contradição	Assumir que eventos de alto impacto ocorreram e explicar o porquê.	Viés do *Status quo*; viés da confirmação.
Brainstorming estruturado	Técnicas de pensamento imaginativo	Usar processo estruturado de discussão em grupo usado para gerar novas ideias e conceitos.	Viés do *Status quo*
Dentro e fora do pensamento	Técnicas de pensamento imaginativo	Identificar forças básicas e tendências que poderiam impactar em um tópico.	Viés do *Status quo*
Análise da Equipe Vermelha	Técnicas de pensamento imaginativo	Tentar replicar como um adversário estaria pensando sobre um tópico.	Viés de confirmação; erro de atribuição; espelhamento de imagem.
Análise de futuros alternativos	Técnicas de pensamento imaginativo	Explorar os múltiplos caminhos como uma situação incerta pode se desenvolver.	Viés do *Status quo*

As técnicas mais utilizadas pela comunidade de Inteligência estadunidense, segundo estudo promovido pela Rand Corporation para avaliar a efetividade dos métodos estruturados (ARTNER *et alii*, 2017), são: i) o *brainstorming* estruturado; ii) a checagem de suposições chave; iii) os indicadores; e iv) a análise de hipóteses competitivas.

O *brainstorming* estruturado é um processo em grupo que segue regras e procedimentos específicos, ao mesmo tempo que promove a flexibilidade na discussão para gerar novas ideias. É geralmente utilizado no começo da análise para identificar a lista de variáveis relevantes, forças motrizes, hipóteses, atores chaves, fontes de informação e potenciais resultados e cenários. O método contribui ainda mais quando combinado a mecanismos como plataformas *wiki* que permitam que os analistas registrem os resultados do *brainstorming* de forma colaborativa.

A checagem de suposições-chaves é uma das técnicas mais utilizadas, pois a análise frequentemente é baseada na combinação entre evidência e suposições que influenciam como estas serão interpretadas. Suposições são necessárias e inevitáveis, pois são uma forma de preencher as lacunas de um quadro de informações incompleto, ambíguo e, muitas vezes, distorcido pela Inteligência adversa. Elas são parte do modelo mental do analista, criado por meio de sua educação, seu treinamento, sua cultura, sua experiência e contexto organizacional em que está inserido. Nesse sentido, a checagem de suposições-chaves é um esforço sistemático para tornar explícitas as suposições envolvidas na interpretação das evidências e questionar sua validade.

Os indicadores são fenômenos observáveis que podem ser revisados periodicamente para auxiliar a rastrear eventos, identificar tendências emergentes e alertar sobre mudanças potenciais. Criar uma lista de indicadores trata-se de pré-estabelecer ações, condições, fatos e eventos observáveis ou potencialmente observáveis cuja ocorrência simultânea indicaria que um fenômeno está ocorrendo ou que muito provavelmente ocorrerá. Indicadores podem ser monitorados para se obter alertas táticos, operacionais e estratégicos sobre algum desenvolvimento futuro que, se ocorresse, teria grande impacto (HEUER e PHERSON, 2011).

Finalmente, a Análise de Hipóteses Competitivas (AHC) é a técnica que originou todo o debate sobre técnicas estruturadas, a partir dos trabalhos de Richard J. Heuer na Divisão de Metodologia Analítica da CIA na década de 1970 (HEUER, 2009). A AHC é uma técnica que envolve identificar uma série de explicações ou resultados (apresentados como hipóteses) mutuamente excludentes, e avaliar a consistência ou inconsistência de cada fração de evidência para cada hipótese alternativa. O objetivo da técnica é mais refutar do que confirmar hipóteses; a hipótese mais provável é aquela com menos evidências contra si, assim como mais evidências a seu favor. A AHC pode ser feita manualmente, mas o uso de *softwares* é fortemente recomendado. Aplicar essa técnica digitalmente reduz o tempo necessário para trabalhar os dados e torna possível a categorização das evidências por seu poder explicativo, sua confiabilidade e sua oportunidade (HEUER e PHERSON, 2011).

Os sistemas de Inteligência de uma série de

países vêm aumentando significativamente a utilização de técnicas estruturadas na última década, o que envolve, inclusive, a cooperação com universidades e empresas para aprimoramento dos métodos. Nos EUA, conforme colocam Artner, Girven e Bruce (2017), a CIA tem promovido contundentemente os formatos de análises estruturadas, que incluem a geração sistemática de hipóteses e a rigorosa revisão de suposições. A Agência de Inteligência de Defesa (DIA) tem treinado seus novos analistas em quatro técnicas estruturadas principais e tem usado várias técnicas em seus produtos finais. A Inteligência do Corpo de Fuzileiros Navais dos EUA, em colaboração com a Rand Corporation, tem desenvolvido um leque de 28 modelos e abordagens que aplicam análises estruturadas a situações táticas no campo de batalha. O Escritório do Diretor de Inteligência Nacional dos EUA (ODNI) promove treinamentos em pensamento crítico e SATs para analistas de várias agências da comunidade de Inteligência, e, na Estratégia Nacional de Inteligência de 2014, apontou que a Inteligência estadunidense deveria reforçar a utilização de métodos analíticos que desafiassem suposições tradicionais e encorajassem novas perspectivas. Nos países europeus, a pesquisa sobre vieses cognitivos e técnicas estruturadas vem avançando. O Projeto REduction of COgnitive BIAses in Intelligence Analysis (RECOBIA)[16], financiado pela União Europeia e coordenado pela Companhia Europeia de Inteligência Estratégica, foi desenvolvido de 2012 a 2015. O principal objetivo do projeto era reduzir o impacto negativo dos 47 vieses cognitivos identificados como os que mais afetam a atividade de Inteligência. Uma das sugestões do projeto foi o uso de análises estruturadas. Ainda que o otimismo em relação às SATs seja geralmente elevado, essas experiências internacionais reconhecem que é necessário avançar na avaliação de resultados do uso das técnicas estruturadas (ARTNER *et alii*, 2017).

No Brasil, ainda que a discussão seja bastante incipiente[17], é possível verificar algumas iniciativas pontuais na comunidade de Inteligência. Segundo Coelho (2017), a Escola de Inteligência (Esint/ABIN), que é responsável pelo ensino de Inteligência e Contrainteligência para os servidores da ABIN e dos demais órgãos do Sistema Brasileiro de Inteligência (SISBIN), busca aprimoramento contínuo de uma metodologia de produção do conhecimento com o ensino de técnicas acessórias de análises estruturadas. Da mesma forma, o Instituto Sagres já ofereceu, para o Subsistema de Inteligência em Segurança Pública (SISP), cursos específicos em análise de Inteligência e técnicas estruturadas[18]. Para aperfeiçoar a Atividade de Inteligência no Brasil, é necessário avançar mais tanto na pesquisa quanto no treinamento em técnicas de análise estruturada. A Esint deveria ser protagonista nesse processo, não só ao avançar no estudo dos métodos e na propagação das técnicas por meio de cursos ao SISBIN, mas também ao promover a discussão na comunidade acadêmica nacional.

16 Disponível em https://www.recobia.eu/about. Acesso em 11 de julho de 2019.

17 Poucos são os estudos sobre a temática de vieses cognitivos na Inteligência, como Ambros (2011) e Machado (2018).

18 Disponível em http://sagres.org.br/curso-de-analise-de-inteligencia-em-seguranca-publica/. Acesso a 12 de julho de 2019.

Conclusão

A incerteza e a complexidade característica de coleta, análise, disseminação e ação na atividade de Inteligência deixa os seus praticantes mais suscetíveis a desvios e erros na interpretação das informações. "As conseqüências de erros nessas operações podem variar desde a mera ineficiência no uso do dinheiro do contribuinte, até a perda de vidas pela falha em identificar e prevenir ataques terroristas" (KEBBEL & MULLER & MARTIN, 2010:95). No ambiente complexo da Inteligência, os vieses cognitivos são um dos tipos de erro de mais difícil detecção e prevenção.

A diminuição das probabilidades de ocorrência de vieses cognitivos é um esforço que tem reunido muitos especialistas em análise de Inteligência, principalmente nas comunidades de Inteligência estadunidense e europeia. Tenta-se desenvolver métodos de análise que os neutralizem ou, ao menos, restrinjam a poucas situações. Nesse sentido é que se inicia o estudo das técnicas de análise estruturada, com o objetivo de mitigar vieses cognitivos, e tornar o processo analítico mais transparente, sistemático e avaliável pelos pares dos analistas, pelos gerentes de unidades e, em último caso, pelos tomadores de decisão.

Todas essas técnicas encontram limites claros quanto ao sucesso de seu objetivo principal, isto é, de sempre produzir análises precisas, na medida em que os vieses cognitivos, muitas vezes, passam despercebidos até mesmo pelo controle do revisor mais atento. Isso acontece porque os vieses cognitivos fazem parte do modo natural como os seres humanos processam informações. Além disso, as crescentes demandas dos sistemas de Inteligência por análises cada vez mais apuradas em curto tempo encontra limites de recursos e de tempo, o que pode aumentar as possibilidades de vieses cognitivos.

Mesmo assim, apesar dos desafios e limitações que o tema suscita, é necessário avançar nos esforços de evitar falhas nas análises de Inteligência causadas por vieses cognitivos. Com esse intuito, o presente artigo se propôs a contribuir com os poucos estudos no Brasil sobre como vieses cognitivos impactam na Atividade de Inteligência (AFONSO, 2009; AMBROS, 2011; MACHADO, 2018). No âmbito da Inteligência brasileira, é importante não só aprofundar o entendimento sobre a temática dos vieses cognitivos e como eles ocorrem nas situações mais recorrentemente enfrentadas pelos órgãos do SISBIN, mas também encontrar formas de incorporar novos processos organizacionais às doutrinas e novas técnicas analíticas na formação profissional que visem a mitigar as armadilhas cognitivas. Em ambos os aspectos, é fundamental que haja ações integradas entre a comunidade de Inteligência e a Academia, por meio do aperfeiçoamento da relação entre a Esint e as universidades brasileiras, o que aprofunda o debate e as linhas de pesquisa conjuntas sobre vieses cognitivos. Posteriormente, devido ao papel central da ABIN na Inteligência Estratégica e à ampla experiência nacional e internacional da Esint em cursos e treinamentos, a Esint, ao investir na temática de vieses e técnicas estruturadas, pode se tornar um polo irradiador de métodos para o aprimoramento da análise de Inteligência para todo o sistema brasileiro.

Referências

AFONSO, Leonardo S. Considerações sobre a relação entre a Inteligência e seus usuários. *Revista Brasileira de Inteligência*. Brasília, v. 5, p. 7-19, out. 2009.

AMBROS, Christiano C. *Inteligência Governamental como Política Pública: fatores cognitivos e institucionais na explicação de falhas e dilemas de efetividade*. Dissertação submetida ao Programa de Pós-Graduação em Ciência Política da Universidade Federal do Rio Grande do Sul, como requisito parcial para obtenção do título de Mestre em Ciência Política. UFRGS, Porto Alegre, 2011.

ARTNER, Stephen; GIRVEN, Richard; BRUCE, James. *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community*. Rand Corporation, 2017.

BAR-JOSEPH, Uri e McDERMOTT, Rose. Change the Analyst and Not the System: A Different Approach to Intelligence Reform. *Foreign Policy Analysis,* nº 4. 2008

BETTS, Richard K. Analysis, war, and decision: why intelligence failures are inevitable. *In:* GILL, Peter & MARRIN, Stephen & PHYTHIAN, Mark (ed.). *Intelligence Theory: Key questions and debates*. New York: Routledge, 2009.

BETTS, Richard K. Surprise despite warning: Why sudden attacks succeed. *In:* ANDREW, Christopher & ALDRICH, Richard & WARK, Wesley. *Secret Intelligence: A Reader*. New York: Routledge, 2009.

BETTS, Richard K. *Enemies of Intelligence: Knowleadge and Power in America National Security*. New York: Columbia University Press, 2008.

BRUNEAU, Thomas & BORAZ, Steven (ed.). *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness.* Austin-TX: University of Texas Press, 2007.

BUTTERFIELD, Alexander P. Jr. *The Accuracy of Intelligence Assessment: Bias, Perception, Judgment in Analysis and Decision*. Newport: Naval War College, 1993

CAVERNI, J.; FABRE, J.; GONZALEZ, M. *Congnitive Biases*. Amsterdam: North Holland, 1990.

CHANG, Welton; BERDINI, Elissabeth; MANDEL, David; TETLOCK, Philip. Restructuring structured analytic techniques in intelligence. *Intelligence and National Security,* v. 33, 2018 - Issue 3.

CLARK, Robert. *Intelligence Analysis: A target-centric approach*. Washington: CQ Press. Second Edition, 2007.

COELHO, Danilo. A Modernização da Inteligência Estratégica na Perspectiva da Segurança

Humana. *Revista Brasileira de Inteligência*. Brasília, n. 12, dez, 2017.

COULTHART, Stephen Why do analysts use structured analytic techniques? An in-depth study of an American intelligence agency, *Intelligence and National Security,* 31:7, 933-948, DOI: 10.1080/02684527.2016.1140327, 2016.

DAMACIO, Antonio. Descartes' *Error: Emotion, Reason, and the Human Brain*. New York: Putnam, 1994.

DAVIS, Jack. A Policymaker's Perspective on Intelligence Analysis. *Studies in Intelligence* 38, no. 5, 1995.

DAVIS, Jack. Combating Mind-Set. *Studies in Intelligence* 36, no. 5., 1992.

DAVIS, Jack. Intelligence Analysts and Policymakers: Benefits and Dangers of Tensions in the Relationship." *Intelligence and National Security* 21, no. 6. Dec., 2006.

ELSTER, Jon. *Peças e engrenagens das ciências sociais*. Rio de Janeiro: Relume-Dumará, 1994

FELLER, W. *An Introduction to Probability*. New York: Wiley, 1968

GEORGE, Roger Z. & BRUCE, James B. (ed.) *Analyzing intelligence: origins, obstacles and innovations*. Washington: Georgetown University Press, 2008.

GILL, Peter. Keeping Easthly Awkwardness: Failures of Intelligence in the United Kingdom .*In*: BRUNEAU, Thomas & BORAZ, Steven (ed.). *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*. Austin-TX: University of Texas Press, 2007.

GILOVICH, Thomas & GRIFFIN, Dale & KAHNEMAN, Daniel (ed.). *Heuristics and Biases: The Psychology of Intuitive Judgment*. New York: Cambridge University Press, 2002.

GINGERENZER, Gerd. How to Make Cognitive Illusions Disappear: Beyond "Heuristics and Biases". *In*: STROEBE, W. & HEWSTONE, M. (ed) *European Review of Social Psychology* —v. 2. Chichester: Wiley, 1991.

HALL, P. A. and TAYLOR, R. C. Political Science and the Three New Institutionalisms. *Political Studies*, 44: 936-957, 1996.

HALLINAN, Joseph T. *Por que cometemos erros?*. São Paulo: Globo, 2010.

HANDEL, Michael I. Intelligence and the problem of strategic surprise, *Journal of Strategic Studies*, 7:3, 229-281, 1984.

HASELTON, Martie G.; NETTLE, Daniel; MURRAY, Damian R. The Evolution of Cognitive Bias. In: BUSS, David M (ed.). *Handbook of Evolutionary Psychology*. Nova Jersey: John Wiley & Sons, 2016.

HERZ, John. Idealist Internationalism and the Security Dilemma. *World Politics,* 2(2), 157-180, 1950.

HERZ, Monica. Análise Cognitiva e Política Externa. *Contexto internacional*. Rio de Janeiro, v. 16, nº 1, 1994, pp. 75-89.

HEUER, Richard J. & PHERSON, Randolph H. *Structured Analytic Techniques for Intelligence Analysis*. Washington: CQ Press, 2011.

HEUER, Richard J. & PHERSON, Randolph H. *Structured Analytic Techniques for Intelligence Analysis*. Washington: CQ Press, 2014.

HEUER, Richard J. The Evolution of Structured Analytic Techniques. Presentation to the National Academy of Science, Washington DC., 2009. Disponível em: https://www.e-education.psu.edu/geog885/sites/www.e-education.psu.edu.geog885/files/file/Evolution_SAT_Heuer.pdf

HEUER, Richard J. *The Psychology of Intelligence Analysis*. Washington: Central Intelligence Agency (CIA), 1999.

JERVIS, Robert. The Politics and Psychology of Intelligence and Intelligence Reform. *The Forum,* v. 4: Issue. 1, 2006

JERVIS, Robert *Perception and Misperception in International Politics*. Princeton: Princeton University Press, 1976

JERVIS, Robert. *Why Intelligence Fails: Lessons from the Iranian Revolution and Iraq War*. New York: Cornell University Press. 2010.

JORDÁN, Javier *Introducción al análisis de inteligencia*. Granada: Grupo de Estudios en Seguridad Internacional (GESI), 2011

KAHNEMAN, Daniel *Rápido e devagar: duas formas de pensar*. Rio de Janeiro: Objetiva. 2011

KAHNEMAN, Daniel & TVERSKY, Amos (ed.). *Choices, Values and Frames*. New York: Cambridge University Press., 2000.

KAHNEMAN, Daniel & TVERSKY, Amos (ed.). *The Psychology of Intuitive Judgment:* Heuristics and Biases. New York: Cambridge University Press, 1982.

KENT, Sherman. Words of Estimated Probability" *In* Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays*. CIA, Center for the Study of Intelligence, 1994.

KERBBELL, Mark R. & MULLER Damon & MARTIN, Kirsty. Understanding and

Managing Bias. In: BAMMER, Gabriele (ed). *Dealing with uncertainties in policing serious crimes*. Canberra: ANU Press, 2010.

KHALSA, Sundri. The Intelligence Community Debate over Intuition versus Structured Technique: Implications for Improving Intelligence Warning and Analysis. *Journal of Conflict Studies*. p. 75-95, 2009.

LANGER, Ellen J. The Psychology of Chance. *Journal for the Theory of Social Behavior,* 7, p. 185-208, 1977.

LOWENTHAL, Mark. *Intelligence: From Secrets to Policy*. Washington-DC, CQ Press, 2006.

MARRIN, Stephen. Intelligence analysis and decision-making: methodological challenges *In*: GILL, Peter & MARRIN, Stephen & PHYTHIAN, Mark (eds.). *Intelligence Theory: Key questions and debates*. New York: Routledge, 2009.

MARRIN, Stephen. Intelligence Analysis: Structured Methods or Intuition? *American Intelligence Journal*. Summer, 2007.

MACHADO, André Mendonça. O impacto de vieses cognitivos sobre a imparcialidade do conteúdo de Inteligência. *Revista Brasileira de Inteligência*. Brasília, v. 13, p. 9-24, dez., 2018.

MINTZ, Alex & DeROUEN, Karl.. *Understanding Foreign Policy Decision-Making*. New York: Cambridge University Press, 2010

PINKER, Steven. *Como a mente funciona*. 2º edição. São Paulo: Companhia das Letras. 1999.

PHYTIAN, Mark. Intelligence Analysis Today and Tomorrow. *Security Challenges*. v. 5, nº1, 2009.

POHL, Rudiger F. (ed.) *Cognitive Illusions: a Handbook on fallacies and biases in thinking, judgment and memory*. New York: Psychology Press, 2004.

ROSITO, Guilherme A. Abordagem Fenomenológica e Metodologia de Produção de Conhecimentos. *Revista Brasileira de Inteligência*. Brasília, v. 2, n. 3, p. 23-28, set., 2006.

TEOVANOVIC, P., KNEZEVIC, G., STANKOV, L. Individual differences in cognitive biases: Evidence against one-factor theory of rationality. *Intelligence*, 50, 75-86, 2015.

TVERSKY, A; KAHNEMAN, D. Judgment under uncertainty: heuristics and biases. *Science, New Series,* 185 (4157), p. 1124-1131, 1974.

US GOVERNMENT. *A Tradecraft Primer, Structured Analytic Techniques for Improving Intelligence Analysis, 2009*. Disponível em: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.

Acesso em 20 de junho de 2019.

ZEGART, Amy. *Flawed by Design: The Evolution of the CIA, JCS and NSC*. Stanford-CA, Stanford University Press,1999.

A PSYCHOLOGICAL APPROACH TO RADICALIZATION, TERRORISM AND MASS MURDERING

The case of Anders Breivik

Guilherme R.

Abstract

Anders Breivik is an individual known to have conducted one of the most devastating terrorist attacks in the history of Europe. All evidence suggests that he acted without the direct support of any group or organization. This article addresses the matter of why, but mainly how an individual can radicalize his thoughts and actions to the point of committing mass murder. The present study analyses Anders Breivik's pathway, from political radicalism to extremist thoughts and, finally, terrorism. An analysis of the Norwegian shooter's discourse, from his manifesto, based on Bandura's moral disengagement model proves to be useful, as it explains some of the mental processes involved in the phenomenon of political violence. Other scholars like Horgan, Borum, and McCauley & Moskalenko were also brought to the discussion. All psychological traits should be considered in accordance to their correlation with personal history and situational factors. Understanding and applying psychological models is a crucial task for countering radicalism and political violence, regardless of the analyst's professional background.

Keywords: *big data; intelligence analysis; artificial Intelligence; prediction capability.*

UMA ABORDAGEM PSICOLÓGICA PARA A RADICALIZAÇÃO, O TERRORISMO E A VIOLÊNCIA EM MASSA:

O caso de Anders Breivik

Resumo

Anders Breivik é um indivíduo conhecido por ter conduzido um dos ataques terroristas mais devastadores da história da Europa. Todas as evidências apontam para o fato de ele ter agido sem o apoio direto de qualquer grupo ou organização. Este artigo discute aspectos ligados aos porquês, mas principalmente a como um indivíduo alcança tamanho grau de radicalização em seus pensamentos e ações a ponto de cometer assassinato em massa. Uma leitura do manifesto escrito por Breivik ajuda a delinear um quadro de seu modelo ideológico. O presente trabalho analisa a trajetória percorrida por Breivik entre o radicalismo político, o pensamento extremista e o engajamento em uma ação terrorista. A análise do discurso apresentado no Manifesto publicado pelo extremista norueguês a partir da teoria do desengajamento moral de Bandura revela-se útil para a compreensão dos processos mentais envolvidos no fenômeno. Também é utilizada a produção de autores como Horgan, Borum e Mcauley & Moskalenko. Os traços psicológicos associados ao comportamento terrorista devem ser considerados a partir de sua correlação com o histórico pessoal e a presença de fatores situacionais. Compreender e aplicar modelos da psicologia é tarefa crucial para analistas de contraterrorismo de todos os campos profissionais.

Palavras-chaves: terrorismo, radicalização, extremismo, desengajamento moral, psicologia, Breivik.

Introduction

On the 22nd of July 2011 a bomb was detonated in a white van parked right in front of Oslo's Cabinet Building (høyblokken), the office of Norway's Prime Minister. The explosion killed eight people and destroyed an important part of important governmental facilities. It took about half an hour for media vehicles to confirm that neither the Prime Minister, nor any other member of the government was injured in the attack. As the security and emergency forces coordinated first response efforts, 32-year-old Anders Breivik stepped down of a ferryboat at the Island of Utoya, where the annual summer youth camp of the Norwegian Labour Party was taking place. There, he shot and killed sixty-nine people, before the first members of a police team arrived at the island. Breivik then surrendered without any resistance. On the previous day, to about 7000 online contacts, the attacker had posted a compendium, consisting of around 1500 pages of far-right ideology and an operational guide, called "2083 – A European declaration of independence". This was the first mass violence event on Norwegian soil since the German occupation during World War II (Eriksen, 2012).

When listening or reading about the attacks of Oslo and Utoya, all kinds of questions shall come to mind. Some might ask how an individual, apparently acting alone, could cause that amount of causalities and stay loose for enough time in order to attack in two different places, acting with such cruelty against his own fellow citizens. Also, how this could happen in such a highly organized and well-developed country, also known for its reputation of having a peaceful and welcoming society as Norway (Lars H. Thorkildsen/Håkon Kavli, 2009). However, maybe more important among all questions, why he did it, and how we could prevent that from happening again. Those are all common issues that come to mind when talking about lone actors (or lone wolf) extremism.

This article addresses some of those questions, with more emphasis given to the 'how' than the 'whys'. Lone wolves, here defined as extremist attackers that act without any direct group or organizational support, tend to have such a number of different profiles, that it may be almost impossible to pinpoint one of them just by putting together a list of personal features. Horgan (2017) says that "neither psychological nor other research has revealed qualities unique to those who become involved in terrorism, or the existence of singular pathways into (and out of) terrorism". However, some scholars indicate that the radicalization process, and even more, the preparatory actions for a terrorist attack, are much more susceptible for data collection, analysis and categorization (Bakker & de Graaf, 2011).

Focusing on Breivik's case, one should start asking about his victims. Why did he choose those specific individuals and those specific buildings to send his message? A reading of Breivik's manifest draws a clear picture of his ideology. According to him, cultural Marxism and the Islamisation of the Continent are a deadly threat to the very existence of the "indigenous people of Europe" (Breivik, 2011). According to his *compendium*, it all starts after World War II, with the notion of political correctness as

the basis of an entire establishment, built up from the pillars of the Marxist ideology, to oppress any form of nationalism, as well as the manifestation of traditional western European values. Breivik takes the 50's as the Continent's golden years and, at the same time, his picture of a perfect future:

> "Most Europeans look back on the 1950s as a good time. Our homes were safe, to the point where many people did not bother to lock their doors. Public schools were generally excellent, and their problems were things like talking in class and running in the halls. Most men treated women like ladies, and most ladies devoted their time and effort to making good homes, rearing their children well and helping their communities through volunteer work. Children grew up in two–parent households, and the mother was there to meet the child when he came home from school. Entertainment was something the whole family could enjoy".
>
> (Breivik, 2011, p. 19).

So, from Breivik's point of view, the logic of choosing the government and the young Labour Party members was made for their value as symbols of everything Breivik denounces: Marxism, multiculturalism, globalism and so on. When considering his world view, the apparent contradiction between his violent attacks and Norway's open and welcoming society disappears completely. Breivik did not commit mass murder in spite of his nation's current values. He did it because of them. Moreover, he selected his targets, because they are an image of everything he hates about his country (and Europe as well). It was the perfect "example of what an effective lone wolf attack can look like" (Pantucci, 2011. P. 35). Apparently random, but meticulously planned and prepared. A result of one man's mind, but drawn from a broader ideology. Based on specific circumstances and opportunities, but built up from a gradual process of radicalization of thought and behaviour.

Literature review

Horgan (2005) shows that violent extremism is the end state of a process resulting from a series of push and pull factors, that could be divided in three basic moments: becoming involved, remaining involved (or 'being' a terrorist), and leaving terrorism behind. The author also demonstrates that it is impossible to establish an exact formula, or a combination of factors that will result in political violence. Feelings of injustice, social exclusion or deprivation, grievances, marginalization (push factors), as much as social dynamics, propaganda, a charismatic leadership, and personal bonds (pull factors); they all play an important role in a terrorist's mind and behaviour. Nevertheless, they alone are not enough to predict violence.

Vergani and his colleagues (2018), discuss a third set of driving forces, playing a decisive role on the path between radical ideas and political violence: the personal features. They can be mental health conditions, personality traits or even some specific demographic characteristics, as gender, age and nationality. Their systematic literature review shows, that radicalization is a "mechanism that entails a real or perceived political grievance, a perceived reward or appeal of violent extremism and a personal vulnerability" (Vergani et al, 2018, p. 30).

In the particular case of lone wolves, McCauley, Moskalenko and Van Son (2013)

indicate some greater influence of those personal factors. Comparing lone wolves to school shooters and assassins, the authors find that "depression, grievance, unfreezing, and weapons experience are the common characteristics uncovered" (2013, p. 19). In a later article McCauley and Moskalenko elaborated on a two-pathway model towards terrorism:

> "Statistical studies indicate what may be called a disconnected-disordered profile: individuals with a grievance and weapons experience who are socially disconnected and stressed with a psychological disorder. But at least three of our case histories do not fit this description: Zasulich, Waagner, and al-Balawi had social skills, solid social connections, and no sign of mental disorder. Rather these individuals have a caring-consistency profile: they felt strongly the suffering of others and a personal responsibility to reduce or revenge this suffering".
>
> (McCauley & Moskalenko, 2014, p. 83).

For both profiles, the authors emphasise the role of situational factors, like the access to weapons and other resources, as well as an opportunity to act. In Breivik's case, it seems more plausible to argue that he followed the path of the socially disconnected killer, who consistently spent years feeding his mind with radical ideas at the same time that he pursued a number of forms of putting together the means to execute his plan. McCauley and Moskalenko (2010) also focused on the difference between activism and radicalism, meaning that a person can have and advocate the most radical ideas without ever engaging in any violent or illegal action. They demonstrate the difference between radicalization of opinion and radicalization of action (2010, 2014).

Breivik is an example of someone that was a radical on both dimensions, had access to the tools and was able to put himself in a situation that allowed him to engage in a behaviour that materialized his radicalism.

Bandura (2016) defines moral agency as a whole set of behaviours that keep the individual consonant with his concept of right and wrong. These actions often include "negative self-sanctions for conducts that violate one's moral standards and the support of positive self-sanctions for conducts faithful to personal moral standards" (Bandura 2016, p. 17). Discussing the human capacity to engage in violence, the author describes a series of psychosocial processes that work in order to weaken, or even disengage, the restrictions on an inhumane conduct. He classifies them as the four different dimensions *(locus)* of moral self-regulation: behaviour, agency, outcome and victims.

In the behavioural *locus,* an individual can disengage morality, by investing his conduct with moral endings (Bandura, 2016). For example, a soldier can say that his killings in the battlefield will assure the security of his nation, and the very existence of his people. Another way to do it would be through a palliative comparison. The same soldier could argue that the battles he fought would assure a sooner ending to the war, preventing more suffering for both sides in the conflict. This could all be reinforced by the use of euphemistic language, like, for example, "killings in the battlefield" could be replaced by "neutralizing the enemy's capabilities". In Breivik's *compendium*, he talks about assuring the security and the existence of the indigenous people of Europe, by

neutralizing the Islamic menace (Breivik, 2011).

In the agency *locus*, Bandura demonstrates how people can evade personal responsibility for their actions by blaming others, or even dispersing it so widely that no one could really bear it. An executioner, working on a lethal injection facility, could find comfort in the notion that he is just a link of a greater process formed by a judge, a jury, his fellow executioners, each one with a small responsibility doing a hard job in the name of his country and its constitutional values. Alternatively, a jihadist could argue that it is not about him killing people, but his hand as a small instrument of his people, acting by the will of Allah. Breivik, on the other hand, depicts the Muslims as violent invaders, and himself as only one of many cells of resistance in the name of "the peoples of Europe" (2011, p. 779), preserving western values, protecting Christianity and their very existence as Europeans.

At the outcome *locus*, the injurious effects of violence are disregarded, or at least minimized. Therefore, using the soldier's example, he could say that he does not have the time to think about the enemies as other human beings suffering, as he is just shooting at the opposite direction of a threat, by instinct, as he was trained to do. He could just say that killing is just a normal part of fighting. This seems even easier for commanders, at a further distance from the battlefield, designing strategies on top of maps, charts and numbers. In Breivik's words: "Some innocent people will die in our operations as they are simply at the wrong place at the wrong time. Get used to the idea. The needs of the many will always surpass the needs of the few" (2011, p. 846).

Finally, at the victim *locus*, attackers tend to dehumanise their targets, labelling them in a deleterious way, or portraying them as a dangerous threat; thus, acting against them is a mere act of self-defence. "In this mode of self-exoneration, perpetrators view themselves as victims forced to behave injuriously by wrongdoers' offensive behaviour or by force of circumstances. By viewing themselves as victims, they may feel self-righteous in their retaliatory actions" (Bandura, 2016, p. 19). Breivik fills his *manifesto* with numerous examples of violent, cruel and supremacist behaviours attributed to Muslims. When describing his mission, he portrays himself as a "Justiciar Knight Commander": according to him, a self-appointed individual with the authority to act as a judge, jury and executioner on behalf of the indigenous people of Europe (Breivik, 2011). Explaining the role of a Justiciar Knight, Breivik affirms: "Never forget that it is not only your right to act against the tyranny of the cultural Marxist/multiculturalist elites of Europe, it is your duty to do so." (Breivik, 2011, p. 846).

Bandura (2016) demonstrates how these regulatory cognitive mechanisms can modulate moral self-sanctions over harmful practices. It provides an individual with the means to preserve his self-image and a sense of self-righteousness while acting harmfully. The author discusses the applications of his model to explain morally disengaged violence in all sorts of situations, like the gun industry, capital punishment and even at the corporate world. He also discusses the applications of this theory as an analytical model to understand terrorism and the

influences of discourse, propaganda and ideology to shape one's view of the attacks, the victims, and the consequences of the terrorist strategy.

The trajectory to terrorism

According to his *compendium*, shortly before becoming concerned about politics, Breivik had been a member (or an acquaintance) of a number of street gangs, including Pakistani Muslim ones. He describes this part of this life as his "graffiti phase", affirming that he had been a very active and well-known member of the hip-hop movement during the 90s (2011, p. 1387). He, however, portrays his contacts with Muslims as pragmatic alliances in order to keep security and respect at the streets of the multicultural and sometimes violent Oslo. Breivik describes what he calls a "Marxist-jihadi youth" movement, as a number of hypocrites and violent people that literally "hijacked segments of the hip-hop movement and used it as a front for recruitment" (2011, p. 1391). He also claims to have suffered, or being involved in, "8 unprovoked assaults and multiple threats and attempted robberies by Muslims" (2011, p. 1394).

Breivik uses his early contact with young Pakistanis as an additional proof that he knows what he is talking about when describing his worldview. For him, the violent attacks perpetrated by Muslims against white Norwegians are no less than a sample of what is happening all around Europe: a new wave of Islamic domination. Moreover, he concludes that his multicultural society depicts Marxists and Muslims as perpetual victims and gives them a free pass over any demonstration of violence against white Europeans as if it was just a reaction against some form of historical oppression: "This is still the case in all Western European major cities. They are allowed to consolidate, while we are not" (2011, p. 1390).

From those roots, Breivik's trajectory towards radicalism, from thought to action, began with traditional politics, according to him, at the age of 16:

> "I broke with the hiphop movement and my network when I was 16 and later joined the Progress Party youth movement, a moderate cultural conservative youth movement of the Progress Party. This became the period where I decided I wanted to dedicate my life to politics in order to contribute to change the system" (Breivik, 2011, p. 1397).

He describes being gradually frustrated with traditional politics and democracy, portraying his Party as being more a part of the problem than a solution, since it would give a false hope to the people, misleading them to believe in the system. In 2003, he ran for a position as a member of Oslo's City Council, but was defeated, in his opinion, due to lack of support from the Party and some undermining movements from his opponent Jøran Kallmyr, then Leader of the Progress Party Youth: "I don't blame him for backstabbing me like that though. After all, he had invested so much more of his time to the organization than I had. He deserved it while I didn't and I would probably have done the same thing if I was him" (Breivik, 2011, p.400).

At the time he was running for the City

Council, Breivik said he was already affiliated to the organization he claimed to be behind his attacks: The Knights Templar (Pauperes Commilitones Christi Templique Solomonici – poor fellow-soldiers of Christ and the Temple of Solomon - PCCTS). Breivik put himself as one of its founding members, though, until this moment, no evidence exists of such organization, and no trace of the other members described at the manifest has ever been found.

Breivik claimed to have attended a meeting in London, in the year of 2002. He described undergoing some screening process, before being called to meet his new PCCTS fellows, during those days at the UK. There they would have been instructed about strategy, ideology and operational doctrine of their new order. On the last day, all members would have been strictly advised not to meet each other again, aiming to preserve the existence, the purposes, as well as the efficiency of each individual cell.

In Breivik's words, "those were not sessions where regular combat cells were created. It was more like a training course for pioneer cell commanders" (2011, p. 1379). He defined the strategy of his new fellows as a long-term one (50-100 years), consisting of single man, or small cells, aiming to perform an attack every 5 to 12 years, so each new event did not obfuscate the effect of the previous one. Their long-term goal would be no more ambitious than to seize power over Europe, getting rid of any trace of Marxism, multiculturalism along with reversing the Islamization of the Continent.

The *compendium* has a whole chapter instructing readers about operational aspects of being a Knight Templar. The author discusses tactics, training and preparation methods, and even formulates a list of targets with priority evaluations. His topics go from how to build and maintain a cover, to how to prepare oneself physically, with training and even cycles of steroids and stimulants. Breivik's operational manual is a meticulous and detailed one, for example, when describing how to obtain the right ingredients and materials for bomb making:

> "You don't start the separate phases until you are completely done with each sub-phase. You DO NOT initiate two or more phases at the same time! You always start with the hardest part – the acquisition of TNT/dynamite/semtex or similar substances, then move on to the next phase.
>
> (Breivik, 2011, p. 853).

Even though it is hard to determine exactly which were the main situational factors concerning his decision to attack, it is safe to assume that Breivik's experiences with Muslims, together with his failed attempts to participate in formal politics, played an important role in his trajectory to violence. Breivik's writings indicate a number of turning points in his life, one of them being the Serbian conflict. "He claims that in 2002 he travelled to Monrovia, Liberia, where he sought out an individual Serbian nationalist who was living there and he was obviously very impressed by him" (Pantucci, 2011, p. 31).

Less on the "whys" and more on the "how", one can argue that Breivik, not only in his writings, was giving a number of indications that he was an individual already capable of breaking the law, shifting from radical

thoughts to violent actions. Records show that he had been involved in number of minor offences (graffiti phase), frauds (selling fake university documents) and other activities (attempting to buy weapons at the Czech Republic's black market) that could have potentially flagged him as a threat (Hemmingby & Bjørgo, 2018). If someone could have put together those previous actions along with his online activity (searching for like-minded individuals and putting together a list of about 7000 contacts) and the purchase of fertilizer, it would have been possible to appoint him as a high priority target; someone engaged in "unambiguous terrorist activity" (Borum, 2011, p. 58).

Maybe this is the greatest issue about preventing lone wolves' violence: their loneliness forces them to raise their level of exposition in order to be able to act, but, at the same time, their lack of any ties, or connections, leads to security and intelligence services disregarding them as a potential threat.

It is, of course, a lot easier to align all the variables and make sense of it after an attack. One cannot really blame it on security services' flaws. The position of some scholars is that post event analysis is not about pointing fingers, but serving the purpose of updating theoretical framework, analytical models, as well as constantly reviewing methods and the workflow of intelligence production in order to prevent future attacks (Bakker & de Graaf, 2011).

Assumptions

Being a perfect example of a lone wolf attack, maybe Breivik is also a perfect case for learning and preventing future events of political violence. What can be learned about him in order to prevent and counter radicalization into violent extremism?

First, his moral disengagement can be described as a multidimensional and comprehensive one. Examples of all four dimensions of Bandura's model could be found in his writings:

- behaviour: just assuring the security of the indigenous people of Europe;

- agency: preserving Western values, protecting Christianity;

- outcome: innocents will die. They are simply at the wrong place at the wrong time;

- victims: globalists are sponsoring the Muslim invasion. It is our duty to liberate Europe from them.

A correlation between behavioural variables and situational factors is also an important element of concern. This makes sense regarding McCauley, Moskalenko and Van Son's (2013) study of school attackers, assassins and lone wolves. Finding a positive correlation between variables like personal and political grievance, slippery slope, risk (or status) seeking, unfreezing and the access to weapons and targets, they suggest that a prevention strategy is a matter of knowledge and communication, as well as involving different actors (psychological services, VA associations, families) in the task of identifying and dealing with possible offenders.

Nowadays, technology and social media make it easy for an individual to publish his ideology as much as make his actions reach a considerable audience, even without any support of a mass communication enterprise. Terrorism is mainly about spreading a message. Recently, in Christchurch, New Zealand, 28-year-old Brenton Tarrant opened fire at two local Mosques, killing 50 people and injuring around other 50. He also published an online manifesto and managed to broadcast his attacks live on the internet. When explaining his motives, he wrote: "to most of all show the invaders that our lands will never be their lands, our homelands are our own and that, as long as a white man still lives, they will NEVER conquer our lands and they will never replace our people" (Tarrant, 2019, p. 5). Among his inspirations to engage in political violence, he cites Anders Breivik as the only true one.

The formal broadcasting industry, even though not anymore in control of all means of publication, still attains a crucial role in interpreting the acts, portraying the perpetrators, as well as the victims, and making sense of what happened. When trying to understand the radicalization process and the possibilities to prevent lone actor violence, it is imperative that the discussion about outcomes and narratives not only advance as a research topic, but also as a major concern to security forces and public policy makers.

Both future studies and intelligence analysis could keep focusing on trying to detect and understand behavioural signs of moral disengagement, changes in discourse and social dynamics, lack of empathy towards a specific population, motivations and activities shifting towards a specific focus. All those psychological traits should be considered in accordance to their correlation with personal history and situational factors. Preventing and countering radicalization into violent extremism is a multidisciplinary task. When dealing with individuals, and how their personal histories and relationships shape their worldview, motivations and actions, understanding and applying psychological models is a crucial task for analysts of all professional fields.

Bibliografy

BAKKER, E.; GRAAF, B. Preventing lone wolf terrorism: some CT approaches. *Perspectives on Terrorism,* Lowell-MA, v. 5, n. 5-6, December 2011.

BANDURA, A. *Moral disengagement how people do harm and live with themselves.* New York Worth Publishers. Macmillan Learning, 2016.

BREIVIK, A. B. *2083 – A European declaration of independence.* London: 2011. Disponível em: https://fas.org/programs/tap/_docs/2083_-_A_European_Declaration_of_Independence.pdf.

BORUM, R. Radicalization into violent extremism II: a review of conceptual models and empirical research. *Journal of Strategic Security.* Tampa-Florida: University of South Florida Board of Trustees, v. 4, n. 4, p. 37-62, winter 2011.

ERIKSEN, A. K. O. *Exclusion and Xenophobia: Norwegian society's influences on Anders Behring Breivik's counter jihadism.* Dissertação (Mestrado em Estudos Internacionais) – University of San Francisco, 2012. Master's Theses. 39. San Francisco-CA, 2012. Disponível em: https://repository.usfca.edu/thes/39.

HEMMINGBY, C.; BJORGO, T. Terrorist Target Selection: The Case of Anders Behring Breivik. *Perspectives on Terrorism,* Lowell-MA, v. 12, n.6, p.164-176, December 2018.

HORGAN, J. *The psychology of terrorism.* London: Routledge, 2005.

McCAULEY, C; MOSKALENKO, S. Measuring political mobilisation: the distinction between activism and radicalism. *Terrorism and Political Violence,* London: Taylor & Francis Group, LLC, v. 21, n. 2, p.239-260, april 2009.

McCAULEY, C.; MOSKALENKO, S.; VAN SON, B. Characteristics of lone wolf violent offenders: a comparison of assassins and school attackers. *Perspectives on Terrorism,* Lowell-MA, v. 7, n. 1. 2013.

McCAULEY, C.; MOSKALENKO, S. Toward a profile of lone wolf terrorists: what moves an individual from radical opinion to radical action. *Terrorism and Political Violence,* London: Taylor & Francis Group, LLC, v. 26, 2014.

McCAULEY , C.; MOSKALENKO, S. Understanding political radicalization: The two-pyramids model. *American Psychologist,* Washington – DC: American Psychological Association, v. 72, n. 3, p. 205-216, april 2017.

PANTUCCI, R. What have we learned about lone wolves from Anders Behring Breivik? *Perspectives on Terrorism;* Lowell – MA, v. 5, n. 5-6, 2011.

SEDGWICK, M. The concept of radicalisation as a source of confusion. *Terrorism and Political Violence,* London: Taylor & Francis Group, LLC, v. 22, 2010.

TARRANT, B. *The great replacement.* 2019. Disponível em: http://www.freepdf.info/index.php?post/Tarrant-Brenton-The-Great-Replacement.

THE NORWEGIAN. The Norwegian Ministry of Foreign Affairs / Innovation Norway. *Improving Norway's reputation.* Prepared by: Lars H. Thorkildsen and Håkon Kavli. Synovate Ltd, 2009.

VERGANI, M.; IQBAL, M.; ILBAHAR, E.; BARTON, G. The 3 Ps of radicalisation: push, pull and personal. A systematic scoping review of the scientific evidence about radicalisation into violent extremism. *Studies in Conflict and Terrorism.* Melbourne: Alfred Deakin Institute for Citizenship and Globalisation. Deakin University, September 2018.

ESTRUTURA BRASILEIRA DE CONTRATERRORISMO E SUA EFICÁCIA NA PREVENÇÃO E NA NEUTRALIZAÇÃO DE AMEAÇAS EXTREMISTAS

Thiago Araújo *

Resumo

O Brasil alcançou recentemente vários avanços em sua estrutura legal, preventiva e persecutória do terrorismo enquanto crime e ameaça interna. O presente trabalho tem como objetivo analisar esta estrutura e as implicações dos avanços alcançados no contexto de inserção do fenômeno na conjuntura interna do país. Por meio do estudo de atos normativos e revisão bibliográfica sobre processos de radicalização, buscou-se avaliar a capacidade brasileira no combate ao terrorismo a partir da análise de casos concretos. Conclui que as experiências recentes em identificação de ameaças e consequentes processos de investigação, indiciamento criminal, denúncia e julgamentos apontam para um eficaz ciclo de combate ao terrorismo do país, que envolve, em seu curso, a participação de vários órgãos públicos e se estende das atividades iniciais da Inteligência até a condenação e a execução de penas pelo poder judiciário e por órgãos de segurança pública. Porém, também são identificadas algumas necessidades de avanços na capacidade dessa estrutura em atuar efetivamente na mitigação da complexa e, muitas vezes, pouco perceptível raiz do extremismo violento. Os avanços alcançados e necessários, em meio a mudanças na dinâmica do terrorismo internacional, geram, aos órgãos que compõem o SISBIN, novos desafios no combate ao terrorismo transnacional.

Palavras-chaves: terrorismo; extremismo religioso; contraterrorismo

BRAZIL'S COUNTERTERRORISM APPARATUS AND ITS EFFECTIVENESS IN PREVENTING AND NEUTRALIZING EXTREMIST THREATS

Abstract

Brazil has recently made several advances in its legal framework, in the prevention and persecution of terrorism as a crime and domestic threat. This article aims at analyzing said framework and advances and how they contributed to make the phenomenon part of the country's public reality. By studying the normative acts and conducting a thorough literature review concerning radicalization processes, the intention was to assess Brazil's capabilities to combat terrorism through the analysis of concrete cases. The conclusion was that recent experiences in identifying threats and the subsequent investigations, criminal indictments, accusations and judgments may show that the terrorism combat cycle has been effective in the country, involving several government agencies from early intelligence stages all the way through law enforcement, judicial prosecution and carrying out of sentences. Nevertheless, the article has identified a few areas for further advancement in that structure as to effectively mitigate the complex and often elusive roots of violent extremism. Advances that are needed specially while facing the ever-changing context of international terrorism bring about new challenges to the organs that are a part of the Brazilian intelligence community.

Keywords: *Terrorism; Religious extremism; Counterterrorism*

* Oficial de Inteligência que atua há 10 anos na área de contraterrorismo e é instrutor de análise do terrorismo da Escola de Inteligência (Esint/ABIN).

Introdução

O fenômeno do terrorismo internacional passou por importantes transformações ao longo da última década, relacionadas, principalmente, aos métodos e técnicas envolvidos na difusão do pensamento radical e na execução das ações terroristas. Essas transformações, que definiram a dinâmica do terrorismo contemporâneo,

iniciaram-se em meados da década de 2000, quando a Al-Qaeda ainda atuava como maior ameaça terrorista global, e atingiu seu ápice nos anos 2014 e 2015, com a formação do então chamado "califado islâmico", estabelecido pelo grupo terrorista Estado Islâmico (EI)[1] .

Estudos acadêmicos realizados nesse período apontam dois importantes vetores que se destacaram na construção do cenário recente do terrorismo internacional: a simplificação do discurso radical e dos métodos de ação das organizações terroristas, aliados à eficiente exploração das redes sociais como principal meio de comunicação e publicidade do discurso extremista[2]. Esses dois vetores foram essenciais para que o discurso extremista islâmico de vertente sunita ganhasse proporções até então inimagináveis, ao alcançar dimensão global e atingir grupos e populações que não apresentavam, à época, quaisquer indicativos de vulnerabilidades à radicalização.

Nos últimos anos, percebeu-se um contínuo processo de simplificação dos ataques terroristas – com maior uso de armas brancas, carros, bombas caseiras improvisadas e outros recursos – que, independentemente do número de mortes resultantes, ganham grande espaço na mídia e comunicam ao grande público um espetáculo de terror[3]. Com o EI, essas ações foram acompanhadas de uma eficiente estratégia de propaganda do ideário extremista, difundida em ambiente virtual, com a utilização de uma linguagem simples, política, impactante e extremamente apelativa (VEILLEUX-LEPAGE, 2016).

Esse modelo de radicalização e eficiente exploração midiática do terror encontrou grande receptividade de jovens brasileiros nesse período e agregou características próprias relacionadas a fatores socioculturais do país (A., THIAGO; O. AUGUSTO; S. ALLAN, 2017).

Em julho de 2016, grupo de radicais foi

1 Quanto aos termos Estado Islâmico, ISIS, ISIL, Daesh etc., optamos por utilizar o termo "Estado Islâmico" nesta obra por ser mais usual na mídia e na literatura brasileiras e por estar em consonância com a abordagem apresentada em HASHIM, Ahmed S. The Islamic State: from Al-Qaeda affiliate to Caliphate. *Middle East Policy*, v. 21, n. 4, p. 69-83, 2014. e Zach Beauchamp, "ISIS, Islamic State or ISIL? What to call the group the US is bombing in Iraq". *OSINT Journal Review*, 17 set. 2014.

2 FARIA, José Augusto Vale. Como se Forma um Terrorista Jihadista no Ocidente: o Processo de Radicalização. Jornal de Defesa e Relações Internacionais, 2013. Faria aborda esses dois aspectos de transformação do terrorismo e suas consequências ao analisar vários atentados no período que antecede o estabelecimento do chamado "califado" na parte introdutória do artigo sobre o paradigma da propaganda terrorista e seus efeitos, cf. WINTER, Charlie. The Virtual 'Caliphate': Understanding Islamic State´s Propaganda Strategy. Quilliam, 2015.

3 Cf FARIA, *op. cit.*, p. 3. A publicação *"Lone Mujahid Pocketbook"*, em 2013, produzida pela Al-Qaeda da Península Ibérica e divulgada pela revista extremista *Inspire,* com o subtítulo *Easy & Safe Irhab – Simple Operations,* apresentou uma compilação de técnicas simples para serem utilizadas em ataques terroristas e para comunicação segura, e ilustra bem esse período de redirecionamento do terrorismo internacional.

preso na primeira grande operação de contraterrorismo brasileira baseada na lei que disciplinou o crime de terrorismo no Brasil (Lei nº 13.260/2016), a Operação Hashtag da Polícia Federal (PF). Essa operação foi acompanhada, nos meses e anos subsequentes, de outras ações policiais, denúncias do Ministério Público Federal (MPF) e sentenças judiciais de primeira e segunda instâncias, que levaram à prisão dezenas de indivíduos envolvidos com o terrorismo no país.

Apesar de o repúdio ao terrorismo ser previsto desde 1988 na Constituição Federal de 1988 (CF/1988) (art. 4º, inc. VIII), o crime de terrorismo só veio a ser tipificado no Brasil em 16 de março de 2016, com a Lei Federal nº 13.260, não obstante as pressões internacionais ao longo desses anos para que o país adotasse medidas mais concretas no enfrentamento do fenômeno[4]. Desde então, outros importantes instrumentos legais têm inserido o tema de enfrentamento do terrorismo entre as prioridades das agendas de segurança, política externa, defesa e Inteligência brasileiras, como são exemplos as promulgações da Política Nacional de Inteligência (PNI), em 2016, e da Estratégia Nacional de Inteligência (Enint), em 2017[5].

O presente trabalho objetiva analisar a estrutura de enfrentamento do terrorismo no Brasil, ao considerar avanços legais alcançados e competências institucionais estabelecidas, além das implicações desses avanços no contexto de inserção daquele fenômeno transnacional na conjuntura interna do país. Adotou-se, como estratégia metodológica, estudo de atos normativos (estrutura, competências e atribuições legais) e revisão bibliográfica das principais pesquisas a respeito de processos de radicalização, de forma a estabelecer um referencial teórico que auxilie a análise de casos já identificados no Brasil para, por fim, avaliar a eficácia e a efetividade de enfrentamento das ameaças à luz da legislação vigente.

Este artigo está divido em três partes. A primeira aborda a estrutura legal e orgânica de prevenção e repressão do terrorismo, e busca estabelecer uma visão sistêmica de competências institucionais, com enfoque nos eixos de segurança e Inteligência. Na segunda parte, são tratados pontos da Lei nº 13.260/2016 julgados mais importantes para o trabalho preventivo e repressivo do contraterrorismo, é analisada a efetividade de sua aplicação em casos concretos e consideram-se os principais estudos sobre

4 Cf. SANTOS, R. F. LEGISLAÇÃO CONTRATERRORISTA DO BRASIL E SEUS LIMITES PARA A ATIVIDADE DE PREVENÇÃO: O papel da Atividade de Inteligência. TCC – Curso de Aperfeiçoamento em Inteligência. ABIN, 2017. Sobre a formação da estrutura legal de enfrentamento do terrorismo no Brasil, ver capítulo "Considerações Iniciais".

5 Importa mencionar as resoluções do Conselho de Segurança de Organização das Nações Unidas (ONU) e as recomendações do Grupo de Ação Financeira Internacional (GAFI) que, há anos, compõem os compromissos internacionais imperativos do Brasil. Como exemplo mais recente, pode-se citar o Decreto nº 9457/2018, sobre tema de grande relevância e considerável impacto para o Brasil, que deu publicidade e determinou o integral cumprimento da Resolução nº 2.396/2017, do Conselho de Segurança de Segurança da ONU, que, ao tratar das ameaças representadas pelos combatentes terroristas estrangeiros, enfatiza a responsabilidade dos Estados-Membros e os necessários esforços coletivos, nos níveis nacional, regional e internacional, para o enfrentamento do terrorismo, e reafirma, em seu corpo, uma série de diretrizes e compromissos que atentam para o aspecto fenomenológico do tema.

processos de radicalização. Por fim, algumas conclusões são apresentadas a partir das principais abordagens exploradas nos tópicos anteriores, a exemplo de pontos positivos e negativos do atual cenário e de novos desafios para o Brasil no combate ao terrorismo transnacional.

Base conceitual: duas dimensões do tema terrorismo

A estrutura de contraterrorismo no Brasil pode ser analisada sob duas perspectivas do tema: o enfrentamento do terrorismo como fenômeno e ameaça transnacional, assunto de acompanhamento prioritário da Inteligência brasileira; e o combate ao terrorismo como ilícito tipificado por lei, por meio de ações de investigação e repressão por parte das autoridades competentes (SANTOS , 2017). As atividades de Inteligência e de segurança relacionadas ao contraterrorismo são complementares e possuem papéis definidos no ordenamento jurídico brasileiro.

Sobre o terrorismo como tema securitário, os Estados devem fazer frente à ameaça interna por meio da implementação, em seu ordenamento jurídico, de uma estrutura que possibilite sua adequada criminalização e ofereça instrumentos investigativos e persecutórios apropriados à gravidade da ameaça, em consonância com os esforços internacionais de combate ao fenômeno. A Resolução 1.373 (2001) do Conselho de Segurança da Organização das Nações Unidas (ONU) determinou que "todos os Estados assegurem a persecução penal de toda pessoa que participe no financiamento, planejamento, preparação ou perpetração de atos terroristas ou preste apoio a esses atos". Já a Resolução 2.178 (2014) estabeleceu que todos os Estados-Membros se assegurem de que seu direito interno estabeleça como crimes graves certas condutas ligadas ao financiamento, ao planejamento, à preparação ou à perpetração de atos terroristas, suficientes para permitir a persecução penal, de forma que as penas reflitam devidamente a gravidade do delito.

Portanto, a criminalização do terrorismo atende às funções persecutória e repressiva da legislação de cada país frente à ameaça interna, que deve conferir ao crime, inclusive, tratamento especial mais gravoso, e refletir, no direito pátrio, a seriedade da conduta. No caso brasileiro, a Lei nº 13.260/2016 criminaliza o terrorismo e outras condutas correlatas com tratamento especial rigoroso, conforme preceituado pela CF/1988, que equipara as respectivas sanções às dos crimes hediondos, cujas penas se iniciam sempre com o regime prisional fechado.

Já o eventual efeito preventivo da criminalização do terrorismo residiria na capacidade intimidadora e dissuasória das penas (como dito, mais rigorosas) e da ampla capacidade persecutória e processual dos órgãos competentes conferidas pela lei. Tal efeito em relação ao terrorismo seria, entretanto, relativo, uma vez que os processos de radicalização resultam, muitas vezes, em uma verdadeira ressignificação de valores e profunda transformação cognitiva por parte dos indivíduos radicalizados, que, eventualmente, passam a entender a violência como moralmente aceitável ou mesmo necessária (SANTOS, 2017).

O terrorismo como fenômeno e ameaça à paz e à segurança internacionais, por sua vez, possui componentes políticos e sociológicos que vão além do crime em si, seja praticado por indivíduos seja por grupos. Para Roberto Santos (2017, p. 6),

> O fenômeno do terrorismo transcende a esfera da conduta puramente interna que merece intervenção penal somente quando afeta terceiros. O Estado necessita intervir no fenômeno muito antes da ação ser externada. O processo de deterioração das relações sociais e da corrosão das instituições políticas e da ressignificação de elementos morais para a execução de uma ação violenta necessita de monitoramento e de intervenção do Estado em fases muito anteriores à exteriorização da conduta.

De acordo com definição de Newman (2017), o extremismo pode ser usado para se referir a ideologias políticas que se opõem aos valores e princípios centrais de uma sociedade. Já Borum (2011) afirma que a radicalização a partir da adoção ou do desenvolvimento de ideias extremistas que justificam a violência é apenas um dos caminhos que podem levar ao terrorismo. Segundo esse autor, as políticas e práticas que visam a mitigar e prevenir a propagação do extremismo violento requerem a compreensão dessas variações e não apenas "tendências gerais".

Nesse contexto, o estudo do processo de radicalização que conduz à violência e do extremismo violento que conduz ao terrorismo[6] desempenha papel essencial no processo de enfrentamento do fenômeno e deve ser prioridade da Inteligência de Estado. Segundo Roberto Santos (2017, p. 9),

> A principal maneira de se prevenir o terrorismo é por meio do conhecimento das causas do fenômeno, de como ele se desenvolve e de como os indivíduos ou grupos assumem ideais radicais e preparam e executam um ato violento. A partir desses conhecimentos é possível antecipar as ações e permitir que se atue para reduzir as causas e desmobilizar e conter pessoas ou grupos. Para tanto, a atividade de inteligência cumpre papel central na atividade de prevenção do terrorismo.

Além dos estudos do processo da radicalização, do ponto de vista individual ou coletivo, uma série de aspectos que circundam o terrorismo como fenômeno devem ser trabalhados pela Inteligência. Disso são exemplos as dinâmicas sociais migratórias e as implicações humanitárias resultantes do terrorismo internacional, a avaliação e o acompanhamento da ameaça representada pelos combatentes terroristas estrangeiros *(foreign fighters)* ou a possibilidade de uso da condição de refugiados por terroristas, a análise das estruturas de financiamento e do *modus operandi* de grupos terroristas, a produção de análises de riscos e a identificação de ambientes e comunidades vulneráveis a processos de radicalização.

A responsabilidade do Estado no

6 Sobre as terminologias utilizadas na relação do processo de radicalização com o extremismo violento ou terrorismo, a Organização das Nações Unidas costuma utilizar a terminologia "extremismo violento que conduz ao terrorismo" [violent extremism conducive to terrorism], também utilizado pelo Professor Peter Neumann – cf. NEUMANN, P. R. *Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region.* Organization for Security and Co-operation in Europe, 2017. Já o pesquisador Randy Borum (BORUM, R., *op. cit.*) trabalha o termo em inglês "radicalization into violent extremism", ou a forma abreviada "RVE".

enfrentamento do terrorismo como fenômeno político e social, portanto, envolve ações efetivas sobre toda a complexidade e a amplitude do tema, que se inicia muito antes da radicalização de um indivíduo ou da formação de um grupo terrorista, e atua em questões que vão, no espaço e no tempo, além da materialização do crime em si.

A estrutura legal e orgânica de enfrentamento do terrorismo no Brasil

A CF/1988 estabelece, em seu art. 4º, inc. VIII, que, em suas relações internacionais, a República Federativa do Brasil rege-se pelo princípio de repúdio ao terrorismo, e, no art. 5º, inc. XLIII, determina que o terrorismo é um crime inafiançável e insuscetível de graça ou anistia, e deixa à lei infraconstitucional sua regulamentação.

Além desses dois dispositivos que abordam diretamente o tema e dos tratados e convenções internacionais ratificados pelo Brasil, a CF/1988 estabelece princípios que fundamentam direta ou indiretamente a atuação estatal no enfrentamento do terrorismo. Encontra-se, nos artigos 3º a 5º da Carta Magna, uma base de fundamentos legais que versam sobre a garantia de direitos individuais e sociais, a proteção à liberdade, à segurança, além de garantias contra atos de preconceitos e discriminações, à inviolabilidade de consciência de crença, ao livre exercício de cultos, entre outros[7].

Percebe-se, assim, que o terrorismo está inserido na Constituição não apenas como um crime que pressupõe tratamento especial, mas também como um fenômeno internacional de caráter mais abrangente, que atinge princípios, direitos e garantias constitucionais fundamentais, e afronta diretamente a paz e a segurança do Estado e da sociedade.

A CF/1988 abriu espaço para a legislação infraconstitucional regular as medidas e os mecanismos estatais necessários às adequadas prevenção e repressão do terrorismo no Brasil, com toda a seriedade e todo o rigor que o assunto demanda, com atenção aos princípios e garantias fundamentais e compromissos do direito internacional. Esse conjunto de instrumentos normativos (leis, decretos, políticas, estratégias etc.) forma a estrutura estatal de enfrentamento do terrorismo no Brasil no contexto dos eixos anteriormente tratados: Inteligência e Segurança.

A atuação no enfrentamento do terrorismo, sob a ótica da Inteligência, é responsabilidade de todo o Sistema Brasileiro de Inteligência

7 Citamos como exemplos: "o Estado Democrático se destina a assegurar direitos individuais e sociais, a liberdade, a segurança (...), como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos (...)" (CF/1988, Preâmbulo); o art. 3º, inc. IV, constitui como objetivo fundamental do Estado "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação"; o art. 4º também estabelece como princípios nas relações internacionais do país a prevalência dos direitos humanos, a defesa da paz e a cooperação entre os povos para o progresso da humanidade; e o art. 5º estabelece garantias fundamentais relativas à igualdade entre sexos, à livre manifestação do pensamento, à liberdade inviolável de consciência de crença, assegurando o livre exercício de cultos religiosos e liturgias.

(SISBIN)[8]. O SISBIN foi instituído pela Lei Federal nº 9.883, de 7 de dezembro de 1999, e regulamentado pelo Decreto Presidencial nº 4.376, de 13 de setembro de 2002. É composto por 38 órgãos federais, e seus integrantes são definidos pelo Presidente da República[9]. A atuação dos órgãos que compõem o SISBIN na temática terrorismo abrange a produção de conhecimentos sobre diversos aspectos do fenômeno, que pode envolver, p. ex., inteligência financeira, relações internacionais, defesa, segurança pública e controle aeroportuário e migratório.

A Política Nacional de Inteligência, instituída pelo Decreto Presidencial nº 8.793, de 29 de junho de 2016, é o documento de mais alto nível de orientação da atividade de Inteligência no país, e que define parâmetros e limites de atuação da atividade e de seus executores no âmbito do SISBIN. [10]São exemplos de órgãos do SISBIN que, na medida de suas atribuições institucionais, participam ativamente dos esforços de prevenção e combate do terrorismo e estão submetidos às diretrizes da PNI, a Receita Federal, a Polícia Federal, o Departamento Penitenciário Federal, as Forças Armadas, o Ministério das Relações Exteriores e o Conselho de Controle de Atividades Financeiras.

O SISBIN também conta com um instrumento norteador em nível estratégico, a Estratégia Nacional de Inteligência (ENINT). O terrorismo é listado tanto na PNI como na ENINT entre as 11 principais ameaças que "apresentam potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil". Conforme a PNI, a temática do terrorismo é área de especial interesse e de acompanhamento sistemático por parte da Inteligência em âmbito mundial.[11]

A ENINT define, ainda, uma lista de desafios da Inteligência e consequentes "Objetivos Estratégicos" a serem alcançados, seguido de orientações "que devem ser consideradas e adotadas, quando do desdobramento dos objetivos da ENINT no Plano Nacional de Inteligência, para garantir a atuação integrada e coordenada do SISBIN e a entrega de

8 Competência estabelecida pelo §1º do art. 2º da Lei Federal nº 9.883/1999, pelo art. 6º do Decreto nº 4.376/2002 e pelo item 6.6 da Política Nacional de Inteligência, estabelecida pelo Decreto nº 8.793/2016.

9 Art. 2º da Lei Federal nº 9.883/1999.

10 A proposta de concepção da PNI é assim apresentada em sua parte introdutória: "A Política Nacional de Inteligência (PNI), documento de mais alto nível de orientação da atividade de Inteligência no país, foi concebida em função dos valores e princípios fundamentais consagrados pela Constituição Federal, das obrigações decorrentes dos tratados, acordos e demais instrumentos internacionais de que o Brasil é parte, das condições de inserção internacional do país e de sua organização social, política e econômica."

11 PNI, item 6.6: Terrorismo (...) é uma ameaça à paz e à segurança dos Estados. O Brasil solidariza-se com os países diretamente afetados por este fenômeno, condena enfaticamente as ações terroristas e é signatário de todos os instrumentos internacionais sobre a matéria. Implementa as resoluções pertinentes do Conselho de Segurança da Organização das Nações Unidas. A temática é área de especial interesse e de acompanhamento sistemático por parte da Inteligência em âmbito mundial. A prevenção e o combate a ações terroristas e a seu financiamento, para evitar que ocorram em território nacional ou que este seja utilizado para a prática daquelas ações em outros países, somente serão possíveis se realizados de forma coordenada e compartilhada entre os serviços de Inteligência nacionais e internacionais e, em âmbito interno, em parceria com os demais órgãos envolvidos nas áreas de defesa e segurança.

resultados que impactem positivamente o Estado e a sociedade brasileira".[12]

A legislação infraconstitucional brasileira, por sua vez, instrumentalizou e conferiu amplos poderes aos órgãos competentes para a investigação e processamento criminal dos crimes relacionados ao terrorismo (promoção de grupos terroristas, recrutamento, financiamento, apoio logístico etc.), em cumprimento aos compromissos e acordos internacionais estabelecidos nos últimos anos sobre essa temática, como visto anteriormente. No aspecto da segurança interna e transnacional, o terrorismo como crime é tipificado pela Lei nº 13.260/2016, cujo art. 11 estabelece que os delitos nela previstos são praticados contra o interesse da União; portanto, cabe à Polícia Federal (PF) a persecução criminal, e à Justiça Federal, seu processamento e julgamento. A atuação de outros órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal também é possível mediante cooperação técnica, conforme o disposto no art. 3º, VIII da Lei nº 12.820/2013.

O Brasil possui, portanto, instrumentos normativos, na cadeia do ordenamento jurídico brasileiro, que direcionam a atividade de Inteligência quanto à análise e à prevenção do terrorismo internacional, e estruturam os mecanismos investigativos, processuais e jurídicos de repressão do ilícito. Além disso, um conjunto de desafios, objetivos estratégicos e orientações são expostos na PNI e na ENINT e direcionam toda atividade de Inteligência desenvolvida pelo SISBIN nos assuntos de interesse do Estado e da sociedade brasileira, dos quais o terrorismo figura entre as principais ameaças.

Alguns aspectos pontuais da lei penal que disciplina essa temática, entretanto, requerem uma análise mais atenta frente à realidade brasileira de enfretamento do terrorismo e à experiência já adquirida em casos concretos.

Tipificação do crime de terrorismo e aplicação da lei penal no Brasil

A Lei nº 13.260/2016 representou um importante marco regulatório na estrutura de enfrentamento do terrorismo no Brasil ao criminalizar o fenômeno, ameaça até então tratada apenas em seu viés Inteligência[13]. Assim, o nascimento da lei penal específica elevou a capacidade persecutória e repressiva do Estado, além de suprir uma pendência normativa entre os compromissos brasileiros frente à comunidade internacional.

A Lei Antiterrorismo foi sancionada em um momento crucial de ameaça interna, quando a Inteligência brasileira havia identificado e monitorava dezenas de indivíduos radicalizados meses antes das Olimpíadas Rio 2016 (A., THIAGO; O. AUGUSTO; S. ALLAN, 2017). Com a Lei nº 13.260/2016, esses indivíduos passaram a ser alvos de investigação policial pelo crime

12 ENINT, item 9.1, p. 31.

13 Há vários anos, o fenômeno do terrorismo tem sido acompanhado em nível estratégico e tático por diversos órgãos que compõem o SISBIN, como ABIN, DAT/PF, Ministério da Defesa, COAF, Receita Federal etc., conforme assuntos relacionados ao tema e às respectivas competências institucionais. Eventuais casos que envolviam ilícitos, como "apologia ao crime", ilícitos financeiros, ameaça, entre outros, eram investigados pelas polícias judiciárias estaduais ou federal, conforme a natureza do delito.

de terrorismo. Desde então, 25 brasileiros foram denunciados pelo MPF por crimes relacionados ao terrorismo internacional, nove deles já foram condenados em primeira instância, e oito, em segundo grau de jurisdição, cujas penas impostas foram superiores a cinco anos de reclusão[14]. As denúncias e condenações nos casos brasileiros envolveram uma série de crimes tipificados na Lei nº 13.260/2016, como o de atos preparatórios de terrorismo (art. 5º), recrutamento com o propósito de praticar atos de terrorismo (art. 5º, §1º, I, C/C §2º), promoção de organização terrorista (art. 3º), além de crimes correlatos não-ligados diretamente ao terrorismo, em especial o de associação criminosa (art. 288 do Código Penal).

À luz do art. 2º da Lei Antiterrorismo, a prática do crime de terrorismo no Brasil requer a combinação de, ao menos, um **ato**, entre os previstos na norma (art. 2º, § 1º), uma **razão** (xenofobia, discriminação ou preconceito de raça, cor, etnia e religião) e uma **finalidade** (provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública).[15]

A primeira implicação desse artigo para o contraterrorismo no Brasil é o de que ele restringe a abrangência de autoria do crime àqueles que o executam apenas por razão de xenofobia, discriminação ou preconceito (além da exceção expressa no art. 2º, § 2º)[16]. O legislador excluiu do tipo penal, p. ex., a motivação política, fator que historicamente possui intrínseca ligação com a definição de terrorismo (FREITAS, 2017). Em função dessa abordagem restritiva relacionada à razão do ato, certos grupos violentos que praticam ações muitas vezes consideradas pelo senso comum como terroristas não poderiam ser enquadrados nesse tipo penal[17].

Outro importante ponto da legislação antiterrorista é a própria definição de

14 MINISTÉRIO PÚBLICO FEDERAL. Denúncia Pública, Curitiba:PR, 2016.
MINISTÉRIO PÚBLICO FEDERAL. Denúncia Pública, Curitiba:PR, 2016.
MINISTÉRIO PÚBLICO FEDERAL. Denúncia Pública, Goiânia:GO, 2017.
JUSTIÇA FEDERAL. Ação Penal nº 5046863-67.2016.4.04.7000/PR, Evento 613 – Sentença- L. 14ªVara Federal de Curitiba. 2016.
JUSTIÇA FEDERAL. Processo nº 0001078-38.2017.4.01.3502/PR – Sentença- L. TRF 4ª Região. 2017.
JUSTIÇA FEDERAL. Apelação Criminal nº 5046863-67.2016.4.04.7000/PR, TRF 4ª Região. 2018.

15 O crime de terrorismo está definido na Lei nº 13.260/2016, nestes termos: "Art.2º. O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública".

16 Lei nº 13.260/2016, art. 2º, § 2º: O disposto neste artigo não se aplica à conduta individual ou coletiva de pessoas em manifestações políticas, movimentos sociais, sindicais, religiosos, de classe ou de categoria profissional, direcionados por propósitos sociais ou reivindicatórios, visando a contestar, criticar, protestar ou apoiar, com o objetivo de defender direitos, garantias e liberdades constitucionais, sem prejuízo da tipificação penal contida em lei.

17 Assim, não é possível, p. ex., uma ação terrorista praticada por uma facção criminosa cujas motivações dos atos envolvem, normalmente, finalidade de obtenção de lucro ou ganho político, pois eventual ato que venha a praticar de "provocar terror social" dificilmente seria executado por uma das razões especificadas na lei. Já eventuais organizações extremistas de matizes não religiosos, como grupos de extremistas xenófobos, poderiam eventualmente cometer o crime de terrorismo desde que praticassem um dos atos descritos na lei com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

"organização terrorista". A ementa da Lei nº 13.260/2016 e seu art. 1º trazem a informação de que ela reformula o conceito de organização terrorista. Tal conceito só é brevemente tratado no art. 19, quando determina a alteração do § 2º, art. 1º da Lei de Organização Criminosa (Lei 12.850/2013), cujos dispositivos passam a ser aplicados também "às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos".

Infere-se, portanto, que a definição legal de "organização terrorista" se resume a qualquer organização voltada para a prática do ato de terrorismo, que é o crime definido no art. 2º da Lei nº 13.260/2016[18]. Ou seja, qualquer organização formada com objetivos de praticar terrorismo, conforme definido em lei, sejam ligadas àquelas ou não, passam a ser consideradas uma organização terrorista para fins de aplicação da Lei Antiterrorismo e da Lei de Organização Criminosa[19]. Importante lembrar que a prática do ato de terrorismo, no entanto, consoante o art. 2º, independe de que este crime seja cometido por pessoas vinculadas a qualquer organização terrorista.

O Brasil, por outro lado, não adota uma lista própria de organizações que considera terrorista, como ocorre em outros países. Para o país, são consideradas terroristas, independentemente da interpretação legal contextual (como visto acima), apenas aquelas organizações assim classificadas em resoluções do Conselho de Segurança da ONU[20].

Além das definições de ato terrorista e organização terrorista, o ponto de maior destaque na Lei nº 13.260/2016, para fins de ações de enfrentamento do terrorismo no Brasil, é o ilícito tipificado no seu art. 3º, o de promoção de organização terrorista.[21]

Até a primeira decisão judicial baseada na Lei nº 13.260/2016, não se sabia qual interpretação jurídica seria dada ao tipo penal do art. 3º, uma vez que o núcleo centrado no verbo "promover" denota amplo campo conceitual (A., THIAGO; O. AUGUSTO; S. ALLAN, 2017). O juiz federal que julgou a primeira denúncia do caso "Hashtag", entretanto, dedicou grande parte de sua fundamentação a um estudo detalhado do significado do verbo "promover", dando-o, por fim, uma interpretação ampla. Assim, conforme a referida sentença, "promover" teria sentido equivalente ao de "difundir, fomentar, encorajar, estimular, impelir,

18 Na realidade, os atos de terrorismo estão elencados no § 1º do art. 2º da Lei nº 13.260/2016. Porém, é claro que esses atos não podem ser percebidos isoladamente como "atos terroristas" senão quando praticados no contexto do caput do artigo.

19 Entendemos que o termo organização, nesse caso, está atrelado à definição de "organização criminosa", que exige na sua composição os requisitos especificados no § 1º, art. 1º da Lei nº 12.850/2013 – associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.

20 Os vários grupos terroristas mencionados em resoluções da ONU podem ser resumidos àqueles vinculados à Al-Qaeda, Taliban ou Estado Islâmico.

21 Lei nº 13.260/2016, art. 3º: Promover, constituir, integrar ou prestar auxílio, pessoalmente ou por interposta pessoa, a organização terrorista: Pena – reclusão, de cinco a oito anos, e multa.

impulsionar, incentivar, instigar ou motivar organização terrorista".[22]

A inserção desse dispositivo normativo no contexto da promulgação da Lei nº 13.260/2016 alcançou importante momento da história do terrorismo internacional, principalmente a partir da formação do califado islâmico, quando a propaganda virtual do terrorismo ganhava sofisticação técnica e multilinguística, e desempenhava papel relevante no recrutamento de novos radicais, que se seduziam com a narrativa apelativa do terror e se dispunham a juntar-se ao grupo terrorista EI (VEILLEUX-LEPAGE , 2016). Essa realidade, como dito, atingiu jovens brasileiros pouco antes da promulgação da Lei Antiterrorismo. Muitos desse público possuíam pouco tempo de conversão e pouco vínculo de identidade com o Islã, e utilizaram as redes sociais como principal meio de troca de material extremista relacionado ao EI (A., THIAGO; O. AUGUSTO; S. ALLAN, 2017).

Nesse contexto, a interpretação jurídica quanto ao significado do verbo "promover" e sua aplicabilidade em casos concretos transformou o tipo penal do art. 3º da Lei nº 13.260/2016 em um importante instrumento no combate à ameaça difusa representada pela propaganda do terrorismo em ambiente cibernético no Brasil e, indubitavelmente, principal percursor de investigações e procedimentos criminais sobre o tema. Todos os indivíduos denunciados no Brasil por crimes relacionados ao terrorismo foram acusados desse delito, e as sentenças já proferidas até o momento, sejam em primeira ou segunda instâncias, mantiveram as condenações pelo crime de promoção de organização terrorista.

Promoção de grupos terroristas, processo de radicalização e efetividade das medidas preventivas e repressivas do Estado

O ato de promover organização terrorista, conforme interpretação do TRF-4[23], "não exige dano concreto", pois causa por si um grave dano potencial à sociedade e à comunidade internacional. A materialidade do crime, conforme interpretação jurídica brasileira[24], dá-se por meio da postagem de vídeos, fotos, mensagens de estimulação e materiais alusivos à organização terrorista ou da manifestação pública cujo discurso denote claro ato de difundir, fomentar, encorajar, estimular, impelir, impulsionar, incentivar, instigar ou motivar organização terrorista, e não há a necessidade de comprovação de especial fim de agir ou da presença de dolo

22 Sentença da ação Penal nº 5046863-67.2016.4.04.7000/PR, Evento 613, p. 22-28.

23 JUSTIÇA FEDERAL. Processo nº 0001078-38.2017.4.01.3502/PR – Sentença- L. TRF 4ª Região. 2017.

24 Conforme sentença da ação Penal nº 5046863-67.2016.4.04.7000/PR, Evento 613, p. 29, segundo fundamentação do juiz federal que julgou o caso Hashtag, "...não há necessidade de comprovação de especial fim de agir ou da presença de dolo específico, bastando o simples ato de promover organização terrorista por meio de atos inequívocos que demonstrem externamente a adesão aos seus ideais e a sua respectiva externalização voluntária".

específico.[25]

Assim, o crime de promoção, no complexo contexto em que se dá a manifestação do terrorismo, guarda pouca relação com a ameaça objetiva que um indivíduo oferece à sociedade quanto a sua capacidade e a sua propensão de cometimento de uma ação violenta ou disposição para a prática de um ato de terrorismo. Tampouco guarda relação direta com o grau de radicalização do indivíduo, mas sim com a forma e a quantidade de material e discurso radical que ele compartilha, pois não é possível precisar o nível de ameaça representada por determinado indivíduo a partir unicamente da análise de seu discurso radical nas redes sociais, não obstante, claro, essa análise seja importante na percepção da ameaça em si. A análise da ameaça objetiva que o indivíduo radical representa requer acompanhamento e avaliação sistemática de sua trajetória de radicalização.

O processo de radicalização não determina uma trajetória necessariamente linear, nem há uma métrica específica que aponte níveis de radicalização (BORUM, 2013). Muitas vezes, o fenômeno da radicalização se manifesta a partir de condicionantes estocásticas, dependentes do ambiente onde se desenvolvem e do contexto histórico e psicossocial do indivíduo[26]. As várias iniciativas na literatura de se delinear um processo-padrão ou métricas de radicalização têm se mostrado infrutíferas ou estão restritas a recortes regionais que, normalmente, não podem ser integralmente aplicadas em outro contexto espacial ou temporal[27]. Porém, fatores de influência de caráter individual, ambiental e relacional são percebidas de forma semelhante na maioria dos casos de radicalização.

Scott Atran (2016), a partir de várias entrevistas realizadas e experimentos comportamentais com jovens radicais e terroristas do EI capturados, buscou identificar fatores de influência individuais atuantes no processo de radicalização desses indivíduos. Atran afirmou, p. ex., que os principais jovens que se voluntariavam para lutar até a morte pela causa do EI sentiam "um prazer que vem da alegria de fazer parte, junto com os companheiros, em uma causa gloriosa, bem como da alegria que vem em saciar a raiva e da gratificação pela vingança".[28]

A análise dos processos de radicalização

25 Consideramos, nessa análise, apenas as situações em que o núcleo do ilícito é o verbo "promover", porque o mesmo artigo também trata de "constituir", "integrar" e "prestar auxílio", ações que denotam ligação com organizações terroristas com componentes de maior pessoalidade do que a mera promoção.

26 SCHMID, A. P., *op. cit.*, aborda causas individuais, sociais e políticos na análise do processo de radicalização e utiliza a classificação de causas nos níveis micro, meso e macro.

27 SCHMID, A. P., *op. cit.*, p. 38. Pinker (2011, p. 357), ao analisar estudos do antropólogo Scott Atran, afirmou que "...provavelmente, o apelo mais eficaz no recrutamento é a oportunidade de se juntar a uma irmandade feliz. As células terroristas geralmente começam como gangues de jovens solteiros subempregados que se reúnem em cafés, dormitórios, (...) ou salas de bate-papo na Internet e, de repente, acham significado para suas vidas no compromisso com um novo pelotão."

28 *[The mainly young people who volunteer to fight for it unto death feel a joy that comes from joining with comrades in a glorious cause, as well as a joy that comes from satiation of anger and the gratification of revenge (whose sweetness, says science, can be experienced by brain and body much like other forms of happiness)].*

dos jovens brasileiros envolvidos com o terrorismo em 2015 e 2016, por usa vez, indicam similitudes com as avaliações de Pinker e Atran, porém em um contexto político-social próprio. Dificuldades de inserção social em ambientes religiosos, distanciamento familiar, desemprego, necessidade de pertencimento, contexto político e social do país, carências, rupturas e isolamento social associados à imersão no mundo virtual e necessidade de autoafirmação, são alguns dos fatores de influência identificados nos casos brasileiros (A., THIAGO; O. AUGUSTO; S. ALLAN, 2017).

O ambiente de convivência social dos indivíduos também pode atuar de forma determinante no processo de radicalização. Fragilidades pessoais circunstanciais associadas à socialização e ao acolhimento do indivíduo por parte de um grupo (irmandade), além do prazer proporcionado no sentimento de pertencer a uma causa ou propósito, são elementos que normalmente caracterizam ambientes "incubadores de radicais"[29]. Nesses ambientes, sejam virtuais (redes sociais, fóruns de discursão, grupos de aplicativos de mensagerias etc.) ou físicos (grupos de estudos, salas de oração, presídios etc.), a postura, a exposição do pensamento e o discurso do indivíduo determinam sua aceitação e sua posição social perante o grupo. Novos integrantes, além daqueles que buscam aceitação ou determinado posicionamento em um grupo social, naturalmente demonstram-se mais entusiasmados e se expõem mais na tentativa de valorizar seu *status* perante os demais membros. Para isso, o discurso violento e o compartilhamento de material extremista são opções usualmente utilizadas no processo de autoafirmação desses indivíduos perante o grupo.

Nos ambientes incubadores, são identificados diferentes papeis que exercem influência nos processos de radicalização. Neles não atuam apenas jovens imaturos, seduzidos pelo ideal radical e entusiasmados com o discurso violento dos grupos terroristas. Diferentes funções são desempenhadas nas interações entre membros de grupos sociais e destes com outros atores externos, o que estrutura uma complexa cadeia que caracteriza os processos de radicalização. Diversos atores podem atuar, direta ou indiretamente, conscientes ou não, em processos de influência, doutrinação, difusão do pensamento radical ou recrutamento. Esses papeis podem ser identificados e representados de diferentes formas por meio de modelos analíticos e dependem de contextos regionais e temporais nos quais se dá o processo[30].

A forma como se dá a interação dos atores é que constrói a dinâmica de ambientes incubadores de radicais, e o acompanhamento atento desse processo

29 Cf. FARIA, *op. cit.*; BORUM, R., *op. cit.*, sobre a aplicação de teorias e modelos analíticos de ciências socais no estudo sobre processos de radicalização.

30 Caso analisado a partir dos indivíduos radicalizados no período anterior às Olimpíadas Rio 2016, Thiago A., Augusto O. e Allan S. (2017, p. 14-15) apontou papeis atuantes em diferentes níveis relacionados a processos de radicalização que podem ser resumidos em duas categorias: aqueles com mais conhecimento do ideal radical, que exercem influência ideológica sobre os demais (doutrinam e difundem o pensamento), e aqueles influenciáveis, normalmente mais imaturos, curiosos e dinâmicos (promovem e executam).

é o que possibilita a identificação pela atividade preventiva da Inteligência do importante momento em que ocorrem os principais pontos de inflexão que conduzem o aspirante a radical a extremista violento (indicadores de radicalização)[31]. Destacam-se, entre esses pontos de inflexão, o momento em que o indivíduo demostra abertura cognitiva ao discurso radical, apresenta comportamentos que indicam alteração de sua percepção moral a respeito do uso da violência (inversão de moralidade) ou pratica atos que sugerem fase inicial de mobilização para ação extremista.

Portanto, diante da complexidade que envolve o acompanhamento de processos de radicalização, a avaliação da ameaça real, seja na detecção de indivíduos radicalizados e dispostos a alguma ação extremista ou daqueles que conduzem processos de radicalização, requer observação criteriosa, sistemática e pontual de aspectos psicológicos, sociais e políticos. O resultado desse processo pode, inclusive, identificar que a realidade cognitiva de um determinado indivíduo radicalizado, seu potencial de propensão à violência e sua real capacidade de atuação sejam completamente diferentes da imagem social (avatar) que ele projeta para o grupo ou para si mesmo por meio de seu discurso público.

Avalia-se, assim, que a atuação preventiva do Estado com base na repressão imposta pelo crime de promoção de organização terrorista (art. 3º da Lei nº 13.260/2016), apesar de eficiente no combate à ameaça difusa imposta pela propaganda terrorista, possui mínima eficiência como mecanismo neutralizador sobre ameaças objetivas impostas pelos atores envolvidos em processos de radicalização[32]. Mesmo eventual efeito intimidador e dissuasório do rigor punitivo da lei, como abordado anteriormente, tem aplicabilidade bastante restrita frente à natureza da ameaça imposta por indivíduos imbuídos em causas ideológicas e religiosas, para os quais a ação violenta é um importante caminho para alcançar um bem pessoal e coletivo maior. Terrorista não age ilegalmente entendendo que seja errado, age achando que é certo.

A prevenção do terrorismo como fenômeno, portanto, não pode se restringir apenas à aplicação da lei penal, que, como visto, possui diversas limitações quanto a sua eficiência em alcançar toda a complexidade da ameaça. Requer, além disso, uma sincronia de ações diversas de Inteligência, seja policial, de defesa ou de Estado, na busca pela identificação de ambientes vulneráveis, análise do discurso radical em seu contexto político-social, avaliação de níveis de radicalização e ameaças potenciais,

31 Vários modelos analíticos que trabalham fases do processo de radicalização e apontam pontos de inversão já foram propostos e são utilizados academicamente e por serviços de Inteligência ou policiais. Trabalhar com um modelo específico fugiria do escopo deste ensaio. Cf. FARIA, *op. cit.*, p. 13-28; SHMID, A. P., *op. cit.*, p. 23-25.

32 Importante lembrar que a organização terrorista, objeto da "promoção", deve ser uma daquelas já reconhecidas pelo Brasil, que, como visto anteriormente, restringem-se às de matiz religioso islâmico definidas em resoluções do Conselho de Segurança da ONU (Al-Qaeda, Taliban ou EI). Portanto, indivíduos que compartilham material radical ou violento e que não estejam associados a uma dessas organizações não poderiam ser alvos de investigação com base apenas nesse artigo. Além disso, a aplicabilidade desse tipo penal fica restrita a detecções de indivíduos que atuam com maior espontaneidade, comumente entre os mais imaturos, e, muitas vezes, não alcança atores mais importantes na cadeia da radicalização.

identificação de fatores de influência, atores e papéis desempenhados em processos de radicalização.

Ainda assim, essas ações aproximam-se do campo de atuação estatal do que tradicionalmente se denomina "contraterrorismo", ou seja, medidas direcionadas à identificação de ameaças e neutralização de organizações terroristas, que, em praticamente todos os países, é responsabilidade primária dos órgãos de segurança, de Inteligência e, em alguns casos, militares (NEUMANN, 2017). O contraterrorismo, conforme aponta o professor Peter R. Neumann, é o pilar central do esforço estatal no combate ao extremismo violento e, quando eficientemente empregado, não apenas ajuda na prevenção de ataques e na proteção de vidas, mas também na integridade dos Estados e de suas instituições. Entretanto, segundo o autor, em situações em que a ameaça se apresenta mais fragmentada e persistente, o contraterrorismo, muitas vezes, mostra-se inadequado e falha em impedir processos de radicalização por não alcançar seus percursores políticos, econômicos e sociais (NEUMANN, 2017).

Já o conceito relacionado ao termo "prevenção do extremismo violento", amplamente utilizado nos últimos anos no meio acadêmico e por diversos governos, diferentemente de "contraterrorismo", foca não no terrorismo em si, mas na prevenção dos processos de radicalização. O "contra-extremismo violento", como argumenta Neumann, não envolve processos, prisões ou uso da força, mas busca mobilizar diferentes atores não tradicionalmente associados às forças de segurança, como governos locais, pequenas comunidades, educadores, sociedade civil etc., para promover resiliência entre a população vulnerável e ajudar indivíduos suscetíveis a processos de radicalização (NEUMANN, 2017, p. 20).

Considerações finais

O terrorismo no Brasil é tratado como ilícito equiparado aos crimes hediondos e considerado uma ameaça de acompanhamento prioritário nas relações internacionais e na agenda da Inteligência de Estado[33]. A estrutura legal, preventiva e persecutória do terrorismo como crime e ameaça interna brasileira tem sido exitosa na identificação, na investigação, no indiciamento criminal, na denúncia e na condenação de diversos indivíduos envolvidos com o ilícito.

Desde a promulgação da Lei Antiterrorismo, já ocorreram diversas experiências de neutralização de ameaças por operações da PF, que geraram dezenas de indivíduos indiciados, denunciados e condenados por crimes relacionados ao terrorismo. Ao se considerar a atuação de Inteligência em momentos anteriores ao início da investigação criminal (na identificação de extremistas e pontos de vulnerabilidade de radicalização), há, no Brasil, importantes exemplos do fechamento do ciclo de atuação dos órgãos públicos responsáveis pela prevenção do terrorismo, que se inicia

33 Art. 4º, VIII e art. 5º, XLIII da CF/88; PNI – 6. Principais Ameaças; ENINT – 6.1 Ameaças.

com a atividade de Inteligência[34] e termina com a neutralização da ameaça e a punição dos autores com as devidas condenações judiciais.

Entretanto, a principal base legal de persecução penal, processo e punição no ordenamento jurídico brasileiro, que é o tipo penal "promoção de organização terrorista", apesar de sua eficiência no combate difuso da propaganda extremista, mostra-se insuficientemente eficaz como instrumento de detecção e prevenção de ameaças pontuais e objetivas, função que depende de técnicas e métodos da atividade de Inteligência. Assim, para se fazer frente a toda a complexa cadeia de ameaças que envolve o terrorismo como fenômeno transnacional, é necessário um trabalho orquestrado entre diversos atores do aparato preventivo e repressivo da estrutura de enfrentamento do terrorismo no Brasil.

O fenômeno do terrorismo tem passado por vários ciclos ao longo da história. Recentemente, o mundo acompanhou importantes transformações na dinâmica do terrorismo internacional, adaptado à era da informação, em que o EI e o estabelecimento do califado islâmico foram os protagonistas. Com o fim do califado islâmico e considerável diminuição da ameaça direta representada pelo EI, porém, há uma nova redefinição na dinâmica do terrorismo internacional, que desafia os órgãos de Inteligência e Segurança. Novos temas passam a ganhar mais importância, a exemplo de processos de radicalização no sistema penitenciário, dinâmicas sociais migratórias e implicações humanitárias, ameaça representada pelos combatentes terroristas estrangeiros e a possibilidade de infiltração de terroristas em grupos de refugiados e novas dinâmicas de financiamento do terrorismo. Além disso, percebe-se o recrudescimento das ações de indivíduos radicais e grupos extremistas violentos de matizes não-religiosos que têm utilizado os mesmos modos simplificados das ações de grupos terroristas tradicionais.

Ao se considerar as novas perspectivas da ameaça e a experiência brasileira nos últimos anos, a atuação conjunta, colaborativa e sincronizada do aparato estatal e da sociedade civil – direcionada por políticas de prevenção estruturadas e eficientes, que possam combater não apenas a ponta do *iceberg* que se materializa no terrorismo, mas também atuar efetivamente na mitigação da complexa e, muitas vezes, pouco perceptível raiz do extremismo violento – resume o profundo desafio dos Estados e deve ser o principal objetivo por parte dos órgãos que compõem o SISBIN no combate ao terrorismo transnacional.

34 A atuação da Inteligência aqui pode envolver, tanto no nível tático como estratégico, vários órgãos do SISBIN em esforço conjunto na detecção de ameaças. Estas podem surgir, p. ex., a partir de um trabalho de Inteligência policial ou financeira com foco em crime organizado, ou de colaboradores com acessos as comunidades virtuais. Importante, entretanto, destacar o delicado e rico debate em torno da transição entre Inteligência e investigação criminal e aspectos peculiares à atividade de Inteligência policial, segundo doutrina específica (que não é o foco deste trabalho). O tema já é bastante explorado na literatura especializada e em trabalhos acadêmicos. Para aprofundamentos sugerimos como ponto de partida: ANDRADE, Felipe S. de. Inteligência Policial: Efeitos das Distorções no Entendimento e na Aplicação. *Revista Brasileira de Ciências Políticas,* 2012; e KRAEMER, Rodrigo. Incompreensão do Conceito de Inteligência na Segurança Pública. *Revista Brasileira de Inteligência,* Brasília: Abin, v. 10, 2015.

Referências

ALY, A.; WEIMANN-SAKS, D.; WEIMANN, G. Making 'Noise' Online: An Analysis of the Say No to Terror Online Campaign. *Perspectives on Terrorism,* v. 8, n.5, p. 33 – 47, 2014.

A., Thiago; O. Augusto; S. Allan. O Processo de Radicalização e a Ameaça Terrorista no Contexto Brasileiro a Partir da Operação Hashtag. *Revista Brasileira de Inteligência,* Brasília: Abin, v.12, p. 7-20, 2017.

ATRAN, Scott. *Talking to the Enemy: Sacred Values, Violent Extremism, and What it Means to be Human.* Penguin Group, 2011.

ATRAN, Scott. ISIS is a Revolution. *AEON*, Pam Weintraub, 2016. Disponível em: https://aeon.co/essays/why-isis-has-the-potential-to-be-a-world-altering-revolution.

BEAUCHAMP, Zach. Isis, islamic state or ISIL? What to call the group the US is bombing in Iraq. *OSINT Journal Review*, 17 set. 2014.

BORUM, R. Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security,* Tampa – Florida, v. 4, n. 4, Article 2, 2011.

BORUM, R. Radicalization into Violent Extremism II- A Review of Conceptual Models and Empirical Research. *Journal of Strategic Security,* Tampa – Florida, v. 4, n. 4, Article 3, p. 37-62, winter 2011.

CUNHA, Ciro Leal M. da. *Terrorismo internacional e a política externa brasileira após o 11 de setembro.* 2009. Dissertação (Mestrado em Diplomacia do IRBr, 2004-2005), - Instituto Rio Branco, Fundação Alexandre de Gusmão. Brasília, 2009.

DEGAUT, Marcos. The Threat of Terrorism Hangs Over Brazil. *Harvard International Review,* 2014. Disponível em: http://hir.harvard.edu/article/?a=7569.

FARIA, José Augusto Vale. Como se Forma um Terrorista Jihadista no Ocidente: o Processo de Radicalização. *Jornal de Defesa e Relações Internacionais*, 2013.

FREITAS, Verônica Tavares de. *A Lei Antiterror como reforço do Estado punitivo no Brasil.* In: Grupo de Trabalho 40: Violência, Polícia e Justiça no Brasil: Agenda de pesquisa e desafios teóricos – metodológicos 18º Congresso Brasileiro de Sociologia. Brasília, 2017.

HASHIM, Ahmed S. The Islamic State: from Al-Qaeda affiliate to Caliphate. *Middle East Policy,* v. 21, n. 4, p. 69-83, 2014.

NEUMANN, P. R. *Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region.* London: Organization for Security and Co-operation in Europe, International Centre for the Study of Radicalisation, 2017. Disponível em: https://www.osce.org/chairmanship/346841?download=true.

PINKER, S. *The Better Angels of Our Nature:* Why Violence Has Declined. Viking Press, 2011.

SANTOS, R. F. *Legislação contraterrorista do Brasil e seus limites para a atividade de prevenção:* O papel da Atividade de Inteligência. 2017. Trabalho de Conclusão de Curso (Curso de Aperfeiçoamento em Inteligência) – Esint/Abin, Brasília, 2017.

SCHMID, A. P. Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. *International Centre for Counter-Terrorism, 2013.*

VEILLEUX-LEPAGE, Yannick. *Paradigmatic Shifts in Jihadism in Cyberspace: The Emerging Role of Unaffiliated Sympathizers in the Islamic State's Social Media Strategy.* The Handa Centre for the Study of Terrorism and Political Violence, 2016.

WINTER, Charlie. *The Virtual 'Caliphate':* Understanding Islamic State´s Propaganda Strategy. Quilliam, 2015.

Peças jurídicas consultadas:

BRASIL. Ministério Público Federal. Denúncia Pública, Curitiba: PR, 2016. Disponível em: http://www.mpf.mp.br/pr/sala-de-imprensa/docs/denuncia-hashtag/. Acesso em: 27 ago. 2018.

BRASIL. Ministério Público Federal. Denúncia Pública, Curitiba:PR, 2016. Disponível em: http://www.mpf.mp.br/pr/sala-de-imprensa/docs/denunciahashtag2.pdf/. Acesso em: 27 ago. 2018.

BRASIL. Ministério Público Federal. Denúncia Pública, Goiânia:GO, 2017. Disponível em: https://s3-sa-east-1.amazonaws.com/nexojornal/www/docs/IPL-Denuncia-12395-39.2017-terrorismo-bmf.pdf. Acesso em: 27 ago. 2018.

BRASIL. Justiça Federal. Ação Penal nº 5046863-67.2016.4.04.7000/PR, Evento 613 – Sentença- L. 14ª Vara Federal de Curitiba. 2016.

BRASIL. Justiça Federal. Processo Nº 0001078-38.2017.4.01.3502/PR – Sentença- L. TRF 4ª Região. 2017. Disponível em: https://portal6.com.br/wp-content/uploads/2017/06/f16334b23756999df7c3763a13ebe2c2.pdf. Acesso em: 27 ago. 2018.

BRASIL. Justiça Federal. Apelação Criminal Nº 5046863-67.2016.4.04.7000/PR, TRF 4ª Região. 2018. Disponível em: https://trf-4.jusbrasil.com.br/jurisprudencia/612016868/apelacao-criminal-acr-50468636720164047000-pr-5046863-6720164047000/inteiro-teor-612016899?ref=serp. Acesso em: 27 ago. 2018.

PANORAMA DA AMEAÇA CIBERNÉTICA À AVIAÇÃO CIVIL

Mateus Vidal Alves Silva *

Resumo

O artigo apresenta abordagem inicial da ameaça de ataque cibernético à aviação civil, sob a ótica conceitual da inteligência da aviação civil. Formulou-se o seguinte problema de pesquisa: quais os parâmetros essenciais para estruturar um panorama da ameaça cibernética como fenômeno que interage e desafia a inteligência da aviação civil? A metodologia propõe pesquisa básica, exploratória e qualitativa, mediante revisão da literatura, utilizada para delinear os marcos teórico-conceituais, as estruturas, as análises e a casuística. A Política Nacional de Inteligência (PNI) destaca a ameaça cibernética, com crescimento exponencial e ampla gama de alvos elegíveis e interconectados. É ameaça assimétrica dinâmica, que apresenta múltiplos formatos e atores possíveis e tem potencial de danificar ativos e infraestruturas críticas. A aviação civil é alvo recorrente de interferências ilícitas. Nessa área, a ameaça cibernética é real e poderia resultar em episódio classificável como "cisne negro", nos moldes dos ataques terroristas de 11 de setembro de 2001. Ao abordar a ameaça de ataque cibernético à aviação civil contemplam-se os conceitos aplicáveis, o estado da arte da inteligência da aviação civil, a irrefutabilidade de possíveis falhas, os alvos potenciais, as categorias de atores e suas motivações, a capacidade de agir e os possíveis métodos de ataque. As considerações finais apontam para a possibilidade de evoluções intermediadas por uma política de mitigação de riscos relacionados à ameaça cibernética na aviação civil subsidiada por análises estruturadas de inteligência.

Palavras-chaves: ameaças, ataque cibernético, aviação civil, inteligência da aviação civil, infraestruturas críticas.

A PANORAMA OF THE CYBERNETIC THREAT TO CIVIL AVIATION

Abstract

The article presents an initial approach to the threat of cyberattacks on civil aviation, from the conceptual perspective of civil aviation intelligence. The following research problem was formulated: what are the essential parameters for structuring a panorama of the cyber threat as a phenomenon that interacts with and challenges civil aviation intelligence? The methodology proposes basic, exploratory, and qualitative research, using a literature review which outlines conceptual theoretical frameworks, structures, analyses and case studies. The Brazilian National Intelligence Policy (PNI) highlights the cyber threat, which has been growing exponentially and has a wide range of eligible and interconnected targets. It is a dynamic asymmetric threat that presents multiple formats and possible actors with the potential to damage critical assets and infrastructure. Civil aviation is a recurring target of unlawful interference, where the cyber threat is real – and could result in a "black swan" episode like the September 11, 2001 terrorist attacks. Addressing the threat of cyberattacks on civil aviation includes applicable concepts, the state of the art of civil aviation intelligence, the irrefutability of possible failures, potential targets, the categories of actors and their motivations, the ability to act and possible attack methods. The final considerations indicate the possibility of developments mediated by a policy to mitigate risks related to cyber threats in civil aviation subsidized by structured intelligence analysis.

Keywords: *threats, cyberattack, civil aviation, civil aviation intelligence, critical infrastructures.*

* Bacharel em Direito. Especialista em Inteligência de Estado e Inteligência de Segurança Pública (INASIS).

Introdução

A história da aviação e da atividade de inteligência comungam de diversos liames. A evolução técnica das aeronaves e de seu emprego como plataformas modais das atividades humanas consignou progressos à atividade de inteligência. Noutro giro, os ataques terroristas de 11 de setembro de 2001, nos Estados Unidos da América (EUA), estigmatizaram a atividade de inteligência e a aviação civil (SILVA, 2017, p. 16). Do paradigma do terrorismo, surgem diversas questões. Para a atividade de inteligência, importa otimizar suas capacidades. Caberá à inteligência, especialmente aplicada ao contexto da aviação civil, ser mais eficaz para se antecipar na mitigação das ameaças[1]. Após o 11 de Setembro de 2001, instaurou-se comissão investigatória no congresso estadunidense, que editou relatório. A análise indicou que condutas preparatórias dos atos terroristas ocorreram no cerne da aviação civil e que o conjunto das agências de inteligência tinha ciência disso. Falhas se impuseram na integração, análise e difusão adequada da inteligência que oportunizaria a neutralização da ação (ESTADOS UNIDOS DA AMÉRICA, 2004, tradução nossa).

Segundo Betts (2007, p. 107), o relatório de inteligência do Departamento Federal de Investigação dos EUA (FBI, na sigla em inglês) conhecido como *Phoenix Memo*, difundido cerca de um mês antes do atentado, esclarecia a existência de atividades terroristas em escolas de aviação civil ianques. A adequada percepção do memorando nos altos escalões, agregada a outros produtos de inteligência existentes, teria sido crucial para desmantelar o plano terrorista. É falacioso atribuir as falhas incidentes à inexperiência ou à ignorância sobre a relevância da inteligência para a aviação. A unidade de inteligência da aviação civil da Administração Federal de Aviação dos EUA (FAA, na sigla em inglês)[2] foi criada em 1986, porque a aviação era alvo recorrente de terrorismo (ESTADOS UNIDOS DA AMÉRICA, 1990, p. 74, tradução nossa).

Diante da complexidade, multiplicidade e inexatidão de resultados, Heuer e Pherson (2016) enaltecem as técnicas estruturadas de análise de inteligência, como a análise de cenários, que embora não revelem o futuro, criam limiar de eventos plausíveis a fim de preparar o decisor. A seu turno, Barreto (2007, p. 63-76) lecionou sobre o terrorismo cibernético em cenários especulativos. Especula-se que atores adversos, suas motivações e capacidades de agir podem extrapolar a paradigmática ação cinética[3] no solo americano. A ação terrorista ocorreu na dimensão tangível, a inteligência estadunidense padeceu na detecção e falhou na neutralização. Exorbitando a concepção

1 Das ameaças destacadas na Política Nacional de Inteligência (PNI) atribuíveis ao contexto do ecossistema da aviação civil, arrolam-se: 1) a espionagem; 2) a sabotagem; 3) a interferência externa; 4) a corrupção; 5) a criminalidade organizada; 6) as ações contrárias à soberania nacional; 7) as atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis; 8) o terrorismo; e 9) os ataques cibernéticos (BRASIL, 2016b).

2 Autoridade de aviação civil nos Estados Unidos da América, sendo comparável, guardadas as devidas proporções analógicas e contextuais históricas, à Agência Nacional de Aviação Civil (ANAC) no Brasil.

3 Ações cinéticas são aquelas desencadeadas no interior da Área de Operações, que envolvem movimentos (fogos, voos, deslocamento de tropas e de blindados) e produzem resultados tangíveis (destruição, captura, conquista etc.) (BRASIL, 2015a, p.17).

preditiva, sob os augúrios de uma técnica estruturada[4], surge uma questão: e se as ações antagônicas ocorrerem no espaço cibernético, intangível, mediante ações não cinéticas?

Com o objetivo de explicitar um panorama da ameaça de ataque cibernético, sob a ótica da inteligência da aviação civil, formulou-se o seguinte problema de pesquisa: quais os parâmetros essenciais para estruturar um panorama da ameaça cibernética como fenômeno que interage e desafia a inteligência da aviação civil? Em uma abordagem inicial e não exaustiva, a metodologia do trabalho propõe pesquisa básica, exploratória e qualitativa, por meio de revisão da literatura. Busca-se delinear os marcos teórico-conceituais, as estruturas, as perspectivas analíticas e as explorações casuísticas. Ao estruturar a ameaça de ataque cibernético à aviação civil, contemplam-se os conceitos preliminares, o estado da arte da inteligência da aviação civil, a irrefutabilidade de possíveis falhas, os alvos potenciais, as categorias de atores e suas motivações, a capacidade de agir e os possíveis métodos de ataque.

Conceitos Preliminares

O neologismo *ciberespaço* remonta à obra *Neuromancer* de Willian Gibson: "uma alucinação consensual, experimentada diariamente por bilhões de operadores legítimos [...]. Linhas de luz dentro do não espaço da mente; aglomerados e constelações de dados". Não há conceitos unívocos em cibernética. A literatura técnica define o ciberespaço como ambiente de informação, constituído digitalmente de dados criados, armazenados e compartilhados. Embora desafie dimensões físicas, não é exclusivamente virtual, por compreender computadores e infraestruturas que permitem aos dados fluir (SINGER e FRIEDMAN, 2017, p. 22 e 23).

O ciberespaço ou espaço cibernético é a dimensão da cibernética. É o mais novo espaço de batalha do teatro de guerra, ao lado dos espaços marítimos, terrestres, aéreos e espaciais (BRASIL, 2015a, p. 105 e p. 265). A cibernética "se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação" (BRASIL, 2015a, p. 62). A Política Nacional de Defesa (PND) relata que "para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear" (BRASIL, 2012, p. 11). Dos três setores estratégicos destacados, a Estratégia Nacional de Defesa (END) destinou ao Exército Brasileiro a

4 A técnica de análise estruturada "e se?" imagina que um evento inesperado ocorreu com potencial de impacto majorado. Diante da "retrospectiva", o analista presume o desenrolar e as consequências desencadeadas no evento. Gera-se consciência situacional, preparando a mente para reconhecer sinais antecedentes de mudanças significativas e propiciar assessoramento preditivo ao decisor (HEURER E PHERSON, 2016, l.3934, tradução nossa).

defesa cibernética[5]. O Exército Brasileiro também se debruça sobre os teclados e fluxos informacionais (BRASIL, 2012, p. 73) no Sistema Militar de Defesa Cibernética[6] (SMDC). Os computadores nos cercam no cotidiano e o teatro de operações cibernético oportuniza ampla gama de ações inéditas diante das tecnologias emergentes. São exemplos arquétipos a computação quântica, a inteligência artificial e a evolução da comunicação sem fio. Quanto à reformatação no campo bélico Barbosa da Costa (2012, p. 62) afirma que:

> O conflito armado permanecerá sendo um esforço intrinsecamente humano, com todas as incertezas que isso implica. No entanto, o caráter dos conflitos continuará a evoluir, permanecendo inerentemente instável, mas intenso e sujeito às novas condicionantes impostas pela revolução digital. Os contendores buscarão empregar métodos convencionais, irregulares e assimétricos, combinando, no tempo e no espaço, ações marítimas, terrestres, aéreas, espaciais e cibernéticas.

Proliferam-se, em todo o mundo, ataques cibernéticos de atores estatais ou não, inclusive contra infraestruturas críticas, além do epidêmico plantio de *fake news,* armas do conflito informacional. Assim, a escolha pelo estudo da ameaça cibernética na aviação civil é justificável. A ameaça cibernética é a "causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse" (BRASIL, 2015a, p. 27). A variedade de ações adversas possíveis dificulta a mitigação de ataques cibernéticos e impõe obstáculos a sua definição e atribuição. Vários conceitos interagem no vulto da ameaça. O que é um ataque cibernético? Eis a terminologia da Política Nacional de Inteligência (PNI) (BRASIL, 2016b):

> Ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que visem a interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional.

O estado da arte da inteligência da aviação civil

Ao estruturar uma ameaça à aviação, é preciso conceituar a inteligência da aviação civil, tão recente na literatura técnica. O documento *DoD Instruction Number 3115.14* traz um rol de atividades da inteligência, sob o estudo de tendências da indústria global que impactam os interesses estadunidenses e da capacidade de "detectar, analisar, monitorar e alertar sobre atividades ilícitas ou ameaças contra os Estados Unidos, seus aliados ou seus interesses envolvendo aviação civil" (ESTADOS UNIDOS DA AMÉRICA, 2011a, p. 6, tradução nossa). Refletindo a trindade conceitual de Sherman Kent e inspirado no paradigma do

5 A defesa cibernética é o "conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente" (BRASIL, 2015a, p. 85).

6 O Sistema Militar de Defesa Cibernética é o "conjunto de órgãos, meios, disponibilidades e relacionamentos, de natureza predominantemente militar, aptos a serem empregados de forma coordenada, no espaço cibernético, com efeitos no campo cinético, em defesa dos interesses nacionais em uma situação definida" (BRASIL, 2015a, p. 257).

departamento de Defesa dos EUA (DoD, na sigla em inglês), surgiu um conceito de inteligência da aviação civil, apto às doutrinas brasileiras (SILVA, 2017, p. 114):

> A inteligência da aviação civil é a expressão das atividades especializadas das autoridades competentes para entender como tendências na aviação civil impactam os interesses das nações, por intermédio da detecção, análise, monitoramento e alerta sobre atividades ilícitas ou ameaças contra os interesses envolvendo a aviação civil, objetivando salvaguardar ativos e produzir conhecimentos para assessorar o processo decisório.

A autoridade de aviação civil brasileira é a Agência Nacional de Aviação Civil (ANAC), autarquia especial criada pela Lei nº 11.182, de 27 de setembro de 2005 (BRASIL, 2005), sucessora do Departamento de Aviação Civil (DAC). A ANAC ingressou no Sistema Brasileiro de Inteligência (SISBIN) mediante edição de decreto (BRASIL, 2017b). Aduz-se que as atividades de inteligência da aviação civil do sobredito conceito circunscrevem-se às competências da ANAC, no escopo de inteligência fiscal e de colaboração no âmbito do SISBIN.

Restam sedimentados na memória popular, como ações ilícitas das últimas décadas relacionadas à aviação civil, os sequestros de aeronaves, os atentados à bomba e, finalmente, as ações suicidas que atingiram o *World Trade Center* e o Pentágono. Todavia o universo real e potencial de ameaças é dinâmico e evolui constantemente, ou seja, não se restringirá ao que já foi historicamente comprovado[7]. Versa a Doutrina Nacional da Atividade de Inteligência (DNAI) (BRASIL, 2016a, p. 63 e 64):

> Os atentados terroristas de 11 de setembro de 2001 deram ensejo a que Estados intensificassem o manejo da informação como instrumento e garantia de segurança coletiva. A exploração do espaço cibernético passou a utilizar sistemas de vigilância eletrônica ainda mais sofisticados e abrangentes. Muitas das ameaças tradicionais encontram correspondente no espaço cibernético, a exemplo da espionagem, do terrorismo, do ativismo extremista, da guerra e das atividades criminais. Nas duas últimas décadas, prejuízos advindos de crimes cibernéticos e desafios à segurança cibernética tornaram-se assunto de amplo debate. Além dos danos causados por crimes comuns, destacam-se aqueles que afetam a esfera econômica e a segurança nacional.

A inteligência perfaz assessoria especializada e preditiva, diante da qual a doutrina interpõe os desafios da segurança cibernética, subentendida como "arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2015a, p. 249). Na evolução histórica da aviação civil, o ataque cibernético desponta como ameaça mais recente. Para Shulsky e Schmitt (2002, l.1531), uma das funções da inteligência é criar sistema de indicadores e alertas para a mitigação de ameaças, baseado na análise de passos que o adversário tomaria ao

7 O manual de campanha do Exército Brasileiro preceitua: "os combates modernos têm se caracterizado pelo uso maciço de tecnologia, pela presença de civis e da mídia no ambiente operacional, pelo emprego de estruturas de combate com maior proteção coletiva, velocidade e letalidade seletiva, pela utilização de aeronaves remotamente pilotadas e pela capacidade de operar no espaço cibernético" (BRASIL, 2015b, p. 13).

preparar um ataque. Sublinhe-se, quanto aos indicadores e alertas (HERMAN, 1999, p. 235-236, tradução nossa):

> A guerra fria também produziu sistemas especializados, em sua maioria militares, de alerta engendrados por "indicadores", começando desde 1948. Os méritos dos arranjos variaram; claramente eles não preveniram falhas nos alertas. Subsiste certa vantagem em designar alguém com a especial responsabilidade de guiar a coleta de alvos de potencial alerta, e para procurar por evidências de alerta. Mas os sistemas de indicadores tem armadilhas, parcialmente porque se tratam de presunções sobre contingências esperadas ao invés de inesperadas e parcialmente porque eles sacam os indicadores fora de seu contexto. Alertar não é uma atividade separada do restante da compreensão de inteligência. A principal conclusão organizacional é que o alerta não pode ser separado da atividade de análise corrente; que noutro giro não pode ser isolada do trabalho a médio e longo termo. Alertar envolve aportar acuradas compreensões de longo termo para lidar em situações correntes; tais falhas tendem a refletir percepções errôneas de longo termo. [...] Então, alertar e avaliar em longo termo são peças de um contexto geral. Avaliações de curto e longo termo devem ser ajustadas não como atividades separadas, mas sim com retroalimentações e intercâmbios entre ambos. Buscar a compreensão dos alvos tem que ser combinado com a manutenção de um olho aberto para ameaças incomuns e comportamentos atípicos.

Ampliando o entendimento de ataque cibernético ao explorar a guerra cibernética[8], definem-se características e tipologias. Consideram-se, no domínio da guerra cibernética, o uso de medidas ofensivas ou defensivas. São verbos reitores de ações no espaço cibernético: negar, explorar, corromper, degradar e destruir. Identificam-se as plataformas utilizadas e os espaços onde o ataque cibernético incide, respectivamente: as ferramentas de tecnologia da informação e comunicações (TIC) e os sistemas de tecnologia da informação e comunicações e comando e controle (STIC2), que são valores baseados em informações, sistemas e redes de computadores. Eis o axioma básico da eficácia do ataque cibernético: a oportunidade de seu emprego é proporcional à dependência do adversário em relação à TIC. A finalidade é obter vantagens, tanto em objetivos militares quanto civis (BRASIL, 2015a, p. 134). Sobreleva notar a estratégica dependência da integração brasileira em relação à aviação civil e ao preparo da mobilização nacional (CHEREM, 2011, p. 34):

> Considerando a extensão territorial do Brasil, com mais de 8,5 milhões de km² – a quinta maior área do mundo – e mais de 5 mil municípios, observa-se com certa facilidade a razão pela qual o modal aeroviário tem sido privilegiado diante dos demais modais, por sua importância para integração nacional, sendo contemplado frequentemente pelas políticas públicas. Adiciona-se a esta assertiva, o fator preponderante da aviação no desenvolvimento nacional,

8 Interpreta-se verbete do glossário das forças armadas: "Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC" (BRASIL, 2015a, p.134).

> especialmente, quanto à fixação da população em regiões mais longínquas do país, fornecendo suporte para atividades econômicas, como por exemplo, a migração da fronteira agrícola no Centro-Oeste, ou ainda, na Região Amazônica, onde não se pode chegar pelo transporte fluvial, de forma perene ou temporária.

Quanto à severidade dos potenciais danos de ataques cibernéticos à aviação, analogia com a potência hegemônica é viável, visto que a estratégia nacional para a segurança da aviação ianque declara o valor do vetor aéreo (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 8, tradução nossa):

> As atividades relacionadas à aviação representam na atualidade aproximadamente cinco pontos percentuais no produto interno bruto da nação, com previsão de crescimento com o advento de tecnologias avançadas. Este horizonte dinâmico requer que os Estados Unidos desenvolvam e sustentem uma persistente metodologia de várias camadas para proteger tal recurso vital. Além disso, o ecossistema da aviação suporta o setor público, a segurança interna e operações aéreas militares contínuas e sob demanda para impedir o desmantelamento da nação.

Da irrefutabilidade de possíveis falhas

Duas características intensificam os riscos de ataque cibernético: é ameaça assimétrica e ação não cinética. A PNI ressalta o perfil não convencional do ataque cibernético ao listar os potenciais atores, evidenciando que são realizáveis por governos, organizações criminosas e "simpatizantes de causas específicas; ou mesmo por nacionais que apoiem ações antagônicas aos interesses de seus países" (BRASIL, 2017). O sinal não ortodoxo do ataque cibernético serve à didática da definição de ameaça assimétrica (BRASIL, 2015a, p. 27):

> Ameaça Assimétrica – Ameaça decorrente da possibilidade de serem empregados meios ou métodos não ortodoxos, que incluem terrorismo, ataques cibernéticos, armas convencionais avançadas e armas de destruição em massa para anular ou neutralizar os pontos fortes de um adversário, explorando suas fraquezas, a fim de obter um resultado desproporcional.

Enquanto as ameaças tangíveis são mais previsíveis no espectro de dados conhecidos oriundos das experiências históricas, o desconhecimento potencial das ameaças cibernéticas é real, e a possibilidade de surpresa estratégica em seu emprego é maior. O traço de ação não cinética do ataque cibernético complica sua detecção (BRASIL, 2015a, p. 19):

> Ações Não Cinéticas – São aquelas desencadeadas no interior da Área de Operações, que não envolvem movimentos (ações de guerra eletrônica, operações psicológicas, ações de assuntos civis, ações no ciberespaço) e produzem resultados intangíveis (interferências eletromagnéticas, bloqueio, percepção positiva da população sobre as forças amigas e suas operações), mas que contribuem para o sucesso da operação.

Há vastos recursos humanos sensibilizados na comunidade de inteligência e segurança pública, com décadas de investimentos em recursos materiais, lidando com ameaças tangíveis. É impossível afirmar o mesmo perante a intangibilidade das ameaças cibernéticas, apesar dos esforços institucionais. Abnegados pesquisadores, integrantes da comunidade de inteligência e militares comungam de tais esforços, dos quais são exemplos o pioneiro grupo de

trabalho editor do "Livro Verde: segurança cibernética no Brasil" e os membros do Comando de Defesa Cibernética do Exército Brasileiro e do Gabinete de Segurança Institucional (BRASIL, 2010). A dinâmica da ameaça cibernética e das tecnologias disruptivas renova-se diariamente. Já a mão de obra destinada à sua neutralização demanda maior tempo de preparação e investimentos, extravasando o interstício de renovação das ameaças. O vácuo de conhecimento sobre segurança cibernética não é exclusividade brasileira e foi destacado pelo general Michael Vincent Hayden, ex-diretor da Agência Central de Inteligência dos EUA (CIA, na sigla em inglês). A incapacidade de decidir linhas de ação pelos líderes decorre da pouca familiaridade de sua geração com computadores, sendo a segurança cibernética discutida com imprecisão e parco entendimento (SINGER e FRIEDMAN, 2017, p. 13). Aportando os raciocínios para as capacidades instaladas na segurança da aviação civil, a possibilidade de detectar ações de atores adversos no espaço tangível é maior do que no espaço cibernético. Na evolução histórica da aviação, a novel ameaça cibernética é aquela com o menor tempo de tratamento dedicado a sua mitigação. A produção técnica ianque coaduna-se com o raciocínio ora apresentado (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 3, tradução nossa):

> Nossos inimigos, continuam a enxergar a aviação como um alvo especial, e o ecossistema da aviação enfrenta ameaças multifacetadas e mudanças constantes nas táticas que constituem um desafio a superar. A última década observou o avanço de tecnologias que geraram benefícios sociais e econômicos, mas que também podem ser usados para desafiar a conformidade e a segurança do ecossistema da aviação. O uso de "tecnologias disruptivas", tais como a conectividade cibernética e as aeronaves não tripuladas, de forma inconsequente ou maliciosa, em conjunto com a constante evolução das ameaças terroristas à aviação tripulada, demandam um tratamento novo e universal pela comunidade.

Rejeitando o alarmismo midiático, é importante enaltecer um século de aprendizado de segurança na aviação: quando a engenharia aeronáutica implementou computadores nas aeronaves, o fez com redundâncias e camadas de segurança. A automação das aeronaves avança e, paulatinamente, prescinde e remodela a manipulação presencial do ser humano. As falhas são raras, como a que supostamente afetou o *software* do sistema de aumento das características de manobra (MCAS) de aeronaves *Boeing 737 MAX,* em evidência por talvez haver contribuído para acidentes aéreos recentes (BOEING, 2019). O erro é imanente à condição humana. Ainda mais raro seria explorar maliciosamente, por meio de violação, falha de concepção similar em ataque cibernético. Entretanto, dada a antítese em elogio à dialética, é improvável negar a miríade de possíveis falhas de engenharia ou execução em salvaguardas que obstaculizam potencial ataque cibernético a sistemas da aviação. Boas práticas da engenharia aeronáutica em aeronaves e sistemas embarcados não extinguem as

possíveis falhas[9]. É improvável também refutar a ocorrência de falhas ocultas na conformação dos sistemas aplicados na aviação civil: cite-se o exemplo da ameaça do *hardware trojan* (BRUZZEGUEZ, NEUMANN e SOUZA, 2018). Qualquer falha em qualquer sistema é potencialmente explorável em um ataque cibernético (BARRETO, 2007, p. 64):

> Qualquer infraestrutura TIC poderia ser alvo de uma ação terrorista. Um exemplo seria a paralisação do sistema de controle de tráfego aéreo de um aeroporto importante. Por outro lado, a infraestrutura TIC poderia ser, não mais o alvo, mas a ferramenta utilizada em um ataque, como uma intencional alteração de dados de voo que objetivasse produzir um acidente aéreo.

Os alvos elegíveis e as categorias de atores motivados que desafiam à Inteligência da Aviação Civil

Subsiste uma profusão de alvos eventuais de ataques cibernéticos na aviação civil: empresas aéreas, fabricantes de aeronaves, infraestruturas aeronáuticas, sistemas dedicados e órgãos de aviação civil. Em reverência à contrainteligência, declinar detalhes de alvos elegíveis é temerário. Em uma simples taxonomia, declina-se uma tríade de alvos elegíveis no ecossistema de aviação civil: infraestruturas críticas, sistemas críticos e plataformas críticas. Dentre as infraestruturas críticas, destacam-se os aeródromos e as instalações físicas do controle de tráfego aéreo. São exemplos de sistemas críticos aqueles destinados ao emprego comercial na gestão de passageiros e cargas, além daqueles relacionados ao controle de tráfego aéreo. As plataformas críticas são as aeronaves comerciais, cargueiras, privadas ou não tripuladas.

No campo teórico, são multitudinários os possíveis atores e motivações finalísticas de um ataque cibernético, por causa das subjetividades inerentes ao agente adverso que conduz a ação. Porém, é possível considerar categorias de atores motivados, tais como o crime organizado, as organizações ou atores terroristas e as nações hostis. As categorias detêm vicissitudes próprias. Na lição de Shulsky e Schmitt (2002), observar as distinções entre os atores motivados possibilita avaliar os indicadores para estruturar alerta preditivo apto ao assessoramento de inteligência.

Os atores motivados pelo crime organizado empregam sistematicamente o ambiente cibernético para o ilícito, atentos ainda à crescente convergência de suas ações com terroristas. Silva (2017, p. 153) destaca que

9 "Muitos sistemas operacionais comerciais são inauditáveis até o presente, uma vez que seus códigos-fonte não são disponibilizados pelos fabricantes. Sob tal análise, poder-se-ia inferir serem tais sistemas operacionais (ditos "fechados") ferramentas dotadas de eficácia potencial para emprego por forças armadas ou serviços de Inteligência adversos. Por exemplo, uma determinada chave criptográfica embutida secretamente em um sistema operacional poderia viabilizar o rompimento remoto de seus mecanismos naturais de segurança, como senhas e controle de portas lógicas. [...] Sistemas computacionais, mesmo aqueles pré-implantados e que não permitam a atualização de seu software, podem ser corrompidos com o passar do tempo. Classificam-se aqui, por exemplo, os equipamentos de controle empregados em aeronaves (denominados aviônicos), que são passíveis de ataques precedidos da infiltração por um programador especializado *(insider)*, ainda na fase de desenvolvimento" (BARRETO, 2007, p. 66 e 70).

"a exploração da aviação civil como vetor de atividades criminosas integra um conjunto de ameaças que demanda estreita interação com os órgãos de inteligência de segurança pública". A estratégia de segurança da aviação ianque aborda o crime organizado, a dimensão cibernética e a aviação civil (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 11, tradução nossa):

> Organizações criminosas transnacionais e outros criminosos afiliados rotineiramente buscam a assistência de funcionários da aviação simpáticos ou volúveis a facilitar o movimento ilícito de mercadorias ou pessoas. [...] Criminosos têm utilizado técnicas cibernéticas para atingir companhias relacionadas à aviação ao cometer crimes financeiros e empregar aeronaves não tripuladas para o tráfico, a vigilância e o reconhecimento de inteligência. Criminosos cibernéticos cometem crimes que têm como alvos redes e websites relacionados à aviação. As capacidades e motivações desse tipo de atores tornam difícil predizer seus alvos e o impacto de suas atividades. Ademais, o anonimato dos criminosos cibernéticos torna a atribuição de suas atividades extremamente complicada.

Para Barreto (2007, p. 63), o terrorismo cibernético é o "emprego, por terroristas, de técnicas de destruição ou incapacitação de redes computacionais de informação". Silva (2017, p. 152) anota que "ameaça terrorista pode se revestir de inúmeras condutas e abordar diversos alvos relacionados direta e indiretamente à aviação civil. De fato, os ativos da aviação civil poderão ser o alvo, o vetor e até a arma empregada na violência terrorista". Os atores e organizações motivadas pelo terrorismo adotam preferência histórica por alvos da aviação civil, cientes do impacto midiático e social. Uma tipologia possível de ataque terrorista cibernético percorre uma tríade de possibilidades: ataque técnico, destruição física ou pessoa infiltrada (BARRETO, 2007, p. 65-67). A probabilidade de terroristas realizarem ataques cibernéticos cresce com a evolução informacional das organizações terroristas. A estratégia da segurança da aviação estadunidense endossa a assertiva (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 10, tradução nossa):

> Terroristas continuam interessados em atacar o domínio da aviação como demonstrado no ataque do *Al-Shabaab a Daallo Airlines* (2016) e no ataque ao voo 9268 da *MetroJet* no Egito (2015), pelo qual ISIS assumiu responsabilidade. Ambos os ataques foram parcialmente assessorados pelo trabalho interno de radicalizados. Adicionalmente, os ataques catastróficos aos aeroportos de Bruxelas e Istambul (2016) demonstraram a intenção e a capacidade dos terroristas de atacar áreas públicas dos aeroportos, o que pode influenciar extremistas violentos domésticos a selecionar alvos similares.

O típico antagonismo entre as nações conduz à promoção de ataques exploratórios, com o objetivo de angariar vantagens na obtenção sub-reptícia de dados classificados. Silva (2017, p. 207) afirma que "o Brasil é um alvo substancial e conveniente para a exploração da inteligência econômica por atores de inteligências adversas, com especial enfoque na ameaça da espionagem industrial, bem como a obtenção de dados dos recursos naturais brasileiros". A exploração da fonte cibernética[10] é vulnerabilidade

10 A fonte cibernética é o "recurso por intermédio do qual se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A Fonte Cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de Inteligência" (BRASIL, 2015a, p. 119).

latente na espionagem industrial. Entre os meios para a consecução da espionagem industrial, evidencia-se a execução de ataque cibernético (ESTADOS UNIDOS DA AMÉRICA, 2018a, p.10-12):

> Nações já conduziram ataques cibernéticos e ciberespionagem contra alvos do ecossistema da aviação. [...] As nações tem cada vez mais visualizado as capacidades cibernéticas ofensivas como meios para avançar nos campos de objetivos militares, políticos e econômicos. [...] Nações hostis e outras entidades de inteligência usam o ecossistema da aviação para conduzir furtos de propriedade intelectual que custam enormes somas monetárias e criam ameaças profundas à nossa segurança nacional.

A CAPACIDADE DE AGIR E MÉTODOS DE ATAQUE: UM RASANTE CASUÍSTICO

Em julho de 2018, soube-se que manuais técnicos secretos do sistema de aeronaves remotamente pilotadas (SARP) militar MQ-9 *Reaper* estavam à venda na internet, pelo preço de cento e cinquenta dólares (MCLAUGHLIN, 2018). Em outubro de 2018, um cidadão chinês foi preso e deportado da Bélgica para os Estados Unidos. Um relatório técnico do FBI, após operação de contrainteligência, originou a acusação judicial de espionagem industrial e furto de segredos comerciais. O agente Xu Yanjun foi relacionado ao ministério da Segurança do Estado da China (MSS, na sigla em inglês). A denúncia à justiça alega que ele recrutava operacionalmente especialistas em patentes de motores de aeronaves comerciais. O principal alvo era a *GE Aviation,* uma das líderes mundiais no segmento (ESTADOS UNIDOS DA AMÉRICA, 2018b).

É também relevante a capacidade de agir da inteligência adversa em ataque cibernético, sintetizável em três pilares: acessibilidade do alvo, uso de artefato cibernético e emprego do poder cibernético. A acessibilidade do alvo depende de fatores ambientais e de segurança orgânica, que adentram a segurança da aviação civil *(security)*, estruturada em camadas. Recente vazamento de dados indica que a inteligência cubana pode haver recrutado operacionalmente servidores no aeroporto de Miami, para obter acesso a áreas restritas de segurança (HANKS e TORRES, 2019). Há múltiplos artefatos cibernéticos. Esse termo significa "equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos" (BRASIL, 2015a, p. 37). Usar o poder cibernético é a meta de quem opera um artefato no ciberespaço. O poder cibernético é a "capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder" (BRASIL, 2015a, p. 211). Presume-se capaz de agir qualquer ator motivado que detenha acesso ao alvo, possua artefato cibernético e seja eficaz no uso do poder cibernético.

E quais são os métodos de ataques cibernéticos? Não há lista exaustiva ou definições unívocas, abundam variações terminológicas. Didaticamente, as ações no campo cibernético constituem medidas defensivas, medidas ofensivas e medidas exploratórias. São vários os métodos possíveis de ataque cibernético: a injeção

de *malware*[11], o ardil do *phishing*[12], o ataque de força bruta[13], o ataque de negação de serviço[14], o ataque de negação de serviço distribuído[15], a interferência por dissimulação de autenticidade no canal *(spoofing)*[16], a interferência por saturação e embaraço *(jammers)*[17], a extorsão criptográfica do *ransomware*, etc.

O desafio da proteção cibernética da aviação civil se amplifica diante das autoridades. Em agosto de 2013, um *jammer* do sistema de posicionamento global (GPS, na sigla em inglês) inadvertidamente usado por um caminhoneiro interferiu nas operações aéreas do aeroporto de Newark, atrapalhando sistemas de navegação aérea. Em junho de 2015, o aeroporto internacional de Varsóvia, capital da Polônia, sofreu ataque cibernético nos *softwares* que influenciam nos planos de voos das aeronaves, afetando milhares de passageiros. Em dezembro de 2016, a agência de aviação civil da Arábia Saudita padeceu de ataque cibernético que danificou vários computadores, apagando e roubando dados críticos (SILVA, 2017, p. 197, 199 e 203). Em abril de 2015, relatório de governança concluiu que a FAA deve abordar com maior abrangência a segurança cibernética nas evoluções do tráfego aéreo (ESTADOS UNIDOS DA AMÉRICA, 2015, p. 40). Entre outros exemplos relacionados às infraestruturas críticas além da aviação, a DNAI indica os ataques cibernéticos aos sistemas governamentais da Estônia em 2007 e da Geórgia em 2008, o uso do *Stuxnet* em 2010 contra a infraestrutura nuclear no Irã e os vazamentos de dados da Agência Nacional de Segurança dos EUA (NSA, na sigla em inglês) promovidos por Edward Snowden em 2013 (BRASIL, 2016a, p. 64). Em 2014, ataque cibernético danificou a indústria siderúrgica alemã ao desligar inopinadamente

11 O termo *malware* relaciona-se ao "ataque cibernético que consiste em infiltrar programas nocivos ou maliciosos em computadores e sistemas do(s) alvo(s). Com o programa infiltrado, o atacante pode corromper ou alterar sistemas, provocar danos e até mesmo roubar informações" (OLIVEIRA et al, 2017, p. 6).

12 O *phishing*, termo que remete à "pescaria", é "ataque cibernético utilizado na prática de fraudes. Esse ataque ocorre de diferentes formas, com uso técnico de informática ou apenas estratagemas que levam os alvos a se comprometerem. Em virtude disso, ele pode ser utilizado tanto para ofensivas contra a segurança cibernética, quanto para afetar a defesa cibernética de um país" (OLIVEIRA et al, 2017, p. 6).

13 O ataque de força bruta *(brute force attack)* ocorre quando "o atacante adivinha, por tentativa e erro, um nome de usuário e sua respectiva senha, permitindo-lhe executar processos e acessar sites, computadores e serviços com o mesmo nome e privilégios do usuário alvo do ataque" (BRASIL, 2015a, p. 39).

14 O ataque de negação de serviço (*denial of service* – DOS) ocorre quando "um atacante utiliza um computador ou dispositivo móvel conectado a uma rede ou à Internet para inundar um servidor em uma determinada rede com um número excessivo de solicitações de modo a tirar de operação um serviço por sobrecarga" (BRASIL, 2015a, p.39).

15 O ataque de negação de serviço distribuído (*distributed denial of service* – DDOS) ocorre quando "o ataque é lançado simultaneamente por um grande número de computadores escravos, atuando em rede, controlados por um atacante mestre por meio de infecção prévia (*vírus, worms*) de modo a aumentar consideravelmente sua eficácia na paralisação de um determinado serviço por sobrecarga" (BRASIL, 2015a, p. 39).

16 "Tipo de ataque em rede de dados em que um elemento da rede falsifica dados para se fazer passar por outro elemento da rede e, assim, obter algum tipo de vantagem" (BRASIL, 2016c, p. 292).

17 Os *jammers* são transmissores ilegais de frequências de rádio, planejados para bloquear, embaraçar ou interferir em comunicações de rádio autorizadas (ESTADOS UNIDOS DA AMÉRICA, 2011b, p. 2).

maquinário de usinagem (BBC, 2014). Em 2015, o Exército Brasileiro foi alvo de ataque cibernético, resultando em vazamento de dados (OLIVEIRA et al, 2017, p. 66). Em junho de 2017, anomalia foi reportada pela Administração Marítima americana (MARAD, na sigla em inglês) (ESTADOS UNIDOS DA AMÉRICA, 2017). Consistia no embaraço eletromagnético de GPS na região do mar Negro, estratégica à influência político-militar russa, prejudicando sistemas que evitam a colisão entre navios. Análises especializadas posteriores dão conta da deliberação do incidente, similar a ataque cibernético de *spoofing* (GOWARD, 2017). Em teoria, os ataques cibernéticos citados são adaptáveis contra alvos na aviação civil. A escassa produção científica sobre riscos cibernéticos contra tal ecossistema, isoladamente, já deveria inquietar a inteligência da aviação civil. O conjunto de amostras casuísticas traça devir de ameaças reais e potenciais exploráveis por atores motivados e capazes, que podem englobar, eventualmente, ações de inteligências adversas.

Derivam da Agência de Segurança de Redes e Informações da União Europeia (ENISA) possíveis soluções perante os ataques cibernéticos, na forma de guia de boas práticas na implementação de estratégias de segurança cibernética[18] (ENISA, 2016). Os objetivos das boas práticas estão organizados em quatro grupos: estruturação, capacitação, cooperação e fomento. Quanto à estruturação, recomenda-se desenvolver planos nacionais de contingência cibernética, proteger informações de infraestruturas críticas, estabelecer linha basal de medidas de segurança, estabelecer mecanismos de comunicação de incidentes, estabelecer capacidade de resposta a incidentes, balancear segurança e privacidade e tratar os crimes cibernéticos. Entre as boas práticas de capacitação, é preciso fortalecer treinamentos e programas educacionais, aumentar a consciência do usuário e organizar exercícios de segurança cibernética. No grupo de cooperação, é recomendável institucionalizar cooperação entre agências públicas, engajar-se na cooperação internacional e estabelecer parcerias público-privadas. Finalmente, nas boas práticas de fomento, é preciso incentivar o setor privado a investir em medidas de segurança e promover a pesquisa e desenvolvimento (ENISA, 2016, p. 23-39).

Considerações finais

O panorama ora estruturado e a experiência histórica apontam que o ecossistema da aviação civil é alvo primário de diversos atores motivados, com variados objetivos finalísticos, relacionáveis à ameaça de ataque cibernético. Embora os paradigmas comparativos auxiliem a compreensão da ameaça, não podem ser adotadas soluções por espelhamento. A título de exemplo, a realidade da inserção brasileira no horizonte de ameaças é distinta e peculiar em relação à realidade estadunidense. A Estratégia Nacional de Inteligência (ENINT) define o eixo estruturante da tecnologia e capacitação, donde sobressai objetivo estratégico crucial à mitigação da ameaça: "ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência cibernética" (BRASIL, 2017,

18 O título original do documento em língua inglesa é: *NCSS good practice guide: designing and implementing national cyber security strategies.*

p. 26). A DNAI divisa o caminho para tal maturidade (BRASIL, 2016a, p. 64):

> Os procedimentos tradicionais da Atividade de Inteligência executados na realidade física estendem-se à realidade virtual. A segurança cibernética não se fundamenta apenas na prevenção e no enfrentamento de ameaças, mas também na antecipação da identificação de intenções e potencialidades de adversários. Ataques cibernéticos implicam atividades que se situam além da rede em si, uma vez que se inserem em questões concorrenciais, geralmente de caráter político e econômico. Há, portanto, uma dimensão humana que não pode ser negligenciada em face dos dados técnicos; o técnico e o comportamental devem ser justapostos no estudo de cada situação.

Aprofundar os conhecimentos existentes sobre a ameaça cibernética na aviação civil, fomentando ações de contrainteligência, é o primeiro passo para incrementar a resiliência cibernética. Na esfera executiva, o início de uma solução factível demanda a interação da atividade de inteligência da aviação civil com órgãos de defesa cibernética instituídos. O ataque cibernético é ameaça extremamente dinâmica, e a casuística corrobora a pluralidade de métodos. É imprescindível a constante atualização nos estudos para mitigar sua ocorrência, especialmente, devido ao despreparo de parte da mão de obra da aviação face à ameaça. É inconteste que a aviação evoluiu sobretudo por meio da investigação de falhas em acidentes e incidentes aeronáuticos, ou seja, de enfoque reativo. A inteligência tem foco preditivo, devendo antecipar-se à recente ameaça cibernética aos ecossistemas da aviação civil. Pelos elementos colecionados, é possível retomar a iniciativa, propondo evolução intermediada pela criação de política de mitigação de riscos relacionados à ameaça cibernética na aviação civil, antes de suportar tragédias decorrentes de omissão. Para tanto, demandam-se análises estruturadas de cenários específicos (HEUER e PHERSON, 2016), contextualizadas aos alvos elegíveis da aviação civil, que considerem os métodos de ataque, os atores motivados e suas respectivas capacidades de agir e gerem indicadores e alertas aptos à assessoria do processo decisório.

Referências

BBC News. *Hack attack causes 'massive damage' at steel works*. Londres: British Broadcast Corporation, 2014. Disponível em: https://www.bbc.com/news/technology-30575104. Acesso em: 20 jul. 2019.

BARBOSA DA COSTA, Carlos Eduardo. Tendências mundiais e seus reflexos para a defesa brasileira. *Revista Brasileira de Inteligência*, Brasília, v. 7, p. 54-66, 2012.

BARRETO, Eduardo Müssnich. Terrorismo Cibernético e cenários especulativos. *Revista Brasileira de Inteligência*, Brasília, v. 4, p. 63-76, 2007.

BETTS, Richard K. *Enemies of intelligence:* knowledge and power in American national security. New York: Columbia University Press, 2007.

BRASIL. Lei n° 11.182, de 27 de setembro de 2005. Cria a Agência Nacional de Aviação Civil – ANAC. *Diário Oficial da União:* seção 1, Brasília, DF, 28 set. 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11182.htm. Acesso em: 12 maio 2019.

_____. Presidência da República. Gabinete de Segurança Institucional. *Livro verde:* segurança cibernética no Brasil. Brasília: Departamento de Segurança da Informação e Comunicações, 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf/view >. Acesso em: 10 maio 2019.

_____. Ministério da Defesa. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa, 2012. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 01 maio 2019.

_____. Ministério da Defesa. Portaria normativa nº9/GAP/MD, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas – MD35-G-01 (5ª.edição/2015). Brasília: 2015a. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 11 maio 2019.

_____. Ministério da Defesa. Exército Brasileiro. Portaria nº032-EME, de 23 de fevereiro de 2015. Aprova o manual de campanha EB20-MC-10.207 Inteligência, 1ª.ed. *Boletim do Exército*, Brasília, n.9, 27 fev. 2015b. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/1/2595/1/EB20-MC-10.207.pdf. Acesso em: 16 jul. 2019.

_____. Presidência da República. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência:* fundamentos doutrinários. Aprovada pela Portaria nº 244 - ABIN/GSI/PR, de 23 de agosto de 2016. Brasília: ABIN,

2016a.

_____. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. *Diário Oficial da União:* seção 1, Brasília, DF, 30 jun. 2016b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em: 01 maio 2019.

_____. Ministério da Justiça. Polícia Federal. *Glossário de ciências forenses:* termos técnicos mais usados pela perícia criminal federal. Brasília: Diretoria Técnico Científica, 2016c.

_____. Presidência da República. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Estratégia Nacional de Inteligência.* Brasília: Abin, 2017a. Disponível em: http://www.abin.gov.br/conteudo/uploads/2015/05/ENINT.pdf. Acesso em: 01 maio 2019.

_____. Decreto n° 9.209, de 27 de novembro de 2017. Altera o Decreto n º 4.376, de 13 de setembro de 2002, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei n º 9.883, de 7 de dezembro de 1999. *Diário Oficial da União:* seção 1, Brasília, DF, 28 nov. 2017b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11182.htm. Acesso em: 12 maio 2019.

BOEING. *Boeing Statement On Ethiopian Airlines Flight 302 Investigation Preliminary Re*port. Chicago: 2019. Disponível em: https://boeing.mediaroom.com/2019-04-04-Boeing-Statement-On-Ethiopian-Airlines-Flight-302-Investigation-Preliminary-Report. Acesso em: 15 jul. 2019.

BRUZZEGUEZ, Gustavo A.; NEUMANN, Clóvis; SOUZA, João Carlos F. O hardware comprometido: uma importante ameaça a ser considerada pela atividade de inteligência. *Revista Brasileira de Inteligência*, Brasília: Abin, v. 13, p. 113-127, 2018.

CHEREM, João Carlos dos Santos. *Infraestrutura de transportes e o preparo da mobilização nacional.* Rio de Janeiro: ESG, 2011.

European Union Agency for Cybersecurity. *NCSS good practice guide: designing and implementing national cyber security strategies.* ENISA: 2016. Disponível em: https://www.enisa.europa.eu/publications/ncss-good-practice-guide. Acesso em 18 jul. 2019.

ESTADOS UNIDOS DA AMÉRICA. The President of United States. *Report of the President's Commission on Aviation Security and Terrorism.* Washington, D.C.: 1990. Disponível em: http://www.policyfutures.com/PCAST/PCASTreport.pdf. Acesso em: 11 maio 2019.

_____. National commission on terrorist attacks upon the United States - public law 107-306. *The 9/11 commission report.* National commission on terrorist attacks upon the

United States, 2004. Disponível em: https://9-11commission.gov/report/911Report.pdf. Acesso em: 11 maio 2019.

_____. Department of Defense. *Instruction number 3115*.14. United States Department of Defense, 29 jul. 2011a. Disponível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/311514p.pdf. Acesso em: 12 jul. 2019.

_____. Federal Communications Commission. *GPS, Wi-Fi, and Cell Phone Jammers:* frequently asked questions (FAQs). Federal Communications Commission, 2011b. Disponível em: https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf. Acesso em: 20 jul. 2019.

_____. United States Government Accountability Office. *Air traffic control* – FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen (report to congressional requesters). United States Government Accountability Office, 2015. Disponível em: https://www.gao.gov/assets/670/669627.pdf. Acesso em: 20 jul. 2019.

_____. United States Departament of Transportation. *MSCI Alert: 2017-005A-Black Sea-GPS Interference*. United States Departament of Transportation. Maritime Administration (MARAD), 2017. Disponível em: https://www.maritime.dot.gov/content/2017-005a-black-sea-gps-interference. Acesso em: 20 jul. 2019.

_____. The President of United States. *National Strategy for Aviation Security of the United States of America*. Washington, D.C.: 2018a. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf. Acesso em 18 maio 2019.

_____. Department of Justice. Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies. *Justice News*. Washington, D.C, 10 oct. 2018b. Disponível em: https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading. Acesso em 15 jul. 2019.

GOWARD, Dana A. GPS spoofing incident points to fragility of navigation satellites – "National Defense". Resilient Navigation and Timing Foundation, 23 aug. 2017. Disponível em: https://rntfnd.org/2017/08/23/gps-spoofing-incident-points-to-fragility-of-navigation-satellites-national-defense/. Acesso em: 20 jul. 2019.

HERMAN, Michael. *Intelligence power in peace and war*. Cambridge, UK: Cambridge University Press, 1999.

HEUER, Richards J. Jr; PHERSON, Randolph H. *Structured analytic techniques for intelligence*

analysis. CQ Press, 2016. Kindle edition. Paginação irregular.

HANKS, Douglas; TORRES, Nora Gámez. *Report:* Cuban spy documents target security at Miami's airport. MIA says no breach. Miami Herald, 2019. Disponível em: https://www.miamiherald.com/news/local/community/miami-dade/article231133238.html. Acesso em: 20 jul. 2019.

MCLAUGHLIN, Jenna. US Reaper drone data leaked on dark web, researchers say. *CNN politics,* 10 jul. 2018. Disponível em: https://edition.cnn.com/2018/07/10/politics/us-reaper-drone-materials-hacker-theft/index.html. Acesso em: 10 jul. 2019.

OLIVEIRA, Marcos A. Guedes, et al. *Guia de Defesa Cibernética na América do Sul.* Recife: Ed. UFPE, 2017. Disponível em: https://pandia.defesa.gov.br/images/acervodigital/GuiaDefesaCiberneticaAmericaSul.pdf. Acesso em: 21 jul. 2019.

SILVA, Mateus Vidal Alves. *Ações de inteligência na produção de conhecimentos da autoridade de aviação civil.* 2017. Trabalho de Conclusão do Curso (Especialização em Inteligência de Estado e Inteligência de Segurança Pública – INASIS 2016-2017) – Associação Internacional para Estudos de Segurança e Inteligência, Faculdades Milton Campos, Nova Lima, 2017.

SINGER, Peter Warren; FRIEDMAN, Allan. *Segurança e guerra cibernéticas:* o que todos precisam saber. Rio de Janeiro: Biblioteca do Exército, 2017.

SHULSKY, Abram N.; SCHMITT, Gary J. *Silent warfare:* understanding the world of intelligence. 3. ed. Washington, DC: Potomac Books, 2002. Kindle edition. Paginação irregular.

AGENTE INFILTRADO E AGENTE DE INTELIGÊNCIA: DISTINÇÕES A PARTIR DE ESTUDO DE CASO JULGADO PELO SUPREMO TRIBUNAL FEDERAL

Luis Fernando de França Romão *

Resumo

A confusão acerca do conceito de Inteligência em segurança pública gera efeitos práticos de consequências significativas, com impacto inclusive na Justiça Criminal. Isso pode ser vislumbrado em nível tático-operacional, notadamente, quando da realização de operações em campo por agentes policiais para a obtenção de dados relevantes. Sobre esse tema, objetiva-se aqui apresentar a diferença entre o agente policial infiltrado e o agente policial de Inteligência, a partir do caso referência *Black blocs*, julgado em 2019 pelo Supremo Tribunal Federal. No referido caso, a controvérsia posta judicialmente restringiu-se à possibilidade ou não de se utilizar dados obtidos por um agente policial infiltrado sem autorização judicial; para isso, os juízes verificaram se a atuação do policial se dera como agente infiltrado ou agente de Inteligência e quais seriam as consequências jurídicas para cada uma dessas alternativas. O método de pesquisa utilizado é o estudo de caso para se registrar dados que trazem à tona uma concepção que se projeta no processo penal brasileiro. O caso *Black blocs* será apresentado em todas as instâncias pelas quais tramitou, e ficará restrito aos aspectos que envolvem a distinção entre agente infiltrado e agente de Inteligência. Após isso, uma análise crítica será apresentada e dará destaque a disfunções de duas ordens: uma no campo da Inteligência: problema de comando e de coordenação no exercício da atividade em nível tático-operacional; e outra no da Justiça Criminal, com falhas e distorções de julgamento que abrangem a concepção e a prática da atividade de Inteligência. O presente artigo aborda um tema teórico-prático da área de Inteligência em sua vertente aplicada à segurança pública.

Palavras-chaves: agente infiltrado; agente de Inteligência; segurança pública.

UNDERCOVER AGENT AND INTELLIGENCE AGENT: DISTINCTIONS DRAWN FROM A CASE STUDY JUDGED BY THE FEDERAL SUPREME COURT

Abstract

Confusion about the concept of Intelligence in public security has practical effects with significant consequences, including for criminal justice. This can be seen at the tactical-operational level, notably when field operations are conducted by law enforcement officials to obtain relevant data. In this sense, this paper aims to present the difference between an infiltrated police officer and an intelligence police officer, based on the Black blocs case, judged in 2019 by the Federal Supreme Court. In this case, the controversy brought to court was restricted to whether or not to use data obtained by an undercover police officer without judicial authorization, although it had been previously checked whether the police officer had acted as an undercover agent or law enforcement officer and what the legal consequences would be for each of these alternatives. The research method is the case study, which records data that bring out a conception that is projected on the Brazilian criminal process. The Black Blocs case will be presented in all the instances through which it was dealt with, and will be restricted to aspects involving the distinction

* Doutorando em Ciências Jurídico-Políticas pela Universidade de Lisboa (Portugal). Mestre em Direito do Estado (USP). Pós-graduando em Ciências Criminais e Segurança Pública (Uerj). Bacharel em Direito (PUC-Rio). Advogado. Membro da Comissão de Direito Constitucional do Instituto dos Advogados Brasileiros.

between undercover agent and Intelligence agent. Next, a critical analysis will be presented and will highlight dysfunctions identified in two spheres: one in the field of Intelligence – a problem of command and coordination of the Intelligence operation at a tactical-operational level; and another related to criminal justice, with flaws and distortions of judgment encompassing the concept and practice of Intelligence. This paper addresses a theoretical-practical theme of Intelligence applied to public security.

Keywords: *undercover agent; Intelligence agent; public security.*

Introdução: considerações sobre Inteligência em segurança pública

Unidades de Inteligência proliferaram nas mais diversas estruturas institucionais no Brasil, como observa Fernando do Carmo Fernandes, de modo que é possível vislumbrar agências, coordenadorias, secretarias ou subsecretarias assim denominadas nas várias esferas de governo. Logo, questão relevante é se as soluções para o esclarecimento de grande parte dos ilícitos e ameaças passaram a depender do êxito dessas unidades instituídas no âmbito da segurança pública. Não obstante, as práticas adotadas, destaca Fernandes (2006, p. 7-8), têm deixado de considerar aspectos relevantes da doutrina[1], tanto no que diz respeito à estrutura dessas unidades, quanto no conhecimento por elas produzidos e, sobretudo, na orientação de seus trabalhos.

Ao tratar do conceito de Inteligência na segurança pública, Rodrigo Kraemer sobreleva que, dentre outros fatores, as semelhanças entre as técnicas operacionais de Inteligência e as técnicas de investigação criminal podem ter contribuído para o entendimento errôneo de que Inteligência seria sinônimo de atividade investigatória, interpretação incorreta e, segundo o autor, já consolidada no sentido de que "inteligência seria uma investigação mais apurada" (KRAEMER, 2015, p. 73-82).

Ao abordar o tema da atividade operacional em benefício da segurança pública no combate ao crime organizado, Cristina Célia Fonseca Rodrigues (2009, p. 61) aponta que a operação de Inteligência de Estado visa a transformar informações táticas em conhecimentos estratégicos que antecipam fatos, alertam para casos específicos e subsidiam documentos para assessorar autoridades governamentais. Já a operação policial, diferentemente, busca produzir provas da materialidade e da autoria de crimes.

Ainda assim, não há dissociação estanque entre a atividade de Inteligência de Estado e a atividade de Inteligência de Segurança Pública, porque, como pondera Josemária da Silva Patrício (2006, p. 56-57), os órgãos de Inteligência criados no âmbito da segurança pública especialmente para a produção de conhecimentos objetivam subsidiar as investigações policiais, entre outras tarefas, uma vez que, se assim não fosse, não seria necessária sua criação, pois já existe a polícia judiciária para investigar delitos, e há ambiente normativo-institucional que conflui para a integração das atividades de Inteligência de segurança pública ao Sistema Brasileiro de Inteligência (Sisbin). Logo, é correto o entendimento de que "investigação policial é o mesmo que inteligência voltada para a segurança pública".

Ademais, mesmo que haja estrutura normativa norteadora das ações de Inteligência, nos dizeres de Josemária da Silva Patrício (2006, p. 57) trata-se de algo ainda inusitado para as polícias e suas instâncias e competências, o que leva a mudança de paradigmas, algo novo no serviço público e que "mexe nas

1 Notadamente: KENT, 1967; PLATT, 1974; CLAUSER & WEIR, 1975; MINISTÉRIO DO EXÉRCITO, 1995; CLARK, 1996; DEPARTMENT OF THE ARMY, 1996; DEPARTMENT OF THE NAVY, 1997; GABINETE DE SEGURANÇA INSTITUCIONAL, 2017; AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2019.

idiossincrasias do universo policial". Mas não só. Na prática, isso também tem efeitos significativos que repercutem na aplicação da Lei Penal pela Justiça Criminal, como se verificará, a seguir, no caso de infiltração de agentes, que explicita a produção e o uso de provas para condenação.

Com efeito, em nível tático-operacional, quando da realização de operações em campo por agentes policiais para obter dados e informações relevantes, sobreleva-se esse confuso entendimento conceitual que envolve Inteligência em Segurança Pública. Neste sentido, objetiva-se apresentar a distinção entre o agente policial infiltrado e o agente policial de Inteligência, a partir do caso referência *Black blocs* julgado em fevereiro de 2019 pela Segunda Turma do Supremo Tribunal Federal, em que a controvérsia posta em julgamento fora a possibilidade ou não de utilização dos dados obtidos por agente policial infiltrado sem autorização judicial e as consequências jurídicas decorrentes do enquadramento da atuação do policial como agente infiltrado e como agente de Inteligência.

Nesta perspectiva, compreende-se que a metodologia do estudo de caso é adequada para registrar dados de uma concepção, ainda nova, que se projeta no processo penal brasileiro, emitida pela mais alta Corte de Justiça do Brasil, que pode influenciar inúmeros outros casos pelo País e tornar-se precedente. Organizar-se-á, metodologicamente, a apresentação do caso a todas as instâncias pelas quais tramitou, e restringir-se-á, contudo, aos aspectos que envolvem a distinção entre agente infiltrado e agente de Inteligência e, ainda, à possibilidade de utilização no processo penal dos dados e informações obtidos pelo agente. Após o relatório que contém a descrição do caso julgado, far-se-á a análise crítica dessa experiência fática com apoio na revisão de bibliografia correspondente à atividade de Inteligência, ilicitude da prova e infiltração de agentes policiais.

A controvérsia da infiltração de agente no caso *Black Blocs*

Na primeira instância[2]

Em julho de 2014, a 27ª Vara Criminal da Comarca da Capital do Rio de Janeiro recebeu denúncia do Ministério Público local em face de vinte e três denunciados por associarem-se para o fim específico de cometer os crimes de dano (depredação do patrimônio privado – agências bancárias, lojas e veículos – e público ou de concessão pública, com destruição de mobiliário urbano e incêndio de ônibus), resistência (arremesso de pedras e artefatos incendiários principalmente contra agentes de segurança pública), lesões corporais, posse de artefatos explosivos (bombas de fabricação artesanal) e corrupção de menores (incentivo à participação de adolescentes nas condutas anteriores). Essas ações foram cometidas por pessoas ligadas a grupos com objetivos declaradamente lícitos de organização de protestos e manifestações contestadoras do *status quo* que tiveram origem em junho de 2013, porém, passaram a praticar atos violentos e de confrontos com a denominada tática *black bloc*.

2 TJRJ, 27ª Vara Criminal Comarca da Capital, Ação Penal nº 0229018-26.2013.8.19.0001, Juiz Flavio Itabaiana de Oliveira Nicolau.

A defesa de um dos réus alegou em juízo de primeira instância a ilicitude da prova testemunhal de policial militar por ter sido originária de infiltração sem autorização judicial. O Juiz de Direito não acolheu o questionamento, e aduziu que não houve infiltração policial, por inexistir o ingresso do agente no meio organizacional composto pelos réus, nem ocorreu simulação de que o policial fosse membro de facção voltada à pratica de crimes, mas houve, tão somente, coleta de informações por parte do agente policial, em locais abertos ao público, durante atos em que a presença de qualquer pessoa era permitida, e não é necessário, assim, segundo o Juízo, que o policial se fizesse passar por membro de qualquer um dos grupos criminosos investigados.

No Tribunal de Justiça[3]

A defesa técnica impetrou, em dezembro de 2014, *habeas corpus* que alegou constrangimento ilegal de um dos réus porque respondia a uma ação penal com denúncia baseada em depoimento de policial militar integrante da Força Nacional de Segurança Pública (FNSP) infiltrado nas manifestações sem autorização judicial exigida pela Lei nº 12.850/2013.

O órgão colegiado frisou que o policial militar informou, em seu depoimento, que estava lotado na Força Nacional, na Operação Pacificadora II, no Rio de Janeiro desde março de 2014, atuava como observador nas manifestações com o intuito de coletar dados para atuação daquele órgão no evento da Copa do Mundo, e limitava-se a ir aos locais para observar os ânimos dos envolvidos e a encontrar-se com integrantes das manifestações para escutar os planejamentos e repassar as informações a seu Comando. Filmava em tempo real e repassava ao vivo as ações realizadas em campo ao Centro Integrado de Comando e Controle (CICC) para acompanhamento das manifestações por outros órgãos de Inteligência. Além disso, durante as transmissões, ao ser abordado por diversas pessoas, o agente policial viu-se obrigado a dizer que estava no local em pesquisa de campo para obter material para trabalho de curso de gestão pública.

Em dia específico de manifestação, o agente policial registrou que o movimento estava pacífico até um dos acusados (paciente do *habeas corpus*) se comunicar de forma peculiar com integrantes dos *black blocs* e a partir disso iniciar atos de vandalismo, fato este reportado ao Comando pelo agente policial de campo que, inclusive, conquistara a confiança dos manifestantes e recebera convite para integrar grupo fechado de conversa criptografada, por onde os atos violentos eram agendados.

A 7ª Câmara Criminal salientou que os réus foram denunciados pela prática do crime de associação criminosa (artigo 288, Código Penal) e não pelo crime de organização criminosa (Lei nº 12.850/2013); logo, não cabe a aplicação do instituto da infiltração policial como meio de obtenção de prova. Além disso, entendeu-se que o policial militar da Força Nacional de Segurança Pública tinha a única finalidade de coletar dados e repassar informações ao CICC e a outros órgãos de Inteligência, sem qualquer

3 TJRJ, 7ª Câmara Criminal, HC nº 0066300-51.2014.8.19.0000, Rel. Des. Siro Darlan de Oliveira, j. 10 fev. 2015, DJ 19 fev. 2015.

vinculação a uma organização criminosa específica, e que sua atuação não era de um agente infiltrado, mas, sim, de um agente de Inteligência, cuja atividade é a defesa do próprio Estado. Julgou-se descabida a tese defensiva de ilicitude da prova pela ausência de autorização judicial para infiltração do policial, já que o crime imputado era o de associação criminosa, que prescinde de autorização judicial para infiltração policial. Denegou-se a ordem em decisão unânime.

No Superior Tribunal de Justiça[4]

A defesa impetrou recurso ordinário ao Superior Tribunal de Justiça contra decisão do Tribunal de Justiça do Rio de Janeiro e alegava que a atuação da testemunha (policial da Força Nacional de Segurança Pública) teria sido a de um agente policial infiltrado, que ganhou a confiança dos alvos da investigação ao usar uma história de cobertura. Aduziu ainda ao recurso que o acórdão da 7ª Câmara Criminal do Estado do Rio de Janeiro tratou uma infiltração ilícita de agente policial como uma simples atividade de Inteligência, e sustentou, ainda, que o único elemento de convicção contra um dos réus era parte do depoimento desse agente policial que mencionou a participação do denunciado como liderança dos grupos violentos, o que serviu de base à acusação criminal formulada. A defesa também requereu, no recurso, o reconhecimento da ilicitude da prova consistente no depoimento do agente policial.

O Ministro Relator Sebastião Reis Júnior entendeu que não se tratava de obtenção de prova produzida mediante a infiltração de agente policial, como previsto na Lei nº 12.850/2013, pois a decisão do Tribunal de Justiça do Rio de Janeiro deixara claro que o agente não atuou com o intuito de investigar suposta existência da organização criminosa, tampouco se fez passar por um de seus membros para com eles interagir, mas, no exercício da função para a qual foi legitimamente designado, como agente de Inteligência da Força Nacional de Segurança Pública, coletou informações sem nenhuma vinculação a uma organização criminosa específica, e, nessa condição, fora prestado seu depoimento. Votou o Relator para negar provimento ao recurso ordinário.

Com efeito, o Ministro Rogerio Schietti Cruz, após pedido de vista, apresentou voto divergente. Mencionou inicialmente que a atividade do agente infiltrado, consubstanciada em método secreto de investigação de delito, traduz dilema ético que envolve a adoção da atual política de segurança pública contra a criminalidade organizada, a exigir que essas novas formas de investigação passem pelo filtro de ponderação frente aos direitos fundamentais. Ressaltou que uma leitura apressada da legislação e da doutrina poderia sugerir que o ordenamento jurídico pátrio admite a infiltração apenas de agentes policiais, o que, segundo o Ministro, não é verdade, pois a infiltração é apenas um método de trabalho, comum tanto à atividade de Inteligência, quanto às investigações criminais, e salientou que a lei veda a infiltração de agentes de Inteligência no âmbito de investigação criminal.

Nesta perspectiva, o Ministro Rogerio Schietti Cruz, em seu voto-vista, distinguiu a

4 STJ, 6ª Turma, RHC nº 57.023/RJ, Rel. Min. Sebastião Reis Júnior, j. 8 ago. 2017, DJe 16 ago. 2017.

ação de infiltração em investigação criminal (nos termos da Lei nº 12.850/2013) da ação de Inteligência, e pontuou que a atividade de Inteligência, inclusive com infiltração, pode ser praticada tanto por agentes de Inteligência quanto por policiais, com uso de métodos moldados pelas necessidades práticas e circunstâncias que envolvem a Inteligência de segurança pública, que cuida do exercício legítimo, permanente e sistemático de ações especializadas para identificação e avaliação de ameaças reais ou potenciais na esfera de segurança pública, orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar a tomada de decisões pelos governos a fim de planejar e executar uma política de segurança pública, ao prevenir, neutralizar e reprimir atos atentatórios à ordem pública.

Atentou ainda o Ministro vistor, em seu voto divergente, que essa atividade exige a coleta e a busca de dados não-disponíveis e protegidos em ambiente hostil, por meio de metodologia específica, para transformá-los em conhecimentos que consigam expressar as intenções das pessoas envolvidas, possíveis ou prováveis consequências dos fatos, a fim de assessorar os destinatários do processo decisório. Não obstante, notou o Ministro que embora os métodos sejam de uso compartilhado, deve evidenciar-se a diferença de escopo entre ações de Inteligência e investigação criminal, de tal modo que agentes de Inteligência podem atuar infiltrados em ações de coletas de dados de interesse nacional, dentro dos protocolos do Sisbin, enquanto policiais podem atuar infiltrados, seja para apurar crimes nos termos da Lei nº 12.850/2013, como polícia judiciária, seja para realizar atos de Inteligência policial, como órgão de Inteligência.

O voto-vista aduziu ainda que os dois primeiros critérios para distinguir a infiltração em ação de Inteligência da efetuada em investigação criminal são a finalidade e a amplitude, posto que a ação de Inteligência tem função preventiva e foco voltado às complexidades das conjunturas sociais, enquanto a investigação criminal é reativa, e dela pode decorrer a prisão de investigados e concentrada na apuração exclusivamente dos fatos imputados. Outra diferença reside na fiscalização judicial, ao prever a Lei nº 12.850/2013 a exigência de que o pedido ministerial ou da autoridade policial descreva o alcance das tarefas dos agentes, confere ao juiz o dever de decidir motivadamente sobre os limites da atuação do agente policial, à luz das peculiaridades do caso concreto e da ponderação de valores entre a atividade invasiva e os direitos fundamentais em conflito.

Nesse entendimento, segundo o Ministro vistor, o que a lei veda é a infiltração de agentes de Inteligência no âmbito de investigação criminal, bem como o compartilhamento em investigação criminal de informações provenientes de infiltração em ação de Inteligência, visto que somente a infiltração prevista na Lei nº 12.850/2013 passa pelo crivo do controle judicial.

No caso, após estruturar essa concepção e entendimento conceitual, o Ministro Rogerio Schietti Cruz verificou a regularidade da atividade de coleta de dados em ação de Inteligência relativa ao plano de segurança da Copa do Mundo de 2014 pelo policial militar até o momento em que ele foi conduzido por agentes da Coordenadoria de Informação e Inteligência Policiais (Cinpol) à Delegacia de

Polícia e prestou depoimento sobre os fatos. Segundo o Ministro, até mesmo quando a testemunha, agente policial, necessitou, por força dos acontecimentos, utilizar-se de uma história de cobertura para ganhar a confiança dos manifestantes, não houve nenhuma ilegalidade, porque se tratava de medida inerente à condição de agente no momento em que coletava dados em ambiente hostil. Não haveria, pois, ilegalidade no uso de seu depoimento por ele ser mero informante. Contudo, a ilegalidade não estava na atuação do agente policial, mas, segundo o Ministro Rogerio Schietti Cruz, no compartilhamento dessas informações na investigação criminal da qual se originou a ação penal.

Segundo o Ministro vistor, não haveria nada ilegal como ação de Inteligência, pois, ainda que se infiltrasse nos grupos *black blocs*, o objetivo era produzir relatório de Inteligência para auxiliar a Força Nacional de Segurança Pública para o controle dos eventos que caracterizaram as manifestações de rua em 2013. Porém, ponderou o Ministro do Superior Tribunal de Justiça, que, por meio dessa infiltração, o policial obteve a confiança dos *black blocs* e reuniu dados e informações posteriormente transmitidos, via depoimento judicial, a inquérito policial instaurado pela Polícia Civil do Rio de Janeiro, e realizou, em essência, ação de infiltração policial que, para fins criminais, somente é legal nas hipóteses e nos termos da Lei nº 12.850/2013. Consignou-se que essa iniciativa policial se constituiu em meio de obtenção de prova e, portanto, inválida para produção de efeitos em ação penal.

Citou-se como exemplo o caso HC nº 149.250/SP (Operação Satiagraha)[5] em que o Superior Tribunal de Justiça concluiu pela impossibilidade de compartilhamento de dados entre a Abin e a Polícia Federal, pois, segundo o Ministro, não obstante algumas diferenças fáticas, a questão de fundo seria a mesma, visto que era importante distinguir as atividades de Inteligência e de investigação criminal, porque submetidas a filtros de legalidade diferentes e com escopos absolutamente diversos, para averiguar se houve ou não constrangimento ilegal.

No caso *Black blocs*, vislumbrou-se inquestionável prejuízo acarretado pelo aproveitamento de atividades de Inteligência na investigação criminal, porquanto manifesta a nulidade da prova produzida a partir do testemunho de agente de Inteligência que, ao operar na coleta de dados, não se submete aos requisitos legais próprios da investigação criminal. Assim, mesmo que reconheça não haver qualquer ilegalidade na ação de Inteligência, em conclusão diversa se chegou quanto à utilização das informações e dados, obtidos na ação de Inteligência, em investigação criminal voltada para apuração do crime de associação criminosa. Votou vencido o Ministro vistor na 6ª Turma, que reconheceu a ilicitude do depoimento do agente policial.

No Supremo Tribunal Federal[6]

Em face da decisão do Superior Tribunal de Justiça que negou provimento ao recurso ordinário, a defesa impetrou *habeas corpus* perante o Supremo Tribunal Federal e

5 STJ, 5ª Turma, HC nº 149.250/SP, Rel. Min. Adilson Vieira Macabu (Desembargador convocado do TJRJ), j. 7 jun. 2011, DJe 5 set. 2011.

6 STF, 2ª Turma, HC nº 147.837/RJ, Rel. Min. Gilmar Mendes, j. 26 fev. 2019, DJe 26 jun. 2019.

reiterou o pedido de reconhecimento da ilicitude da prova consistente no depoimento do policial militar infiltrado sem autorização judicial. O Ministro Relator Gilmar Mendes registrou que a controvérsia se restringia à possibilidade de utilização, em ação penal, de dados obtidos por agente policial infiltrado sem autorização judicial, cuja finalidade inicial seria subsidiar a Força Nacional de Segurança Pública para fins de elaboração de plano de segurança para a Copa do Mundo.

Após delimitar as distinções, ao adotar o que fora exposto pelo voto vencido do Ministro Rogerio Schietti Cruz no Superior Tribunal de Justiça, entendeu o Ministro Gilmar Mendes que o policial militar não precisava de autorização judicial para, nas ruas, colher dados destinados a orientar o plano de segurança para a Copa do Mundo, mas, no curso de sua atividade originária, infiltrou-se no grupo dos *black blocs* para, assim, proceder à autêntica investigação criminal, o que configura, segundo o Ministro do Supremo, evidente a clandestinidade da prova produzida, porquanto o referido policial, sem autorização judicial, ultrapassou os limites da atribuição que lhe foi dada e agiu como incontestável agente infiltrado. Logo, reside a ilegalidade não em sua designação para atuação na coleta de dados genéricos nas ruas do Rio de Janeiro, mas em sua infiltração, inclusive ao ingressar no grupo de mensagens *Telegram,* criado pelos investigados, e participar de reuniões do grupo em bares com a finalidade de realizar investigação criminal específica e subsidiar a condenação ocorrida.

O Ministro Relator no Supremo Tribunal Federal pontuou que as informações obtidas pelo agente policial não poderiam ser destinadas à persecução penal, pois isso demandaria prévia autorização judicial, e somente poderiam ser utilizadas com fins preventivos em atos de Inteligência governamental. Além disso, sustentou que embora os meios excepcionais de obtenção de prova sejam cabíveis apenas nas persecuções penais de delitos relacionados a organizações criminosas, os procedimentos probatórios regulados na Lei nº 12.850/2013 deveriam ser respeitados por analogia em casos de omissão legislativa. Votou o Relator para declarar a ilicitude da prova, o desentranhamento da infiltração policial realizada pelo agente da Força Nacional de Segurança Pública e de seus depoimentos prestados em sede policial e em Juízo, e para se declarar nula a sentença condenatória proferida, por ter seu embasamento em elementos probatórios declarados ilícitos.

Na Segunda Turma, o Ministro Edson Fachin acompanhou o voto do Relator e salientou que as circunstâncias da matéria acerca da associação criminosa acolheriam, nesta hipótese, por incidência legítima, a previsão da prévia autorização judicial do agente policial para obtenção de prova, e reconhecia a ilicitude do depoimento e o respectivo desentranhamento para que o magistrado de primeiro grau pudesse prolatar nova decisão, identificar os elementos contaminados pelas circunstâncias e expurgar dos autos as provas dependentes e originadas da ilícita.

Já a Ministra Cármen Lúcia, ao votar, afirmou a importância do caso, porque nele se examinava a diferença entre a atuação legítima de um policial que colabora e leva a efeito os instrumentos necessários para o exercício da Força Nacional e

o desbordamento dessa atuação sem a competente e necessária subsunção de sua atuação às determinações legais. Verificou ainda a Ministra que havia um quadro demonstrativo de infiltração inicial, no sentido de o agente policial estar presente e coletar informações, e que era imprescindível prévia autorização judicial para se fazer o controle, a fiscalização e, eventualmente, até a constrição daquilo que tivesse desbordado da legislação.

Ao acompanhar também o Relator, o Ministro Ricardo Lewandowski ressaltou a exigência, sempre que necessário e factível, de autorização judicial e mandado de busca e apreensão relativos a qualquer tipo de ação de natureza invasiva, quebra de sigilos telefônicos, fiscais, telemáticos, bancários, e infiltração em grupos específicos de natureza criminosa, pois o Poder Judiciário é o guardião último dos direitos e garantias fundamentais, conforme assenta a Constituição.

Análise crítica

No caso exposto, é possível vislumbrar problemas de duas ordens, um no campo da Inteligência e outro referente à Justiça Criminal. No que se refere à Inteligência policial, houve um problema de comando e de coordenação no exercício da atividade em nível tático-operacional, isto porque o produto Inteligência ficou absolutamente comprometido pelas Informações não terem sido geridas e direcionadas tão somente para o plano de segurança do governo para a Copa do Mundo no Rio de Janeiro, pois, muito embora o agente policial da Força Nacional de Segurança Pública tivesse transmitido em tempo real dados e informações ao nível estratégico, frisa-se que o produto da atividade de Inteligência deveria ter sido tratado com grau de sigilo adequado, e seu manuseio e seu conhecimento deveriam ser restritos somente a pessoas que tivessem necessidade de utilizá-lo (cf. FERNANDES, 2006, p. 17), o que não é o caso de uma investigação criminal que possui os instrumentos investigatórios próprios e os meios de obtenção de provas e elementos de informação para materializar a justa causa em matéria processual penal, tudo sob controle ministerial e judicial.

Ao compartilhar as informações colhidas em campo com o inquérito policial e a ação penal correspondente, o agente policial de Inteligência atuou em investigação criminal, e obteve dados e informações, mas limitado no tempo e no espaço ao nível tático-operacional, e não realizou o conhecimento em nível estratégico com o produto de Inteligência. Como salienta Fernando do Carmo Fernandes (2006, p. 19), fazer Inteligência não é só descobrir quem cometeu um ilícito, independentemente de sua natureza, ou quando o crime ocorrerá, mas sim buscar o entendimento sobre ações futuras e, principalmente, sobre o que isso significará, de forma isolada ou conjugada com outras situações semelhantes ou até diferentes. Assevera ainda o mesmo autor o risco que existe em se flexibilizar a atividade de Inteligência e, com isso, cometer-se distorções nas ações, no entendimento da missão, no produto elaborado e no papel da própria atividade.

No que se refere à Justiça Criminal, pelas decisões das instâncias judiciais no caso em referência, é possível verificar que as falhas e distorções que envolvem a concepção

e a realização da atividade de Inteligência comprometem o julgamento das ações penais. Observa-se que, até o caso chegar ao Supremo Tribunal Federal, o entendimento majoritário das instâncias inferiores era de que o policial "observador" de manifestações populares em função de Inteligência não se enquadraria no conceito de agente infiltrado, e que poder-se-ia usar as provas obtidas por esse meio, inclusive para oferecimento de denúncia e condenação penal. Há, ainda, um desconhecimento, pelo Judiciário, da função e da importância do magistrado que pode não só evitar a banalização do uso da infiltração, como impedir seu uso de forma irresponsável, pois o juiz é garantidor e ferramenta de aprimoramento deste meio especial de investigação (WOLFF, 2018, p. 106).

Em razão desse desconhecimento por grande parte dos magistrados, tanto das distinções e concepções que envolvem as atividades de Inteligência policial, quanto dos aspectos atinentes à infiltração do agente policial e do agente de Inteligência, tem-se por vezes, como no caso em referência, a declaração de nulidade de provas ilícitas, que gera nulidade de sentenças e decisões judiciais comprometedoras do devido processo legal e, sobretudo, da liberdade, porque "as regras probatórias devem ser vistas como normas de tutela da esfera pessoal de liberdade: seu valor é um valor de garantia" (GRINOVER, 2013, p. 415). Prova ilícita, ou obtida por meios ilícitos, é prova vedada que o será sempre que for contrária a uma específica norma legal ou a um princípio do direito positivo, segundo Ada Pellegrini Grinover (2013, p. 416).

Ademais, ensinou a referida doutrinadora que as provas ilícitas, consideradas pela Constituição como inadmissíveis, não existem como provas, não têm aptidão para surgirem como provas, daí sua total ineficácia e, além disso, recordou ainda que as *exclusionaries rules* do direito norte americano, aplicáveis para exclusão processual das provas obtidas por meios ilícitos *(illegal obtained evidence)*, têm como finalidade prevenir e reprimir as ilegalidades da polícia na interação com o cidadão e suas garantias constitucionais (GRINOVER, 2013, p. 424, 638).

Por outro lado, nem tudo é responsabilidade dos magistrados da Justiça Criminal e dos próprios agentes policiais, pois nota Rodolfo Queiroz Laterza haver no Brasil uma insipiência intolerável na utilização do instituto da infiltração policial, "até mesmo certo desprezo acadêmico e institucional, talvez em decorrência de estereótipos que aludem a infiltração policial às práticas arbitrárias perpetradas pelos órgãos de repressão política durante o regime militar" (2015, p. 252). Diz o mencionado autor que a Lei nº 12.850/2013 não esgotou os desafios operacionais e procedimentais inerentes a esta medida investigatória, pois as polícias deverão criar estruturas necessárias à capacitação, à formação e à especialização de policiais aptos psicológica e profissionalmente para serem selecionados para o cumprimento dessa diligência, desafiadora e iminentemente fatal, e que são necessárias a criação de uma doutrina policial operacional, a estruturação de uma escolástica com metodologia rigorosa e consolidação de uma estrutura organizacional que dê respaldo institucional, profissional e pessoal aos policiais que voluntariamente se ofereçam para o

cumprimento de tais funções (LATERZA, 2015, p. 263).

Não obstante, apesar das falhas institucionais, judiciais e legais que envolvem a infiltração de agentes policiais em investigações, como visto no caso *Black blocs*, e, também, como recorda Alexandre Lima Ferro, apesar da carência de legislação mais específica que defina claramente até onde a Inteligência pode ir e gere segurança a seus agentes, a base legal atual, comparada com a base legal existente há quinze anos, já sofreu grande evolução (FERRO, 2011, p. 28). Isso porque, no campo jurídico-penal, foi editada legislação definidora de organização criminosa que dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e respectivo procedimento criminal, e que incorpora, dessa maneira, previsão de infiltração policial (Lei nº 12.850/2013), além de norma antiterrorismo (Lei nº 13.260/2016), que regulamenta disposição constitucional. A par disso, no campo jurídico-institucional, nesse lapso temporal, sobressaem a instituição do Sisbin e criação da Abin (Lei nº 9.883/1999), a criação do Subsistema de Inteligência de Segurança Pública no âmbito do Sisbin (Decreto nº 3.695/2000), aprovação da Estratégia Nacional de Inteligência (Decreto de 15 de dezembro de 2017), bem como a regulamentação do artigo 144, § 7º da Constituição da República e instituição do Sistema Único de Segurança Pública (Lei nº 13.675/2018).

Tem-se, pois, um desenvolvimento contínuo da base jurídico-penal e institucional para as atividades de Inteligência e a atuação policial na segurança pública, muito embora se verifique, ainda, distorções na aplicação prática, como no caso de referência analisado que envolve a infiltração de agente, o enquadramento da atividade empreendida e respectivas consequências jurídicas.

Conclusão

Pelos julgamentos do caso *Black blocs* nas diversas instâncias do Poder Judiciário, vislumbra-se que, em nível tático-operacional, notadamente quando da realização de operações em campo por agentes policiais para obtenção de dados e informações relevantes, sobreleva-se incompreensão e confusão conceitual quanto à Inteligência em sua vertente Segurança Pública, o que pode apresentar riscos de cometimento de distorções nas ações, no entendimento da missão, no produto elaborado e no próprio papel da atividade desempenhada.

Com efeito, com a decisão do Supremo Tribunal Federal no caso em referência, adotada no HC nº 147.837/RJ influenciado, em grande medida, pelo voto-vista vencido no RHC nº 57.023/RJ do Superior Tribunal de Justiça, pode-se apontar as seguintes conclusões que envolvem as distinções entre agente infiltrado e agente de Inteligência, no âmbito da segurança pública: *i)* a infiltração é apenas um método de trabalho, comum tanto às atividades de Inteligência quanto às investigações criminais; *ii)* a lei veda a infiltração de agentes policiais de Inteligência no âmbito de investigação criminal, não no âmbito das atividades de Inteligência; *iii)* a finalidade e a amplitude da ação policial são critérios para distinção entre a infiltração em ação de Inteligência (função preventiva e voltada às complexidades das conjunturas sociais) e a efetuada em investigação criminal

(reativa, concentrada em apuração exclusiva dos fatos imputados e de que pode decorrer prisão); *iv)* a fiscalização judicial é critério distintivo da ação de infiltração de agentes policiais em tarefa de investigação, e exige-se decisão judicial prévia nos termos da Lei nº 12.850/2013; *v)* como só a infiltração do agente policial no âmbito da investigação criminal passa por controle judicial, é vedado o compartilhamento em investigação criminal de informações provenientes de infiltração de agentes de Inteligência; *vi)* embora o meio excepcional de obtenção de prova da infiltração de agentes policiais seja cabível apenas nas persecuções penais de delitos relacionados a organizações criminosas, os procedimentos probatórios regulados pela Lei nº 12.850/2013 devem ser respeitados por analogia em casos de omissão legislativa, e há incidência legítima para exigir prévia autorização judicial do agente policial para obtenção de prova em investigações criminais que envolvam outros delitos, como o de associação criminosa, verificado no caso *Black blocs*.

Referências

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. *Atividade de inteligência no Brasil (legislação).* Brasília: Abin, 2019. Disponível em: http://www.abin.gov.br/central-de-conteudos/publicacoes/. Acesso em: 4 out. 2019.

CLAUSER, Jerome K.; WEIR, Sandra M. *Intelligence research methodology:* an introduction to techniques and procedures for conducting research in defense intelligence. Washington, D.C.: Defense Intelligence School, 1975.

CLARK, Robert M. *Intelligence analysis:* estimation and prediction. Baltimore: American Literary Press, 1996.

DEPARTMENT OF THE ARMY, Headquarters. *Field Manual nº 100-6: FM 100-6 Information Operations.* Washington, D.C., 1996.

DEPARTMENT OF THE NAVY, Headquarters United States *Marine Corps. Marine Corps Doctrinal Publication (MCDP) 2: Intelligence.* Washington, D.C., 1997.

FERNANDES, Fernando do Carmo. Inteligência ou informações? *Revista Brasileira de Inteligência.* Brasília: Abin, v. 2, n. 3, p. 7-21, set. 2006.

FERRO, Alexandre Lima. Direito aplicado à atividade de inteligência: considerações sobre a legalidade da atividade de inteligência no Brasil. *Revista Brasileira de Inteligência.* Brasília: Abin, n. 6, p. 27-39, abr. 2011.

GABINETE DE SEGURANÇA INSTITUCIONAL. *Estratégia Nacional de Inteligência.* Brasília: GSI, 2017. Disponível em: http://www.abin.gov.br/conteudo/uploads/2015/05/ENINT.pdf. Acesso em: 4 out. 2019.

GRINOVER, Ada Pellegrini. *Provas ilícitas, interceptações e escutas.* Brasília: Gazeta Jurídica, 2013.

KENT, Sherman. *Informações estratégicas.* Tradução Cel. Hélio Freire. Rio de Janeiro: Biblioteca do Exército, 1967.

KRAEMER, Rodrigo. Incompreensão do conceito de inteligência na segurança pública. *Revista Brasileira de Inteligência.* Brasília: Abin, n. 10, p. 73-82, dez. 2015.

LATERZA, Rodolfo Queiroz. Breves considerações críticas sobre os desafios da infiltração policial da persecução penal. In: ZANOTTI, Bruno Taufer; SANTOS, Cleopas Isaías (Coord.). *Temas avançados de polícia judiciária.* Salvador: JusPodivm, 2015.

BRASIL. Ministério do Exército. Estado-Maior do Exército. *Instruções Provisórias IP 30-1 – A atividade de inteligência militar.* Brasília: EGCF, 1995.

PATRÍCIO, Josemária da Silva. Inteligência de segurança pública. *Revista Brasileira de Inteligência.* Brasília: Abin, v. 2, n. 3, p. 53-58, set. 2006.

PLATT, Washington. *Produção de informações estratégicas*. Tradução Maj. Álvaro Galvão Pereira e Cap. Heitor Aquino Ferreira. Rio de Janeiro: Biblioteca do Exército; Livraria Agir Editora, 1974.

RODRIGUES, Cristina Célia Fonseca. A atividade operacional em benefício da segurança pública: o controle ao crime organizado. *Revista Brasileira de Inteligência.* Brasília: Abin, n. 5, p. 57-64, out. 2009.

WOLFF, Rafael. *Agentes infiltrados:* o magistrado como garantidor e ferramenta de aprimoramento deste meio especial de investigação. 2. ed. São Paulo: Almedina, 2018.

PERFILAÇÃO OPERACIONAL: APLICAÇÕES NO RECRUTAMENTO DE FONTES HUMANAS

Maurício Viegas Pinto *

Resumo

O artigo examina a aplicação da perfilação operacional no recrutamento e na gestão de fontes humanas, em especial no que diz respeito ao procedimento de seleção dos alvos mais indicados para o cumprimento da missão. Inicialmente, descrevem-se os fundamentos da perfilação operacional com base no enfoque dos traços de personalidade. A seguir, apresenta-se a metodologia utilizada para aferir a percepção dos alunos que participaram de curso sobre o tema em 2018 e 2019. Os resultados obtidos nas duas turmas ministradas sugerem que o tema ainda é praticamente desconhecido entre membros da comunidade brasileira de Inteligência. A perfilação operacional foi validada pelos alunos, os quais a consideraram de grande relevância para o recrutamento de fontes humanas. Eles também avaliaram que a perfilação operacional poderia ser empregada nas suas respectivas unidades de Inteligência, e a maior parte deles demonstrou interesse pessoal em atuar com a aplicação dessa técnica.

Palavras-chaves: Inteligência de fontes humanas. Recrutamento de fontes humanas. Perfilação operacional.

INTELLIGENCE PROFILING: APPLICATIONS IN THE RECRUITMENT OF HUMAN SOURCES

Abstract

The article examines the use of Intelligence profiling in the recruitment and management of human sources, in particular with regard to the procedure for selecting the target most suitable for the accomplishment of the mission. Initially, the fundamentals of Intelligence profiling are described based on the personality traits approach. Then there is the methodology used to evaluate students' perceptions regarding the employment of Intelligence profiling. The results obtained in two classes taught in the years 2018 and 2019, respectively, suggest that the subject is still practically unknown among members of the Brazilian Intelligence community. The Intelligence profiling was validated by the students, who considered it of great relevance for the recruitment of human sources. Students also assessed that Intelligence profiling could be employed in their respective Intelligence units, and most of them demonstrated a personal interest in working with the application of this technique.

Keywords: *Human Intelligence. Recruitment of human sources. Intelligence profiling.*

* Especialista em Inteligência Estratégica pela Universidade Gama Filho e Instrutor do Instituto Ministro Luiz Vicente Cernicchiaro - Escola de Formação Judiciária do Distrito Federal.

Introdução

Este artigo utiliza a expressão "perfilação operacional" para designar a metodologia aplicada à identificação e à exploração de perfis comportamentais de alvos no recrutamento e na gestão de fontes humanas, mediante o emprego de técnicas operacionais. Nesse sentido, pretende-se diferenciá-la da perfilação tradicional, ou seja, daquela que se realiza com o consentimento da pessoa, por meio da aplicação de questionários e testes psicológicos.

Ao se observar as diversas etapas que constituem o recrutamento de fontes humanas, percebe-se a existência de processo contínuo de convencimento e persuasão[1], cujo ápice ocorre na fase da "abordagem", e se caracteriza pela anuência do alvo em atender ao que lhe fora demandado. O êxito nessa fase, contudo, está fortemente relacionado ao sucesso obtido nas etapas anteriores, as quais abrangem os procedimentos de "investigação", "seleção" e "aproximação" do alvo.

Conquanto o conhecimento sobre aspectos relacionados à personalidade do alvo seja fator decisivo em todas as fases do recrutamento, o sigilo imposto às ações de Inteligência – em especial no que tange ao trabalho com informantes e colaboradores – torna inviável, nesse contexto, solicitar a um alvo que ele se submeta à aplicação de questionários e testes psicológicos para o estabelecimento do seu perfil comportamental. Desse modo, entende-se como essencial o desenvolvimento de metodologia que permita a realização desse procedimento de forma sigilosa.

Nesse sentido, realizou-se a presente pesquisa com o objetivo de se verificar a validação – por parte de profissionais de Inteligência que participaram de dois cursos ministrados sobre o assunto nos anos de 2018 e 2019 – de metodologia destinada à inferência de perfis comportamentais a partir da observação, análise e interpretação de ambientes ocupados privativamente pelos alvos. Procurou-se averiguar também qual a percepção dos participantes da pesquisa quanto ao emprego dessa metodologia nas suas respectivas unidades de Inteligência e, de forma concreta, quantos deles teriam interesse pessoal em aplicar a técnica.

Ressalte-se que a viabilização de metodologia destinada à perfilação operacional em muito contribuiria para o desenvolvimento da atividade de Inteligência em nosso país, pois tornaria possível o compartilhamento de perfis comportamentais entre diferentes agências que operem com fontes humanas.

Fundamentos da perfilação operacional

Embora a habilidade persuasiva do recrutador seja elemento essencial no processo de recrutamento, o êxito na execução da "abordagem" depende, fundamentalmente, do resultado obtido nas fases anteriores. Nesse sentido, especial

1 Embora os verbos *convencer* e *persuadir* sejam usualmente tomados como sinônimos, eles possuem campos semânticos específicos e bem delimitados. Enquanto o "convencimento" se dá essencialmente no plano cognitivo e está mais relacionado aos argumentos de natureza racional, a "persuasão", de acordo com Abreu (2009, p. 15), ocorre quando "[...] alguém realiza algo que desejamos que ele realize".

atenção deve ser destinada às fases de "investigação", "seleção" e "aproximação", nas quais se procura, respectivamente, reunir dados operacionais sobre os alvos, identificar qual deles apresenta o perfil mais adequado para o cumprimento da missão e estabelecer o primeiro contato com o alvo selecionado.

Neste artigo, trataremos da aplicação da perfilação operacional especificamente nas fases de "investigação" e "seleção" de alvos. Outras aplicações, referentes aos procedimentos adotados durante as fases de "aproximação" e "abordagem", por exemplo, serão apresentadas de forma mais detalhada em estudos posteriores.

A princípio, deve-se salientar que o estudo de temas relacionados à personalidade colocanos em terreno complexo, em que sempre será mais prudente abordar o assunto em termos de tendências e probabilidades. Por essa razão, optou-se por desenvolver a presente pesquisa com base na abordagem dos traços de personalidade, os quais, no entendimento de Schultz e Schultz (2015, p. 198), constituem "formas constantes e duradouras de reagir ao nosso ambiente".

A partir desse entendimento, pode-se inferir os dois principais atributos de um traço: 1) "estabilidade": tendência de se manter ao longo do tempo; e 2) "consistência": tendência de se manifestar em diferentes situações.

Importante destacar, nesse contexto, que um traço não pode ser observado diretamente. Ao se afirmar, por exemplo, que uma pessoa é extrovertida, o que se está a dizer é que essa pessoa apresenta "indicadores de extroversão", tais como gostar de conversar, de participar de eventos sociais ou de fazer novos amigos. Em outras palavras, a partir de um conjunto de situações nas quais se observa comportamento semelhante, percebe-se a presença, em maior ou menor grau, de determinado traço de personalidade. Se, na perfilação tradicional, essas observações são feitas pela própria pessoa ao responder a testes e questionários desenvolvidos exclusivamente para essa finalidade, na perfilação operacional, por outro lado, essa observação deve ser realizada pelo profissional de Inteligência a partir da aplicação de metodologia específica[2].

Registre-se, ainda, que cada um dos traços que compõem a personalidade humana deve ser compreendido de forma bipolar, ou seja, o traço da extroversão, citado anteriormente, equivaleria a um eixo sobre o qual poderíamos posicionar toda e qualquer pessoa, desde a mais introvertida até a mais extrovertida.

Outra premissa a ser considerada para a observação e análise dos traços de personalidade é a concepção de que eles são independentes entre si.

Isso significa que o fato de um indivíduo apresentar alta ou baixa pontuação em determinado traço não afetaria a forma como ele se comportaria ao ser observado em relação a outros fatores da sua

2 Desde a primeira turma ministrada adotou-se a expressão *Intelligence Profiling* como referência à metodologia aplicada à perfilação operacional de alvos em ações de recrutamento de fontes humanas.

personalidade[3].

De acordo com essa perspectiva, todas as pessoas apresentariam, em maior ou menor grau, todos os traços de personalidade. Desse modo, ao identificar a intensidade com que os principais traços se manifestam em um alvo, seria possível estabelecer uma curva de perfil comportamental, a partir da qual poderiam ser feitas, com acentuado grau de sucesso, inferências a respeito da sua aptidão para o cumprimento da missão. Assim, de posse de perfil comportamental que aponte para uma tendência do alvo a adotar determinada conduta diante de uma situação específica, o recrutador poderia dispor de elementos mais objetivos para fundamentar a sua escolha durante a fase da "seleção".

Um importante desafio a ser enfrentado no processo de perfilação operacional consiste em identificar, entre as diversas condutas apresentadas pelo alvo, quais delas refletem verdadeiros traços de personalidade e quais poderiam ser resultantes de mero estado de ânimo (variação de humor que pode afetar a conduta de qualquer pessoa). Evidentemente, para que seja útil ao recrutador, o perfil operacional deve expressar aspectos que sejam estáveis, que perdurem no tempo. Isso somente será possível a partir da identificação correta dos traços de personalidade.

Para evitar o erro de se interpretar conduta isolada e pontual como reflexo de efetivo traço de personalidade, sugere-se que os comportamentos do alvo sejam observados por período razoável de tempo[4] e que metodologia criteriosa para a análise e a interpretação dos dados obtidos seja obrigatoriamente aplicada[5].

De acordo com *Gosling et al.* (2002), as teorias interacionistas[6] sugerem que os indivíduos selecionam e criam os seus ambientes sociais, tais como amizades e outras formas de relacionamento, com o propósito de reforçar as suas disposições, preferências e atitudes pessoais. Dessa maneira, indivíduos extrovertidos, por exemplo, tendem a se relacionar com pessoas que lhes permitam dar vazão a esse aspecto da sua natureza. Por extensão, os autores propõem que os ambientes físicos também seriam estruturados de modo a refletir e reforçar a natureza dos seus ocupantes. Em razão disso, assinalam a possibilidade de que observadores realizem inferências sobre o perfil comportamental das pessoas a partir de indícios encontrados nos ambientes que ocupem de forma privativa.

Para ilustrar essa linha de raciocínio, pode-se citar o exemplo de uma mesa de escritório muito bem organizada e mantida constantemente dessa forma, apesar de ser utilizada todos os dias. Um observador

3 Nesse sentido, conforme assinala McCrae (2008, p. 208), "saber que alguém é altamente ansioso não diz coisa alguma sobre quão extrovertida essa pessoa é".

4 Nas turmas ministradas em 2018 e 2019 o tempo destinado para cada equipe inferir um perfil comportamental preliminar do seu respectivo alvo foi de duas semanas. Evidentemente, muitas pesquisas ainda precisam ser desenvolvidas para que se possa determinar a duração adequada para esse período.

5 Durante o curso *Intelligence Profiling* apresenta-se aos alunos a proposta de uma metodologia que possa ser aplicada para a inferência de perfis comportamentais a partir da observação e análise de indícios ambientais.

6 Teorias que explicam a personalidade a partir da interação do indivíduo com o meio circundante.

atento poderia inferir um elevado grau de realização (conscienciosidade)[7] por parte de quem trabalha no local.

Note-se que duas premissas são basilares para que as ideias propostas por Gosling et al. (2002) sejam aplicáveis à metodologia de perfilação operacional: a primeira é a existência de relação efetiva entre indícios encontrados em ambientes ocupados privativamente pelo alvo e o seu respectivo perfil comportamental; e a segunda, a possibilidade de identificação, análise e interpretação, por parte de observador externo (profissional de Inteligência), dos indícios encontrados nesses ambientes.

Ao se considerar que as premissas acima sejam atendidas, novos elementos poderiam ser agregados à perfilação operacional. Registre-se ainda, quanto a esse aspecto, que Gosling et al. (2002) descrevem quatro tipos de indícios observáveis em ambientes ocupados de forma privativa, os quais, acredita-se, também possam ser aplicados para inferir o perfil comportamental de alvos em ações de recrutamento de fontes humanas[8]:

a) Indicadores de identidade voltados para si mesmo

Os autores assinalam que as pessoas passam a maior parte do tempo nas suas casas e nos seus locais de trabalho. Em razão disso e com o intuito de tornar esses espaços próprios, tendem a personalizá-los, a adorná-los com objetos que reforcem a sua visão de mundo, as suas crenças e os seus valores. Esses objetos constituiriam, por assim dizer, declarações simbólicas sobre o próprio alvo. Pode-se imaginar, como exemplo, um porta-retratos colocado na sala de trabalho, com a foto de um parente que o alvo tenha perdido em acidente de carro, cuja mera lembrança o faça refletir sobre a necessidade de dedicar mais tempo aos familiares, o que poderia sugerir uma faceta do traço de socialização ou amabilidade.

b) Indicadores de identidade voltados para terceiros

Pessoas também podem adornar os seus ambientes privativos com objetos que possuam significado compartilhado por terceiros. Esses objetos, segundo os autores, podem ser utilizados para comunicar os seus valores para outras pessoas que tenham acesso a esse ambiente. Deve-se destacar, contudo, que tal mecanismo pode ser de duas modalidades: sincero, quando realmente expresse crenças ou valores compartilhados pela pessoa, ou enganoso, quando é utilizado com a finalidade de exibir, estrategicamente, crenças ou valores que ela não possua. Para exemplificar esse último caso, pode-se citar a sala de trabalho de um alvo que tenha sido decorada com canecas e outros apetrechos referentes a determinado time de futebol, que, embora não seja efetivamente apreciado por ele, faça muito sucesso com outras

7 Um dos cinco grandes fatores do modelo *Big Five*, a realização ou conscienciosidade *(conscientiouness)* está associada aos aspectos de responsabilidade, cumprimento de normas, autodisciplina e organização.

8 Há registros de pesquisas anteriores no mesmo sentido. Já em 1942, nos Estados Unidos, o Escritório de Serviços Estratégicos (OSS) instituiu um programa para selecionar agentes especiais em que uma das tarefas consistia precisamente em solicitar aos candidatos que descrevessem o perfil de pessoas desconhecidas a partir de objetos que elas houvessem deixado nos seus respectivos aposentos.

pessoas que frequentem o local, e para as quais ele tenha interesse em se mostrar atrativo.

c) Vestígios de conduta interior

Os autores destacam, ainda, que pessoas com alta pontuação em determinado traço de personalidade tendem a realizar mais atos relacionados a esse traço do que outras, que demonstrem baixas pontuações. Note-se que a execução reiterada desses atos, nos mesmos ambientes, deixaria vestígios que poderiam ser identificados por um observador. Como exemplo, pode-se imaginar a presença de um cinzeiro com grande número de guimbas de cigarros, que tenham sido acesos recentemente, sobre a mesa de um alvo. Tal fato, ao menos potencialmente, refletiria estado de ansiedade, uma das facetas associadas ao traço do neuroticismo[9].

d) Vestígios de conduta exterior

O quarto tipo de indicador, assim como os anteriores, também integra a metodologia da perfilação operacional. Nesse caso, o objeto de observação são vestígios de condutas que, embora tenham sido gerados em locais externos, foram posteriormente transportados para o interior do ambiente. Curiosamente, algo semelhante ao exemplo citado pelos autores – a exibição do programa de uma ópera da qual o ocupante havia participado[10] – chegou, inclusive, a ser constatado durante os exercícios realizados pela primeira turma.

Metodologia da pesquisa

A presente pesquisa procurou verificar a validade da aplicação de perfis comportamentais, traçados a partir da observação das quatro tipologias citadas anteriormente, como instrumento de apoio para a *seleção* de alvos controlados[11] em ações de recrutamento de fontes humanas. Os dados foram aferidos por meio de um questionário semiestruturado, elaborado pelo autor. Ao todo, trinta e seis alunos participaram da pesquisa, dezesseis dos quais na primeira turma e vinte na segunda. As turmas foram heterogêneas, compostas por profissionais de diferentes unidades de Inteligência, civis e militares, com atuação tanto em âmbito estadual quanto federal. Os alunos organizaram-se em equipes compostas por quatro integrantes (quatro equipes na primeira turma e cinco equipes na segunda turma). Cada equipe elegeu um monitor (aluno responsável por fazer a interface com o instrutor durante a fase prática do exercício). O instrutor atribuiu, de forma aleatória, um alvo controlado para cada equipe, o que resultou na atribuição de quatro alvos controlados para a primeira turma e cinco para a segunda. Destaca-se, ainda, que os alvos eram, geralmente, servidores das próprias instituições nas quais os cursos foram ministrados, com exceção de dois casos específicos em que os alvos foram escolhidos entre funcionários

9 Conforme assinalam Hutz e Nunes (2001, p. 7), o neuroticismo "refere-se ao nível crônico de ajustamento e instabilidade emocional e representa as diferenças individuais que ocorrem quando pessoas experienciam padrões emocionais associados a um desconforto psíquico (aflição, angústia, sofrimento, etc.) e os estilos cognitivos e comportamentais decorrentes".

10 Em nosso exercício, o programa observado pelos alunos referia-se a um concerto de música clássica.

11 Para fins deste artigo, entende-se como *alvos controlados* aqueles que tenham sido previamente indicados por gestores das instituições em que os cursos foram realizados.

de empresas terceirizadas, prestadoras de serviço a essas instituições.

As equipes analisaram ambientes ocupados privativamente pelos seus respectivos alvos. Na sua grande maioria, esses ambientes eram salas e mesas de trabalho. A opção por restringir a análise unicamente aos objetos presentes nas mesas de trabalho ocorreu sempre que o uso da sala era compartilhado simultaneamente por mais de uma pessoa o que, de modo evidente, comprometeria o resultado das inferências realizadas sobre o perfil comportamental do alvo. O acesso aos ambientes foi efetuado de forma discreta, sempre durante o horário de expediente, e na presença dos seus ocupantes. Ao acessarem os ambientes que seriam posteriormente analisados, os alunos procuraram identificar e observar, de maneira minuciosa, os objetos que se encontravam no local. Para assegurar melhor apreensão das particularidades de cada ambiente, os acessos foram efetuados individualmente por todos os integrantes da equipe, de forma intercalada, durante o período de duas semanas. Com base nessas observações e, eventualmente, em algumas imagens obtidas, foram realizadas as inferências sobre o perfil comportamental dos alvos.

Ao final de cada turma em que a metodologia da perfilação operacional *(Intelligence Profiling)* foi avaliada, nos anos de 2018 e 2019, solicitou-se aos alunos que respondessem ao seguinte questionário[12], formatado em escala do tipo Likert, e assinalassem, entre as cinco opções de resposta, aquela que mais indicava o seu grau de concordância com a pergunta:

12 Neste primeiro artigo serão analisadas apenas as respostas fornecidas às perguntas nº 1, 2, 8 e 9.

Figura 1 - Questionário de pesquisa aplicado aos alunos das turmas 4 e 5 do curso *Intelligence Profil*

QUESTIONÁRIO DE AVALIAÇÃO DA METODOLOGIA DE PERFILAÇÃO OPERACIONAL				
1ª) Você participa de treinamentos que abordem o emprego da perfilação comportamental no recrutamento de fontes humanas?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
2ª) Você acredita que a perfilação operacional possa auxiliar durante a fase de seleção em uma ação de recrutamento de fontes humanas?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
3ª) Você acredita que a perfilação operacional possa auxiliar durante a fase de aproximação em uma ação de recrutamento de fontes humanas?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
4ª) Você acredita que a perfilação operacional possa auxiliar durante a fase de abordagem em uma ação de recrutamento de fontes humanas?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
5ª) Você acredita que a perfilação operacional possa auxiliar na identificação do profissional de Inteligência com o melhor perfil para desempenhar a função de recrutador?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
6ª) Você acredita que a perfilação operacional possa auxiliar na identificação do profissional de Inteligência com o melhor perfil para desempenhar a função de controlador?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
7ª) A sua unidade de Inteligência trabalha com o recrutamento de fontes humanas?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
8ª) Você acredita que a perfilação operacional possa ser aplicada em sua unidade de Inteligência?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
9ª) Você se interessaria em atuar com a perfilação operacional em sua unidade de Inteligência?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre
10ª) Você recomendaria ao gestor de sua unidade o emprego da metodologia de perfilação operacional?				
Não	Raramente	Ocasionalmente	Frequentemente	Sempre

Fonte: Elaboração própria.

Como forma de garantir a validade da metodologia aplicada, foram envidados esforços para que os alvos não tomassem conhecimento prévio sobre os exercícios que seriam realizados, o que poderia resultar na alteração intencional dos ambientes antes de serem observados pelos alunos. Esses esforços compreenderam, entre outras medidas, a assinatura de Termos de Compromisso e Manutenção de Sigilo (TCMS) por parte dos alunos e a orientação direcionada aos gestores quanto à necessidade de manutenção do sigilo em relação ao nome dos alvos indicados.

Dois requisitos foram considerados essenciais para que uma pessoa fosse indicada como alvo controlado no exercício de perfilação operacional: 1) a pessoa indicada, presumidamente, não deveria ter conhecimento sobre a realização do curso na sua instituição. Caso ela viesse a ter conhecimento do curso, não deveria saber detalhes sobre a temática a ser abordada em sala de aula; e 2) o gestor deveria ter livre acesso a essa pessoa para que lhe solicitasse, posteriormente, a realização de teste autodeclarado, cujo resultado seria confrontado com o perfil comportamental inferido pelos alunos durante a realização do exercício[13]. Atendidos esses requisitos, os nomes dos alvos foram distribuídos de

13 Embora essa confrontação ainda não tenha sido finalizada, pretende-se utilizá-la como base para a discussão sobre a efetividade da perfilação operacional em estudos posteriores.

forma aleatória aos monitores das equipes.

De posse dos nomes dos seus respectivos alvos, cada equipe elaborou um planejamento que destacava como seriam executadas as ações destinadas à obtenção dos dados necessários à inferência dos perfis operacionais. Deve-se ressaltar, quanto a esse aspecto, que, embora conteúdos provenientes de publicações em redes sociais tenham sido utilizados na elaboração desses planejamentos, a conclusão propriamente dita dos perfis comportamentais restringiu-se, em todos os casos, aos dados obtidos em ambientes ocupados privativamente pelos alvos.

Essa etapa do exercício, em ação efetiva de recrutamento operacional, estaria inserida no que costuma ser denominado como "fase de investigação", ou seja, a fase em que são empregadas técnicas operacionais para a obtenção de dados que permitam um "levantamento completo e minucioso sobre o alvo". Todas as equipes das duas turmas pesquisadas obtiveram êxito em acessar algum tipo de ambiente ocupado privativamente pelos seus respectivos alvos[14]. Em três casos também foram obtidas imagens que colaboraram para a análise posterior do ambiente.

Os ambientes a que os alunos tiveram acesso foram analisados e interpretados sob a perspectiva das quatro tipologias de indícios comportamentais apresentadas anteriormente. Os dados obtidos foram agrupados e correlacionados com os cinco grandes fatores[15] do modelo *Big Five,* o qual, nas palavras de Nunes, Hutz e Nunes (2010), tem sido extensamente estudado por possibilitar uma descrição simples, elegante e econômica da personalidade. Os cinco grandes fatores da personalidade do modelo *Big Five* podem ser descritos, de forma sucinta, da seguinte maneira[16]:

• "Abertura à experiência": descreve uma pessoa criativa, curiosa, imaginativa, visionária, precursora e eclética.

• "Realização": caracteriza uma pessoa eficiente, organizada, metódica, confiável, responsável e meticulosa.

• "Extroversão": caracteriza uma pessoa ativa, assertiva, enérgica, entusiasta, expansiva e falante.

• "Socialização": descreve uma pessoa solidária, fraterna, generosa, afável, compreensiva e confiante.

• "Neuroticismo": descreve uma pessoa ansiosa, autopiedosa, tensa, susceptível, instável e preocupada.

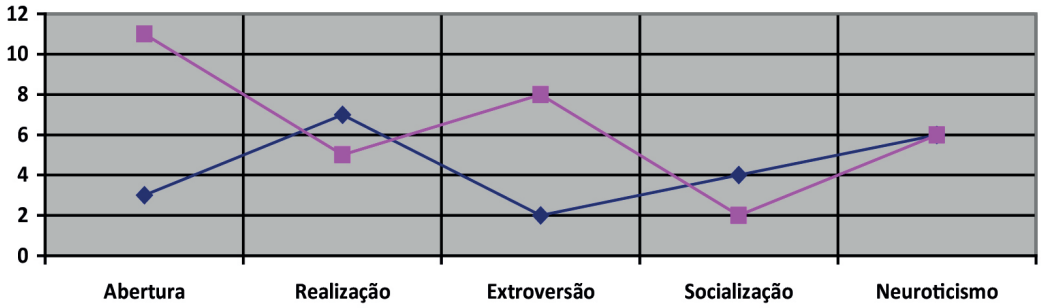
Após atribuir, com base nos dados obtidos, pontuação específica para cada um dos cinco grandes fatores da personalidade, os alunos representaram os resultados graficamente, por meio da geração de curva para o perfil comportamental dos seus respectivos alvos, conforme imagem a seguir:

14 Uma das equipes conseguiu acessar dois ambientes do mesmo alvo. Um deles era uma garagem que estava publicamente anunciada para aluguel durante o período do curso.

15 Utiliza-se, neste artigo, a nomenclatura adotada no Brasil, conforme citado por Silva e Nakano (2011).

16 Traduzido livremente e adaptado a partir da descrição em inglês feita por McCrae e John (1992).

Figura 2 - Comparação entre duas curvas de perfil comportamental traçadas pelos alunos em sala de aula.



Fonte: Elaboração própria.

A Figura 2 exemplifica a comparação entre as curvas de perfil comportamental, sobrepostas, de dois alvos nos cinco grandes fatores do modelo *Big Five,* elaboradas pelos alunos em sala de aula. Análise preliminar dos perfis obtidos já permitiria constatar que, embora os dois tenham recebido a mesma pontuação quanto ao fator "neuroticismo" e valores relativamente próximos para os fatores "socialização" e "realização", a pontuação atribuída aos alvos foi bem diferente no que tange aos aspectos "abertura à experiência" e "extroversão".

Enquanto a pontuação mais alta no fator "abertura à experiência" sugere um indivíduo mais curioso e propenso a aceitar ideias novas, que ainda não tenham sido experienciadas, a pontuação mais alta no fator "extroversão", por sua vez, tende a caracterizar um indivíduo com comportamento mais expansivo, enérgico e falante.

Nesse sentido, é importante registrar que não existe perfil comportamental que seja melhor que os demais para ações de recrutamento de fontes humanas. O que há, de fato, são perfis que estejam mais ajustados à natureza e às características da missão que deverá ser realizada.

Assim, na parte do exercício equivalente à fase da "seleção", os alunos realizaram quatro procedimentos distintos: 1) traçar o perfil operacional dos alvos; 2) identificar, com base na natureza da missão, quais características seriam desejadas (ou indesejadas) para o alvo a ser recrutado; 3) assinalar a quais fatores da personalidade essas características estariam mais associadas; e 4) com base nos fatores identificados e na curva resultante do perfil operacional, selecionar o alvo mais indicado para o cumprimento da missão.

No exemplo da figura apresentada acima, considerada a natureza da missão (que durante o curso foi descrita pelo instrutor em sala de aula como: "aproximar-se de um grupo de pessoas que organizam festas noturnas e supostamente estariam envolvidas com o tráfico de drogas") e a necessidade de selecionar apenas um dos alvos previamente assinalados para dar continuidade à ação de recrutamento, as equipes optaram, entre

os perfis analisados, por aquele que obteve as maiores pontuações em "abertura à experiência" e "extroversão". Isso porque os atributos desejados para o cumprimento da missão exigiriam, sobretudo, grande aptidão para o estabelecimento de novos relacionamentos interpessoais, habilidade que tende a se manifestar com maior intensidade em indivíduos que apresentem maiores pontuações nesses traços.

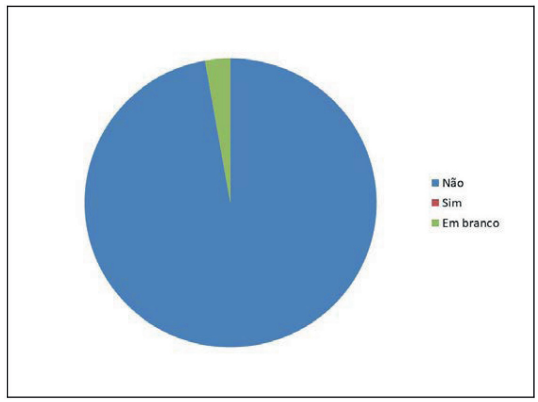
Observe-se que, usualmente, na fase da "seleção", já são considerados alguns critérios no intuito de tornar mais objetivo o procedimento de escolha do alvo a ser recrutado. Nesse sentido, costuma-se atribuir ao alvo um valor que indique o seu grau de acesso ao dado de interesse e outro que esteja relacionado à sua motivação. Desse modo, quanto maior a pontuação obtida pelo alvo nesses dois critérios (grau de acesso e motivação)[17], maior também a probabilidade de que ele seja selecionado, o que justifica a sua escolha de maneira mais objetiva e criteriosa em detrimento de outros alvos que também tenham sido previamente assinalados.

Não se propõe aqui a substituição de outros critérios, tradicionalmente utilizados na fase de "seleção", pela metodologia da perfilação operacional que, neste artigo, foi apresentada apenas de forma breve e superficial. Ao contrário, propõe-se tão somente agregar, aos critérios já aplicados, novo parâmetro, capaz de tornar mais efetiva a escolha a ser feita pelo recrutador.

Apresentação dos resultados

A primeira pergunta do questionário objetivou verificar se os alunos já haviam participado de algum treinamento que abordasse o emprego da perfilação comportamental no contexto do recrutamento de fontes humanas. Note-se que o aspecto verificado foi a "perfilação comportamental", de forma abrangente, a despeito da metodologia utilizada.

Figura 3 – Participação dos alunos em treinamentos que abordassem a temática da perfilação comportamental.



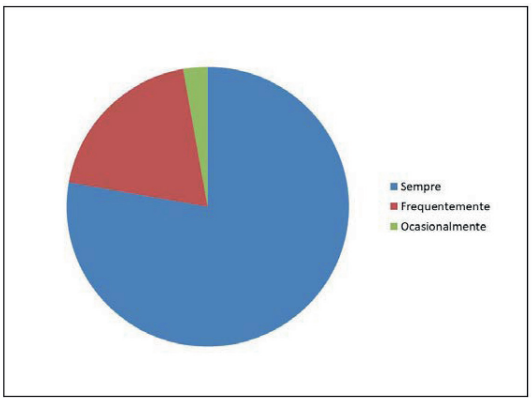
Fonte: Elaboração própria.

Embora um dos participantes tenha deixado esse campo do questionário em branco, trinta e cinco alunos declararam que "não", ou seja, mais de 97% dos que responderam informaram nunca ter participado de cursos que abordassem o emprego da perfilação comportamental nesse contexto. Sobre esse tema, as respostas sugerem a inexistência de treinamentos especializados. Importante destacar, contudo, que esse resultado pode ter sido influenciado pelo reduzido universo amostral da pesquisa (36 alunos).

17 Esses são apenas dois critérios ilustrativos entre vários outros que também poderiam ser utilizados.

A segunda pergunta buscou aferir se, na percepção dos alunos, a técnica da perfilação operacional poderia auxiliar durante a fase de seleção de alvos no recrutamento de fontes humanas[18].

Figura 4 – Percepção dos alunos sobre a aplicação da perfilação operacional na fase de seleção em ação de recrutamento de fontes humanas.

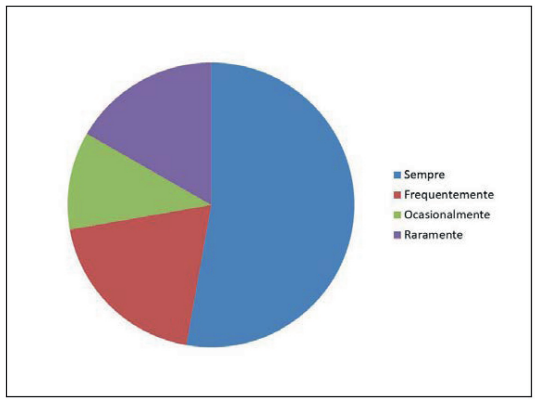


Fonte: Elaboração própria.

Vinte e oito alunos, mais de 77%, declararam "sempre", e outros sete, mais de 19%, responderam "frequentemente". Apenas um aluno informou "ocasionalmente". Os resultados obtidos com as respostas "sempre" e "frequentemente", se interpretados em conjunto, indicam que mais de 97% dos alunos validaram o emprego da perfilação operacional como instrumento eficaz para auxiliar o recrutador durante a fase de seleção de alvos em ação de recrutamento de fontes humanas.

A oitava pergunta procurou sondar se os alunos visualizavam a possibilidade de aplicação da metodologia de perfilação operacional nas suas respectivas unidades de Inteligência.

Figura 5 – Percepção dos alunos quanto à possibilidade de aplicação da perfilação operacional nas suas respectivas unidades de Inteligência.



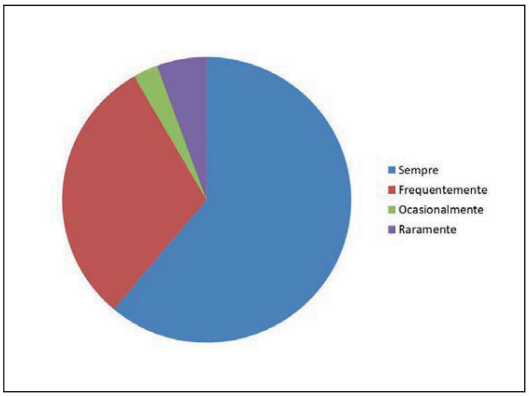
Fonte: Elaboração própria.

Dezenove alunos responderam "sempre"; sete assinalaram "frequentemente"; quatro marcaram "ocasionalmente"; e seis responderam "raramente". A soma dos resultados dos que informaram "sempre" e "frequentemente" resulta em mais de 72% das respostas, o que significa que, na percepção da maioria dos alunos, existe possibilidade concreta de aplicação da perfilação operacional nas suas respectivas agências.

A nona pergunta procurou aferir se haveria interesse pessoal por parte dos alunos em aplicar a metodologia da perfilação operacional nas suas respectivas agências.

18 Embora o questionário também contemplasse perguntas referentes às fases de aproximação e abordagem, os resultados obtidos em relação a esses quesitos serão apresentados em estudos posteriores.

Figura 6 – Interesse dos alunos em aplicar a perfilação operacional nas suas respectivas unidades de Inteligência.



Fonte: Elaboração própria.

Vinte e dois alunos responderam "sempre"; onze declararam "frequentemente"; um assinalou "ocasionalmente"; e dois marcaram "raramente". Ao somar as respostas dos alunos que declararam "sempre" e "frequentemente", percebe-se que mais de 91% dos participantes demonstraram interesse pessoal em aplicar a metodologia da perfilação operacional nas suas respectivas agências.

Considerações finais

Embora a pesquisa também tenha analisado a aplicação da perfilação operacional em outras fases do recrutamento de fontes humanas, optou-se por explorar, em artigos posteriores, os aspectos referentes às fases de "aproximação" e "abordagem", de forma a tratar separadamente as várias especificidades que envolvem esses temas. De fato, haveria muito ainda o que acrescentar sobre a própria fase da "seleção", abordada com maior ênfase neste artigo, todavia, julgou-se que este não seria o espaço adequado para fazê-lo. Em treinamentos ministrados com exclusividade para profissionais de Inteligência esses aspectos são abordados de forma mais detalhada.

Visualiza-se como essencial, neste momento, a padronização da metodologia destinada à perfilação operacional. Esse procedimento seria imprescindível para permitir o compartilhamento de perfis comportamentais entre diferentes unidades de Inteligência. Desse modo, acredita-se que, no futuro, seria possível a utilização do perfil operacional de um alvo, produzido por determinada unidade de Inteligência, por outras agências que necessitem realizar, por exemplo, entrevista com esse mesmo alvo. De fato, são inúmeros os cenários em que se poderia cogitar o emprego compartilhado de perfis comportamentais nas operações com fontes humanas.

Por fim, sugere-se que a perfilação operacional seja inserida no rol das técnicas operacionais e ações de busca empregadas pela Atividade de Inteligência. Com efeito, em consulta a algumas das principais doutrinas aplicadas em nosso país[19], identificou-se que não há, nos seus textos, qualquer menção que possa ser diretamente associada à metodologia de inferência de perfis comportamentais em operações destinadas ao recrutamento de informantes e colaboradores. Acredita-se que a previsão doutrinária da perfilação operacional em

19 Entre os documentos consultados, destacam-se as seguintes doutrinas: Doutrina Nacional de Inteligência de Segurança Pública – DNISP (BRASIL, 2014), Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro – DISPERJ (RIO DE JANEIRO, 2015), Doutrina Nacional de Inteligência Penitenciária – DNIP (BRASIL, 2013), Doutrina de Inteligência de Defesa (BRASIL, 2005), Doutrina Nacional de Inteligência: Bases Comuns (BRASIL, 2004) e o Manual de Operações de Inteligência do Exército Brasileiro: IP 30-4 (BRASIL, 1996).

muito contribuiria para a sua difusão entre profissionais de Inteligência de todo o Brasil, além de possibilitar o aperfeiçoamento da sua metodologia, que passaria a ser debatida e ensinada nas mais conceituadas Escolas de Inteligência do nosso país.

Referências

ABREU, A. S. *A arte de argumentar:* gerenciando razão e emoção. São Paulo: Ateliê Editorial, 2009.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (Brasil). Sistema Brasileiro de Inteligência. Conselho consultivo. *Manual de Inteligência:* Doutrina Nacional de Inteligência: bases comuns. Brasília, DF: Abin, 2004.

BRASIL. Ministério do Exército. Estado-Maior do Exército. *Manual de Operações de Inteligência do Exército Brasileiro IP 30-4*. 1. ed. Brasília, DF, 1996.

BRASIL. Ministério da Defesa. Departamento de Inteligência Estratégica. *Doutrina de Inteligência de Defesa.* 1. ed. Brasília, DF, 2005.

BRASIL. Ministério da Justiça. Departamento Penitenciário Nacional. Diretoria do Sistema Penitenciário Federal. *Doutrina Nacional de Inteligência Penitenciária (DNIP)*. Brasília, DF, 2013.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. *Doutrina Nacional de Inteligência de Segurança Pública (DNISP)*. 4. ed. rev. e atual. Brasília, DF, 2014.

GOSLING, S. D. et al. A room with a cue: personality judgments based on offices and bedrooms. *Journal of Personality and Social Psychology,* v. 82, n. 3, p. 379-398, 2002.

HUTZ, C. S.; NUNES, C. H. S. S. *Escala fatorial de ajustamento emocional/neuroticismo.* São Paulo: Casa do Psicólogo, 2001.

MCCRAE, R. R. O que é personalidade? *In:* FLORES-MENDOZA, C.; COLOM, R. *Introdução à psicologia das diferenças individuais.* Porto Alegre: Artmed, p. 203-218, 2008.

MCCRAE, R. R.; JOHN, O. P. An introduction to the five-factor model and its applications. *Journal of Personality,* v. 60, n. 2, p. 175-215, 1992.

NUNES, C. H. S. S.; HUTZ, C. S.; NUNES, M. F. O. *Bateria Fatorial de Personalidade (BFP):* Manual técnico. São Paulo: Casa do Psicólogo, 2010.

RIO DE JANEIRO (Estado). Secretaria de Estado de Segurança Pública. Subsecretaria de Inteligência. *Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ)*. Rio de Janeiro, 2015.

SCHULTZ, D. P.; SCHULTZ, S. E. *Teorias da personalidade*. Tradução Priscilla Lopes e Lívia Koeppl. 3. ed. São Paulo: Cengage Learning, 2015.

SILVA, I. B.; NAKANO, T. C. Modelo dos cinco grandes fatores da personalidade: análise de pesquisas. *Avaliação Psicológica,* v. 10, n. 1, p. 51-62, 2011.

ATIVIDADE DE INTELIGÊNCIA: LIMITES E POSSIBILIDADES DAS GUARDAS MUNICIPAIS COM O AVANÇO DAS LEGISLAÇÕES

Waleska Medeiros de Souza *

Resumo

Pretende-se com este estudo demostrar a importância do investimento na criação de setores de inteligência dentro da guarda municipal, bem como apontar os limites e as possibilidades que decorrem deste processo para o compartilhamento de conhecimentos. Para tal tarefa, foi feita uma pesquisa bibliográfica, com abordagem qualitativa sobre o assunto inteligência policial, que se balizou posteriormente no desenho da contrainteligência. Focalizaremos o conceito da contrainteligência como a proteção de conhecimentos produzidos pelas instituições. Buscaremos também demonstrar a necessidade de uma harmonia entre a proteção e o compartilhamento dos conhecimentos suscitados pelas organizações. Neste percurso metodológico investigativo, faremos um recorte para a instituição Guarda Municipal e seus ganhos potenciais a partir da promulgação da lei federal que cria a Política Nacional de Segurança Pública e Defesa Social (Pnspds) e institui o Sistema Único de Segurança Pública (Susp), com o viés para a implementação de setores de inteligência e a divulgação de informações entre agências de segurança pública. A criação de uma política e um sistema nacional de segurança pública foi anunciada como um divisor de águas no quesito produção e difusão do conhecimento institucional, ou seja, a melhoria no fluxo do compartilhamento das informações. A guarda municipal se insere neste processo de intercâmbio de informações. Disso surge a preocupação com quais dados podem ser compartilhados, e emerge a efetividade da contrainteligência dentro desta agência de segurança pública.

Palavras-chaves: Contrainteligência, Guarda Municipal, Inteligência de segurança pública.

INTELLIGENCE ACTIVITY: MUNICIPAL GUARDS 'LIMITS AND POSSIBILITIES WITH THE ADVANCE OF LEGISLATION

Abstract

The aim of this study is to demonstrate the importance of investing in the creation of intelligence sectors within the municipal guard, as well as to point out the limits and possibilities that derive from this process for the sharing of knowledge. For this task, a bibliographical research was carried out, with a qualitative approach on the subject of police intelligence, which was later used in the design of counterintelligence. We will focus on the concept of counterintelligence as the protection of knowledge produced by institutions. We will also try to demonstrate the need for a harmony between the protection and sharing of the knowledge raised by organizations. In this research methodological path we will highlight the Municipal Guard institution and its potential gains based on the promulgation of the federal law that creates the National Public Security and Social Defense Policy (Pnspds) and establishes the Public Security System (Susp), focused on the implementation of intelligence sectors and the dissemination of information among public security agencies. The creation of a national public security policy and system was announced as a watershed in the production and dissemination of institutional knowledge, i.e. improvement in the flow of information sharing. Thus, the municipal guard is inserted in this process of information exchange which generates the concern of which data can be shared. From this setting, the effectiveness of counterintelligence within this agency of public security emerges.

Keywords: *Counterintelligence, Municipal Guard, Intelligence of public security.strategy.*

* Graduada em Pedagogia pela UFOP. Pós-graduada em Neuropsicopedagogia, Educação Especial e Inclusiva pela Faveni. Pós-graduanda em Inteligência Policial pela Faveni.

Introdução

Com o aumento da criminalidade nas cidades brasileiras, nas últimas décadas, ocorreram movimentos massivos de implementação de guardas municipais por parte de prefeitos a fim de tentar conter e prevenir boa parte dos delitos ali cometidos. Nesse cenário de ampliação das guardas municipais (GM), ocorre a necessidade de investimentos em profissionalização de pessoal e a criação de setores específicos para garantir a efetividade na prevenção ao crime. Desses setores específicos, na atualidade, destacamos a inteligência policial para atender as reais necessidades da sociedade, a exemplo da prevenção ao crime organizado.

A atividade de inteligência desempenha um papel essencial em organizações de segurança, visto que lidam com um dos maiores patrimônios de uma sociedade: o conhecimento. Na atual sociedade da informação, quem tem conhecimento avança muito mais do que quem não o possui. Dessa forma, o domínio do conhecimento é condição indispensável para o desenvolvimento e a implementação de boas tomadas de decisão, por parte das agências de segurança pública, mais ainda as Guardas Municipais (GM) que atuam fixas nas localidades. A produção de conhecimento por parte de instituições policiais auxilia os gestores na adoção de políticas públicas efetivas em proveito dos sujeitos que compõe a sociedade, e pode ser muito eficaz nos municípios que possuem GM, por possuírem informações locais privilegiadas que favorecem a resolução do problema. Embora a atividade de inteligência seja uma valiosa ferramenta para a elaboração de políticas públicas voltadas à segurança pública e para a tomada de decisão na condução delas, ainda está pouco presente no campo dos estudos e investimentos estratégicos das guardas municipais, característica que representa um fator limitante da melhor ação a ser desempenhada, no que tange a inteligência.

Assim, esta pesquisa pretende demostrar a importância do investimento na criação de setores de inteligência na guarda municipal, bem como apontar os limites e as possibilidades que decorrem deste processo para o compartilhamento de conhecimentos. Para essa tarefa, primeiro será apresentada a definição dos conceitos de inteligência e contrainteligência, com foco na segurança pública. Posteriormente, faremos uma análise da instituição Guarda Municipal e de seus ganhos potenciais a partir da promulgação da lei federal que cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e institui o Sistema Único de Segurança Pública (Susp), com o viés para a implementação de setores de inteligência e a divulgação de informações entre agências de segurança pública. Por último, serão apresentados os aspectos conclusivos desta pesquisa.

Inteligência e contrainteligência: uma breve conceituação

A atividade da inteligência é descrita, *grosso modo,* como flexível, pois cada agência de segurança pública deve buscar o melhor desenho institucional que atenda aos seus interesses. A inteligência policial não se resume ao simples acúmulo de dados e fontes ocultas e/ou abertas. Logo, toda a informação coletada deve passar por um

tratamento qualitativo para se tornar relatório de inteligência, que subsidiará a melhor tomada de decisão por parte do gestor da instituição de segurança pública. Nesse contexto, percebemos que a inteligência se traduz em uma possibilidade de ações preventivas ao crime. No percurso conceitual, destacamos a definição contida no Decreto nº 4.376/2002, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência (Sisbin):

> Art. 2o [...] entende-se como inteligência a atividade de obtenção e análise de dados e informações e de produção e difusão de conhecimentos, dentro e fora do território nacional, relativos a fatos e situações de imediata ou potencial influência sobre o processo decisório, a ação governamental, a salvaguarda e a segurança da sociedade e do Estado (BRASIL, 2002).

Para o pesquisador brasileiro Cepik (2003, p. 27-32), a definição conceitual possui duas vertentes para inteligência: (i) conhecimento e/ou informação analisada e (ii) informação secreta, fruto de coleta de dados sem o devido consentimento. Já para Sims (1995), seria toda a coleta de informação que deve ser organizada e analisada para subsidiar a tomada de decisão dos gestores em suas atividades. A partir desta breve análise conceitual, a função dos órgãos de inteligência e suas atividades convergem para o auxílio do gestor no melhor ato decisório. Para este estudo, o gestor é o Comandante da instituição Guarda Municipal (CMT GM), pois o papel da GM, *grosso modo*, é a proteção dos direitos humanos fundamentais e a preservação da vida por meio de patrulhamento preventivo (BRASIL, 2014). Dessa forma, a atividade da inteligência compreende também "[...] a coleta e análise de informação para elaboração de um produto final – conhecimento – criado para instrumentar o processo decisório da gestão policial, tanto através da análise criminal tática quanto estratégica" (DANTAS, 2003, p. 1). Assim, o CMT GM, ao possuir documentos confiáveis e válidos de inteligência, pode propor ato decisório estratégico mais apropriado para a demanda. O autor Gonçalves (2016) elaborou um quadro ilustrativo (quadro I) do ciclo da inteligência, que se traduz em:

Quadro I - Ciclo da inteligência: do evento à inteligência

Fonte: (GONÇALVES, 2016, p. 16)

A partir dos estudos de Dantas (2003) e de Gonçalves (2016), conclui-se que o objeto com que a atividade da inteligência policial trabalha é a informação, que, tratada, torna-se conhecimento de inteligência. A atividade da inteligência é uma ação de ato contínuo, de caráter sensível e/ou sigilosa que subsidia a tomada de decisão. Assim, caminhamos para o segundo conceito que precisa de definição, ou seja, a contrainteligência, que entendemos como:

> Art. 3º [...] a atividade que objetiva prevenir, detectar, obstruir e neutralizar a inteligência adversa e ações de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem (BRASIL, 2002).

Sob o grande guarda-chuva da inteligência, há a contrainteligência, tão importante para o cuidado com o conhecimento produzido. A inteligência produz documentos orientadores (conhecimentos), e a contrainteligência os salvaguarda. Essa proteção do sistema é importante para a tomada de decisão eficiente por parte do CMT GM, pois, assim, pode planejar ações preventivas estratégicas na prevenção ou na mitigação ao crime. De tal modo, o CMT GM também protege a imagem e a missão da instituição, bem como a honra de seus subordinados, na garantia da divulgação de conhecimentos suficientes e confiáveis. Para tanto, há de se conhecer e identificar, no contexto em que a GM se insere, o que é um conhecimento sensível e/ou sigiloso, para que, a partir daí, passe a ser constituída uma

cultura de contrainteligência, que derivará em ações de proteção ao material produzido. Assim, identificamos que esse conhecimento é uma possibilidade e que sua salvaguarda é um desafio.

Por conseguinte, deve haver uma cultura de proteção dos conhecimentos e um cuidado quanto a quem esse material é compartilhado. O conhecimento produzido pela inteligência pode ser compartilhado com outras agências de segurança pública; a questão é o nível de intercâmbio desse produto. Para tanto, deve-se ter um equilíbrio entre a proteção do processo de produção de conhecimento pela GM e o seu compartilhamento com as demais instituições. Assim sendo, essa regulação do fluxo ocorre pela contrainteligência organizacional, atrelada à inteligência. A GM que não investe na criação do setor de inteligência/contrainteligência é o grande limite a ser superado, nesse contexto atual da sociedade da informação.

Após uma breve contextualização conceitual, passaremos a seguir para o aprofundamento das políticas nacionais em segurança pública no prisma da atividade de inteligência da guarda municipal, e com atenção a seus limites e suas potencialidades.

Guarda municipal: as políticas nacionais de segurança pelo viés da atividade de inteligência

Esta pesquisa reforça a importância da corporação Guarda Municipal no contexto da produção e do compartilhamento das informações de segurança pública, ao partir da premissa que as ocorrências e os crimes acontecem na esfera do município (ente federado). Por conseguinte, os servidores dessa instituição são lotados nos municípios e, em sua maioria, são nativos ou passam a residir no local. Dessa forma, conseguem estreitar as relações com a comunidade, passam a possuir informações privilegiadas e importantes que podem auxiliar na atividade de inteligência da GM. Daí a relevância dessa agência se inserir em políticas nacionais de segurança pública; neste caso, focalizaremos as atividades de inteligência. Para isto, faremos um mosaico com políticas nacionais e a inferência com a Guarda Municipal.

O primeiro documento norteador que abordaremos é a Lei n° 9.883, de 7 de dezembro de 1999, que instituiu o Sistema Brasileiro de Inteligência e criou a Agência Brasileira de Inteligência (Abin). Esta lei prevê:

> Art. 2° Os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do Presidente da República.
>
> § 1° O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.
>
> § 2° Mediante ajustes específicos e convênios, ouvido o competente órgão de controle externo da atividade de inteligência, as Unidades da Federação poderão compor o Sistema Brasileiro de Inteligência (BRASIL, 1999)

Este documento esclarece o conceito e a filosofia da inteligência a serem instituídos pela Federação a partir de então. Assegura que as demais unidades da Federação poderão integrar o Sistema Brasileiro de Inteligência (Sisbin). Nesse ponto, percebemos as potencialidades do conhecimento de inteligência produzido pela GM, uma vez que este conteúdo pode ser compartilhado pelo SBI, no subsídio da melhor tomada de decisão pelos entes federados.

Em virtude da Lei n° 9.883 de 1999, em 13 de setembro de 2002, foi promulgado o Decreto nº 4.376, que dispõe sobre a organização e o funcionamento do Sisbin. O art. 4° define, em seu parágrafo único, que "Mediante ajustes específicos e convênios, ouvido o competente órgão de controle externo da atividade de inteligência, as unidades da Federação poderão compor o Sistema Brasileiro de Inteligência" (BRASIL, 2002). Em virtude deste parágrafo, observa-se o reforço na garantia da integração das demais agencias de segurança pública, entre elas, a guarda municipal, no compartilhamento e na produção de conhecimentos de inteligência. Deste decreto, destacamos a diretriz a ser seguida, no âmbito de suas competências, para os órgãos que compõem o SBI, art. 6°:

> I - produzir conhecimentos, em atendimento às prescrições dos planos e programas de inteligência, decorrentes da Política Nacional de Inteligência;
>
> II - planejar e executar ações relativas à obtenção e integração de dados e informações;
>
> III - intercambiar informações necessárias à produção de conhecimentos relacionados com as atividades de inteligência e contra-inteligência;
>
> IV - fornecer ao órgão central do Sistema, para fins de integração, informações e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais; e
>
> V - estabelecer os respectivos mecanismos e procedimentos particulares necessários às comunicações e ao intercâmbio de informações e conhecimentos no âmbito do Sistema, observando medidas e procedimentos de segurança e sigilo, sob coordenação da ABIN, com base na legislação pertinente em vigor (BRASIL, 2002).

Observamos, nesse excerto da legislação, a evidência para conceito de intercâmbio de informações entre os integrantes que compões o Sisbin. Para essa tarefa, há de ocorrer a articulação coordenada dos órgãos, e há de se respeitar "a autonomia funcional de cada um e observadas as normas legais pertinentes a segurança, sigilo profissional e salvaguarda de assuntos sigilosos" (BRASIL, 2002). Dessa forma, a articulação da GM junto a outros órgãos ainda é um grande limite, visto que seu protagonismo na segurança pública ainda é muito recente, só foi alcançado efetivamente após a criação do Estatuto Geral das Guardas Municipais (BRASIL, 2014). Com essa característica, essa ação de intercâmbio da inteligência é regida pelo compartilhamento e pela salvaguarda do material produzido; logo, existem produtos de inteligência desenvolvidos pela GM que só interessam à municipalidade e outros que devem ser divididos com outras instituições que atuem na mesma localidade e/ou com o Sisbin, por afetarem outras esferas. Defendemos que o curso inverso também deve contemplar a instituição GM, ou seja, as informações produzidas por outras esferas, quando afetem a municipalidade, devem ser

divididas, fluxo que vemos pouco ocorrer. No problema de fluxo de conhecimentos compartilhados, encontramos os limites de uma política nacional, quando poderia focalizar nas potencialidades do intercâmbio entre as agências de segurança pública.

Neste percurso cronológico de políticas nacionais, passaremos para a especificidade da Guarda Municipal com a publicação da Lei nº 13.022, de 8 de agosto de 2014, que dispõe sobre o Estatuto Geral das Guardas Municipais. Deste documento norteador, destacamos, entre outras, algumas das competências atribuídas a seus integrantes: colaborar, de forma integrada com os órgãos de segurança pública, em ações conjuntas que contribuam com a paz social e estabelecer parcerias com os órgãos estaduais e da União, ou de municípios vizinhos, por meio da celebração de convênios ou consórcios, com vistas ao desenvolvimento de ações preventivas integradas (BRASIL, 2014). Percebe-se que a colaboração técnica com os demais entes federados e organizações é uma premissa atribuída à instituição GM. Muitas vezes, a via é de mão única, pois as guardas municipais compartilham seu conhecimento de inteligência e, em sua maioria, não recebem informações elaboradas por outras instituições, que são relevantes à adoção eficaz na tomada de decisão.

Chegamos a última legislação federal analisada para esse estudo, a Lei nº 13.675, de 11 de junho de 2018, que cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e institui o Sistema Único de Segurança Pública (Susp). Este documento, em seu art. 9°, traz a composição do Susp, de que, entre outros, está a guarda municipal. Esta legislação assegura o compartilhamento da atividade de inteligência e prevê:

> Art. 10. A integração e a coordenação dos órgãos integrantes do Susp dar-se-ão nos limites das respectivas competências, por meio de:
>
> I - operações com planejamento e execução integrados;
>
> II - estratégias comuns para atuação na prevenção e no controle qualificado de infrações penais;
>
> III - aceitação mútua de registro de ocorrência policial;
>
> IV - compartilhamento de informações, inclusive com o Sistema Brasileiro de Inteligência (Sisbin);
>
> V - intercâmbio de conhecimentos técnicos e científicos;
>
> VI - integração das informações e dos dados de segurança pública por meio do Sinesp (BRASIL, 2018)

Nota-se a preocupação do documento com a produção e a difusão do conhecimento produzido pela atividade de inteligência entre os órgãos que o integram. Desta forma, aborda que o intercâmbio do conhecimento será, preferencialmente, realizado por meio eletrônico para facilitar o acesso de todos aos dados, devido à grande extensão territorial que é o Brasil. Outro limite vivenciado é o acesso eletrônico aos registros, visto que muitas instituições ainda não foram introduzidas em bancos de dados estaduais, a exemplo de Minas Gerais e da dificuldade da GM em ser inserida para Registro de Eventos de Defesa Social (Reds) (MIRANDA, 2015). Infelizmente, ainda não é uma realidade este compartilhamento de todos os dados coletados, e não foi anunciado pelo órgão competente como esta ação ocorrerá, e se será disponibilizado

um cadastro único de registro de eventos.

No planejamento organizacional que as guardas municipais estão promovendo para se integrarem ao Susp, há de se investir na atividade de inteligência, posto que o domínio do conhecimento é uma condição essencial para o desenvolvimento de uma instituição de segurança pública, como a GM. Assim:

> Aqui convém destacar que o destino final de um documento de inteligência não é a publicação, divulgação, ou instrução de um processo administrativo, conclusão de um inquérito e produção de provas. O relatório de inteligência destina-se ao tomador de decisão e tem o objetivo de esclarecê-lo, contribuindo para o processo decisório daquela autoridade (GONÇALVES, 2016, p. 14).

A Lei nº 13.675/2018 também instituiu a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e trouxe como objetivos, entre outros, fomentar a integração em ações estratégicas e operacionais, em atividades de inteligência de segurança pública e em gerenciamento de crises e incidentes, e estimular o intercâmbio de informações de inteligência de segurança pública com instituições estrangeiras congêneres (BRASIL, 2018). Em decorrência dessa política, a GM, ainda de forma tímida, passou a criar setores específicos e especializados de inteligência, na esperança do intercâmbio do conhecimento, de um melhoramento estrutural e de suas ações gerenciais, operacionais e administrativas. Nesse processo, "não há nada mais importante nas informações do que as relações adequadas entre o seu pessoal e as pessoas que utilizam o produto de seu trabalho" (KENT, 1967, p. 173).

Kent (1967) alerta que as informações transformadas em conhecimento e atividade da inteligência, em determinada medida, devem ser discutidas entre quem as produziu e os tomadores de decisão. Dessa maneira, o gestor reflete sobre a validade e a confiabilidade do relatório produzido, para que consiga conhecimentos imparciais, necessários e suficientes para a melhor decisão. Esse autor parte do princípio de que quem trabalha na produção da atividade de inteligência é pessoa dotada de valores pré-existentes que, de alguma maneira, podem incidir sobre o relatório, e pontua que:

> Uma equipe de informações [inteligência] habituada a esforçar-se para uma análise raciocinada e imparcial, para produzir algo de valor, tem suas dificuldades com os pontos de vista, posições, opiniões pessoais e linhas. Acima de tudo, ela é constituída de homens cujos padrões de raciocínio provavelmente colorirão suas hipóteses, e cujas hipóteses coloridas, provavelmente se tornarão uma conclusão mais atraente do que o demonstram as evidências (KENT, 1967, p. 189).

Esse assunto foi abordado ao final dessa seção para reforçar a complexidade que envolve o setor de inteligência e os documentos que eles produzem para a melhor tomada de decisão por parte do CMT GM. Ressaltamos que há de se ter pessoas, nestas instituições, especializadas e estudiosas sobre o assunto para evitar que ocorra um esvaziamento e uma banalização da atividade de inteligência. Simplesmente infiltrar, em um evento, um agente que não sabe o que deve fazer ou que escuta uma informação sensível e a expõe a todos pode criar discursos inapropriados. Como a GM é uma instituição que vem criando sua identidade na prevenção ao crime e compõe o Sisbin, esta questão é emergente

e latente, mesmo com os limites impostos de pouco investimento financeiro, de recursos humanos e de pouco compartilhamento da atividade de inteligência. A Guarda Municipal possui potencialidades quando se vale do privilégio de que os eventos ocorrem nos municípios, assim pode promover ações que auxiliam na melhor política pública de segurança pública, com o foco na prevenção.

Conclusão

No Brasil, ainda pouco se publica e se estuda sobre a atividade de inteligência policial; basta uma busca em periódicos científicos para esta constatação, visto que, até há poucas décadas, era ação mais restrita aos militares; contudo, assistimos essa mudança de paradigma a partir da criação da Abin e das ações que essa instituição desempenha. Com o avanço das questões nacionais, observamos a um avanço na criação de legislações que facilitaram e permitiram esse intercâmbio de produções de inteligência entre agências de segurança pública, porém as Guardas Municipais ainda não conseguiram muitos avanços nesse compartilhamento de conhecimentos; dessa forma, consideramos a principal dificuldade enfrentada por essa corporação, por falta de articulação interna ou externa. Percebemos que algumas políticas caminham lentamente e que sua execução ainda não está bem definida, como a integração, o intercambio e o compartilhamento de conhecimentos de inteligência, principalmente no que tange ao acesso as Guardas Municipais, o que configura um grande limite no caminho para a melhor tomada de decisão.

Observa-se, neste contexto, que a capacitação das pessoas que produzirão este conhecimento de inteligência é um fator essencial ao sucesso no cumprimento dos encargos a eles atribuídos. A maioria das GMs ainda possui seus altos quadros indicados por livre nomeação pelo executivo; essa ação; às vezes, não colabora com a necessidade de pessoal especializado, neutro e imparcial que os setores de inteligência precisam. Por conseguinte, essa atividade de inteligência necessita de mais pesquisas e estudos voltados ao tema, que permitam aos que nela ingressem o acesso a profissionalização para a adoção das ações estratégicas e para a produção de relatórios confiáveis e válidos. Acreditamos que a profissionalização e a produção de conhecimentos, neste contexto, sintetizam a maior possibilidade, na cultura organizacional, para a mais confiável, válida e melhor tomada de decisão.

Uma instituição de segurança pública que investe em serviço de inteligência está à frente de organizações que não as possuem. Esse investimento também passa por encontrar o melhor desenho do serviço de inteligência, e não se limita à simples cópia de modelos já existentes. Na atualidade, compreendemos que as poucas guardas municipais que já investiram em atividades de inteligências estão muito à frente das que não o fizeram, daí a importância das demais fazerem esse investimento, de forma válida e confiável, porque quem detém o conhecimento avança na prevenção, e quem não o tem fica para trás.

Referências

BRASIL. Decreto nº 4.376, de 13 de setembro de 2002. Dispõe sobre a organização e o funcionamento do sistema Brasileiro de Inteligência, instituído pela lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências. *Diário Oficial da União:* seção 1, Brasília, DF, 13 set. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/D4376.htm. Acesso em: 30 jun. 2019.

BRASIL. Lei n° 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. *Diário Oficial da União:* seção 1, Brasília, DF, 8 dez. 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm. Acesso em: 30 jun. 2019.

BRASIL. Lei nº 13.022, de 8 de agosto de 2014. Dispõe sobre o Estatuto Geral das Guardas Municipais. *Diário Oficial da União:* seção 1, Brasília, DF, 8 ago. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13022.htm. Acesso em: 30 jun. 2019.

BRASIL. Lei nº 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. *Diário Oficial da União:* seção 1, Brasília, DF, 11 jun. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13675.htm. Acesso em: 30 jun. 2019.

CEPIK, M. A. C. Espionagem e democracia. Rio de Janeiro: FGV, 2003.

DANTAS, G. F. de L. *A gestão científica da segurança pública:* estatísticas criminais. Paper elaborado em: 2002. Disponível em: http://www.vivaciência.com.br. Acesso em: 15 jun. 2019.

GONÇALVES, J. B. *Atividade de inteligência e legislação correlata.* 4. ed. Niterói: Impetus, 2016.

KENT, S. *Informações estratégicas.* Rio de Janeiro: Biblioteca do Exército Editora, 1967.

MIRANDA, B. Prefeitura quer guardas municipais registrando Boletins de Ocorrência. *O Tempo.* Belo Horizonte, 25 de mar. 2015. Disponível em: https://www.otempo.com.br/cidades/prefeitura-quer-guardas-municipais-registrando-boletins-de-ocorrencia-1.1014756. Acesso em: 15 jun. 2019.

SIMS, J. What is intelligence? Information for decision makers. In: GODSON, Roy; SCHMITT, G.; MAY, E. (ed.). *U.S. intelligence at the crossroads:* agenda for reform. New York: Brassey's, 1995.