e-ISSN 2595-4717
ISSN 1809-2632

RBI Revista Brasileira de Inteligência

20
Dezembro • 2025

ABIN

PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Revista Brasileira de Inteligência

2025 • Nº 20

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

Capa
Luciano Mendes

Projeto Gráfico
Luciano Mendes

Editoração Gráfica
Escola de Inteligência

Catalogação Bibliográfica Internacional, Normalização e Elaboração
Escola de Inteligência

Disponível em
http://rbi.abin.gov.br

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

Impressão
Agência Brasileira de Inteligência

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência.
– n.20 (dez. 2025) – Brasília: Abin, 2025.
Anual
ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online
1. Atividade de Inteligência – Periódicos – Brasil. 1. Agência Brasileira de Inteligência.

CDU: 355.40(81)(051)

Sumário

Revista Brasileira de Inteligência
2025 • nº 20 • Editorial
ISSN 2595-4717

Editorial

A Escola de Inteligência da ABIN apresenta à sociedade brasileira a 20ª edição da Revista Brasileira de Inteligência (RBI). Por vários motivos, essa edição constitui-se em um marco para a Agência e para os leitores interessados em assuntos de Inteligência de Estado.

O número consagra o projeto iniciado em 2024 de aprimoramento da RBI nos moldes científicos mais rigorosos, com adoção das melhores práticas editoriais. Reafirmamos nosso compromisso com a democratização do conhecimento, reforçando o acesso aberto a todos os artigos da Revista e a possibilidade de submissão gratuita de contribuições pelos autores.

Destacamos, ainda, a publicação contínua preconizada pela Biblioteca Eletrônica Científica Online (Scientific Electronic Library Online – SciELO), uma mudança que nos possibilitou agilizar a difusão do conhecimento, oferecendo amplo acesso e no menor tempo possível ao que há de mais avançado na literatura brasileira sobre as temáticas de Inteligência, mantendo os leitores na vanguarda das discussões.

O novo modelo da RBI está alinhado também ao objetivo de promover o campo interdisciplinar dos estudos sobre a Atividade de Inteligência. Esse objetivo foi revigorado com o lançamento, em maio de 2025, da Rede de Pesquisa em Inteligência Estratégica, iniciativa inédita no Brasil que visa à articulação entre universidades e instituições nacionais para estimular e fortalecer reflexão crítica na área.

Com apoio da Rede, a ABIN publicou, em dezembro de 2025, o segundo relatório ostensivo prospectivo "Desafios de Inteligência – Edição 2026" – convidamos os leitores interessados na temática de Inteligência a acessá-lo, gratuitamente, no repositório da Escola Nacional de Administração Pública

(Enap), outra escola de governo parceira da Esint.

É importante destacar, ainda, que todas essas iniciativas convergem para os esforços de consolidação da ABIN como Instituição Científica, Tecnológica e de Inovação (ICT), conforme anunciado em evento com autoridades do Ministério da Ciência, Tecnologia e Inovação (MCTI) em novembro de 2024. Esse outro marco histórico permite que a ABIN celebre acordos e convênios com órgãos públicos, agências de fomento, empresas privadas ou outras ICTs públicas ou privadas, para execução de projetos de pesquisa, desenvolvimento e inovação.

É nesse ânimo, em meio a tantas ações de fomento à "cultura de inteligência", que oferecemos aos leitores, na atual edição da RBI, dez artigos científicos. O conjunto de textos aborda, primeiramente, a questão da criminalidade transnacional, com o artigo "Narcossubmarinos no Oceano Atlântico: crime transnacional emergente, desafios para o Brasil". Em seguida, o segundo artigo traz contribuições para o aprimoramento do processo de produção do conhecimento de Inteligência, sob o título "A aplicação das técnicas de análise estruturadas no processo de análise de Inteligência".

O terceiro, intitulado "Formalizando a inclusão da neurodiversidade na Inteligência e defesa nacional do Brasil", oferece um novo olhar sobre as contribuições que a inclusão e a diversidade têm a oferecer aos trabalhos da Inteligência e da Defesa no Brasil. O quarto artigo aborda os limites das estratégias atuais de enfrentamento à questão da radicalização virtual terrorista com o título "A inadequação da estratégia da deterrance diante da radicalização virtual terrorista".

O quinto artigo, "Inteligência de Estado e ética no Brasil", investiga os paradigmas éticos e sua aplicação à inteligência. O sexto artigo, "Matriz SOC de difusão: uma ferramenta prática em auxílio à velocidade informacional", busca mapear desafios e oferecer solução aos problemas de integração das informações no âmbito da Atividade de Inteligência.

O sétimo artigo, sob o título "Aplicação dos fundamentos da Metodologia da Produção do Conhecimento para a Inteligência Cibernética", aborda os problemas que se situam na interface entre a metodologia de produção do conhecimento e as questões específicas afetas à inteligência e a defesa cibernéticas. O oitavo artigo, "Parâmetros legais para o uso estatal de ferramentas tecnológicas potencialmente intrusivas para fins de segurança", trata, por sua vez, dos problemas que se situam na interface entre as questões jurídicas e

o uso de ferramentas tecnológicas.

O nono artigo investiga, sob o título "A exploração de fatores humanos e tecnológicos em campanhas de desinformação patrocinadas por Estados-nações", o emprego de ações estruturadas de desinformação por parte de atores estrangeiros como instrumento de interferência externa. Por fim, o décimo artigo, no formato de "artigo curto", é intitulado "Desafios na formação de recursos humanos em Inteligência Estratégica de Defesa" e analisa o processo de formação e capacitação de recursos humanos por parte do Exército Brasileiro para a Atividade de Inteligência Estratégica de Defesa.

Manifesto profundo agradecimento a autores, pareceristas e editores pelo trabalho que, juntos, agora entregamos. Aos leitores, espero que encontrem nesta edição oportunidade de análise cuidadosa sobre uma atividade que muito tem a contribuir para integridade e prosperidade do Estado brasileiro.

Boa leitura!

Anna Cruz
Diretora da Escola de Inteligência da ABIN

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Artigo de pesquisa

Alberto Dantas[1]
ORCiD 0009-0007-2223-8334

NARCOSSUBMARINOS NO OCEANO ATLÂNTICO: CRIME TRANSNACIONAL EMERGENTE, DESAFIOS PARA O BRASIL

https://doi.org/10.58960/rbi.2025.20.255

Dantas, Alberto. 2025. "Narcossubmarinos no Oceano Atlântico: crime transnacional emergente, desafios para o Brasil," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.255. https://doi.org/10.58960/rbi.2025.20.255.

Recebido em 08/10/2024
Aprovado em 14/04/2025
Publicado em 22/04/2025

1 Agente de Polícia Federal. Bacharel em Direito pela Universidade Federal do Rio de Janeiro (UFRJ), com pós-graduação em nível de especialista em Inteligência Estratégica pela Escola Superior de Defesa (ESD). Especialista em Análise de Risco e em Organizações Criminosas Transnacionais.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

NARCOSSUBMARINOS NO OCEANO ATLÂNTICO: CRIME TRANSNACIONAL EMERGENTE, DESAFIOS PARA O BRASIL

Resumo

O uso de narcossubmarinos por organizações criminosas transnacionais no Oceano Atlântico com o objetivo de enviar cocaína a outros continentes (Europa e África, em especial), ainda carece de estudo e de avaliação mais acurada. À Inteligência cabe a tarefa de estruturar, mapear e analisar casos passados relacionados a narcossubmarinos, nos quais o Brasil (e seu entorno estratégico) foi parte principal ou acessória. Este estudo utiliza uma abordagem metodológica de análise de casos para aumentar a consciência situacional, a fim de apresentar caminhos para prevenção, redução e/ou mitigação de riscos associados a essa ameaça contemporânea, considerando os desafios e as oportunidades identificados. Os resultados destacam a necessidade de cooperação internacional e recomendam ações práticas para a Inteligência brasileira.

Palavras-chave: narcossubmarinos, organizações criminosas transnacionais, entorno estratégico brasileiro, Atlântico Sul, cooperação internacional em inteligência.

NARCO-SUBMARINES IN THE ATLANTIC OCEAN: EMERGING TRANSNATIONAL CRIME, CHALLENGES FOR BRAZIL

Abstract

The use of narco-submarines by transnational criminal organizations in the Atlantic Ocean to ship cocaine to other continents (especially Europe and Africa) still requires more accurate study and assessment. The task of intelligence is to structure, map and analyze past cases related to narco-submarines, in which Brazil (and its strategic environment) was a main or secondary party. This study uses a methodological approach of case analysis to increase situational awareness in order to present ways to prevent, reduce, and/or mitigate risks associated with this contemporary threat, considering the challenges and opportunities identified. The results highlight the need for international cooperation and recommend practical actions for Brazilian Intelligence.

Keywords*: narcosubmarines, transnational criminal organizations, strategic surroundings, South Atlantic, international cooperation in intelligence.*

NARCOSUBMARINOS EN EL ATLÁNTICO: CRIMEN TRANSNACIONAL EMERGENTE, DESAFÍOS PARA BRASIL

Resumen

El uso de narcosubmarinos por organizaciones criminales transnacionales en el océano Atlántico con el objetivo de enviar cocaína a otros continentes (Europa y África, en particular) aún requiere estudio y evaluación más precisa. La inteligencia es responsable de estructurar, mapear y analizar casos pasados relacionados con narcosubmarinos, en los que Brasil (y su entorno estratégico) fue parte principal o cómplice. Este estudio utiliza un enfoque metodológico de análisis de casos para aumentar la conciencia situacional con el fin de presentar vías para prevenir, reducir y/o mitigar los riesgos asociados a esta amenaza contemporánea, considerando los desafíos y oportunidades identificados. Los resultados destacan la necesidad de cooperación internacional y recomiendan acciones prácticas para la Inteligencia brasileña.

Palabras clave*: narcosubmarinos, organizaciones criminales transnacionales, entorno estratégico brasileño, Atlántico Sur, cooperación internacional en inteligencia.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Introdução

O tráfico de drogas por meio de narcossubmarinos no Oceano Atlântico, uma prática disruptiva na rota transatlântica da cocaína, foi comprovado em 2019 com a apreensão na Espanha do semissubmersível artesanal apelidado de "Che", tornando-se assim mais uma forma de manifestação da crescente criminalidade transnacional. Esse modus operandi constitui uma ameaça tanto interna quanto externa, com potencial capacidade de impactar negativamente o Brasil. Nesse contexto, destaca-se o papel da Inteligência em analisar e tratar esse risco de forma antecipada e preventiva, evitando que se torne mais um dos problemas críticos do país.

Este trabalho, de natureza exploratória, tem como objetivos principais analisar o uso de narcossubmarinos por organizações criminosas transnacionais no Oceano Atlântico, com foco na rota de cocaína para outros continentes, especialmente Europa e África; identificar os desafios e oportunidades que essa modalidade de tráfico de drogas apresenta para a segurança nacional e marítima do Brasil; e contribuir para futuras oportunidades de estudos, pois os resultados das pesquisas para consecução deste artigo demonstraram que há uma escassez de dados e conhecimentos no país acerca dessa temática, ainda insuficientemente analisada pela literatura nacional.

Além disso, este artigo busca identificar e estruturar casos passados relacionados a narcossubmarinos, nos quais o Brasil foi parte principal ou acessória, sendo esses casos essenciais para elaboração de estratégias de prevenção, redução e mitigação de riscos associados ao uso de narcossubmarinos, com base na análise preditiva e na consciência situacional. Nesse contexto, são apontados sete casos sobre narcossubmarinos nos quais o Brasil esteve inserido. A análise retrospectiva desses casos, combinada com a atual conjuntura que inclui inovações tecnológicas, poder econômico e a expansão internacional de facções criminosas brasileiras, possibilita ao fim o esboço de um minicenário sobre o tema em nosso país.

A metodologia aplicada neste estudo foi a pesquisa descritiva bibliográfica, complementada por uma análise de matérias jornalísticas. A pesquisa descritiva bibliográfica envolveu a revisão de literatura acadêmica relevante, incluindo artigos científicos, livros e relatórios técnicos, que forneceram a base teórica para a compreensão do fenômeno dos narcossubmarinos. As referências teóricas estão listadas ao final do trabalho.

As matérias jornalísticas foram utilizadas como fontes complementares, pois

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

documentam ocorrências recentes e específicas do uso de narcossubmarinos em território brasileiro, fornecendo dados empíricos que não estão disponíveis na literatura acadêmica. A inclusão dessas fontes jornalísticas foi essencial para contextualizar e ilustrar a aplicação prática do tema estudado, possibilitando uma perspectiva mais ampla e contextualizada sobre o tema estudado.

Adicionalmente, foi realizada uma análise retrospectiva dos casos, considerando a crescente incidência de casos envolvendo narcossubmarinos nas últimas três décadas em diversos países. Com relação ao Brasil, em especial no período de 2010 a 2025, identifica-se, mediante uma análise qualitativa, possíveis padrões e tendências relevantes para a Inteligência.

Breve histórico do fenômeno dos narcossubmarinos

O uso do termo narcossubmarino[1] abrange uma variedade de embarcações utilizadas no tráfico transnacional de drogas, especialmente cocaína e seus derivados. Trata-se de "embarcações marítimas autopropulsadas personalizadas destinadas ao contrabando de mercadorias ilícitas" (Jaramillo 2016, 50), difíceis de serem detectadas pelos sistemas de radares, sonares e infravermelhos, bem como por aviões de observação/monitoramento e satélites.

Dentre essa gama de embarcações estão os submarinos (*self-propelled fully--submersibles* – SPFS), os semissubmersíveis (*self-propelled semi-submersibles* – SPSS) e as embarcações de baixo perfil (*low profile vessel* – LPV), além dos narcotorpedos (contêineres de carga/tubos que são rebocados por barcos ou navios). Nos últimos anos, a maioria das apreensões são de LPV e/ou SPSS.

Essas embarcações, já utilizadas por mais de três décadas, principalmente nas águas do Pacífico e do Caribe, surgiram na Colômbia como uma evolução do tráfico por meio de lanchas ou barcos rápidos (*go-fast boats*) da década de 80 e início dos anos 90. Em meados da primeira década dos anos 2000, surgiram as primeiras embarcações de baixo perfil (*low profile vessel* – LPV, por não submergirem totalmente), inspiradas no design e uso das lanchas rápidas (*go-fast boats*). Essas embarcações oferecem melhor desempenho operacional, maior velocidade e tamanho, ao mesmo tempo em que mantêm a furtividade, uma vez que submergem quase completamente, tornando-as difíceis de serem detectadas. Além disso, em comparação com os submarinos

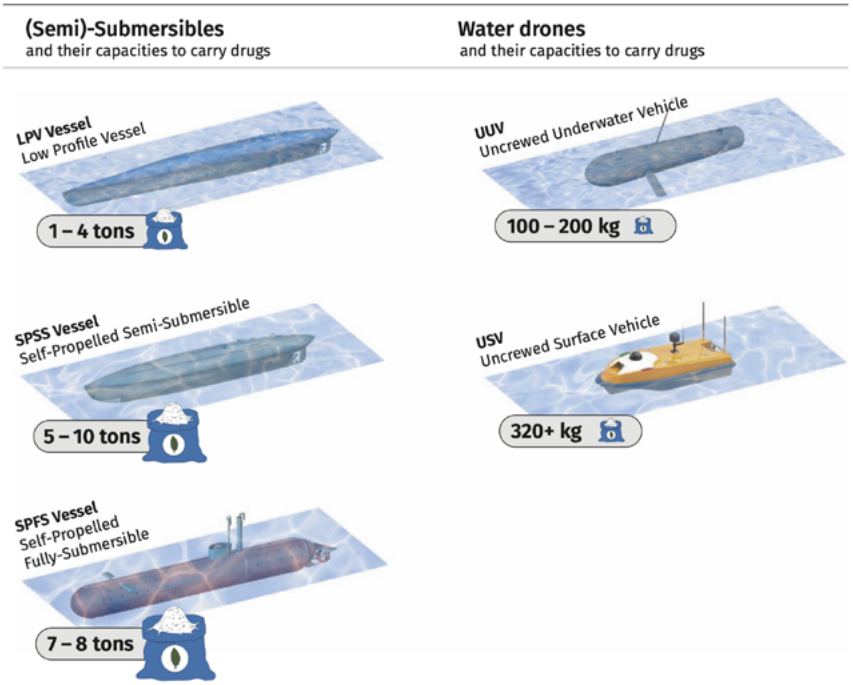
1 Definição em dicionário de Portugal: "embarcação submersível ou semissubmersível utilizada no tráfico de narcóticos, geralmente adaptada e equipada de forma específica para esse fim" (Infopédia, s.d.).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

artesanais, as LPV possuem menor custo de fabricação, variando de um a dois milhões de dólares.

O assunto abordado está em total consonância com a expansão da criminalidade organizada transnacional e o crescimento do modal narco-marítimo pelo Brasil e o mundo, conforme destacado no Global Report on Cocaine 2023 do Escritório das Nações Unidas sobre Drogas e Crime (*United Nations Office on Drugs and Crime* – UNODC), o qual adverte que há forte potencial para expansão na África e Ásia (UNODC 2023). Nesse relatório também é destacado o uso de narcossubmarinos (os *[semi]-submersibles*) e de drones subaquáticos (*water drones*) para transportar drogas (Figura 1).

Figura 1
Tipos de Narcossubmarinos e Drones Subaquáticos



Fonte: UNODC (2023, 170).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Apreensões em outros Países

Na Colômbia, o uso, construção, comercialização, posse e transporte de semissubmersíveis estão tipificados criminalmente com penas de até 14 anos de prisão (G1 2023). De 1993 até março de 2023, a Marinha da Colômbia apreendeu 228 narcossubmarinos (G1 2023). Dessas apreensões, 152 ocorreram no período de 2017 a 2021 (O Globo 2023a), o que representa aproximadamente 66,67% do total.

Em 9 de maio de 2023, a Marinha colombiana interceptou no Pacífico o maior narcossubmarino da história, resultando na prisão de 3 tripulantes e na apreensão de 3 toneladas de cocaína, avaliadas em 103 milhões de dólares. A embarcação tinha 30 metros de comprimento por 3 metros de largura (G1 2023). Até outubro de 2023, quando mais um semissubmersível foi apreendido pela Marinha da Colômbia – este com 20 metros de comprimento, contendo mais de 3 toneladas de cocaína e com 4 tripulantes presos –, já haviam sido apreendidos 19 semissubmersíveis durante o ano (O Globo 2023b), o que representa aproximadamente 8,33% do total de 228 narcossubmarinos apreendidos pela Marinha da Colômbia no período de 1993 a março de 2023.

Tem sido observado ao longo dos anos um aumento no uso de narcossubmarinos nas rotas do Pacífico. Além da Colômbia, há apreensões no Equador, Peru e países da América do Norte (México e Estados Unidos), bem como no Caribe, abrangendo também Venezuela, Suriname e Guiana; esses dois últimos localizados no Oceano Atlântico). Em geral, o destino final nesses casos são países do Caribe, México ou Estados Unidos da América.

No final de janeiro de 2024, operação conjunta dos governos da Colômbia e Equador resultou na apreensão marítima de dois narcossubmarinos: um no Equador, em 20 de janeiro de 2024, com quase três toneladas de cocaína e três tripulantes colombianos presos; e outro na Colômbia, em 21 de janeiro de 2024, com quase oitocentos quilos e três tripulantes presos; ambas as embarcações com 15 metros de comprimento (O Globo 2024).

No México, o maior narcossubmarino em dimensão (com 26 metros, 2 motores internos, velocidade média de 8 km/h e autonomia para navegar 20 dias) e capacidade de carga apreendido até então foi em 27 de junho de 2023. Ele foi interceptado pela Marinha mexicana no Oceano Pacífico, na região marítima do estado da Baixa Califórnia. Essa operação resultou na prisão de 5 tripulantes e a apreensão de 3,5 toneladas de cocaína (O Globo 2023c).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Em 2012, a *Drug Enforcement Administration* (DEA) já estimava que aproximadamente 30 por cento do fluxo marítimo de drogas dos Andes para os Estados Unidos se dava por meio de narco-submarinos (Jaramillo 2016, 50-51). Posto isso, ainda restava ocorrer a obtenção de alguma prova de que esses "*Frankenstein de la navegación*" (Romero 2022, 16) poderiam cruzar o Oceano Atlântico até a Europa e África. A engenharia e a tecnologia empregadas na construção dessas embarcações evoluíram bastante (Jaramillo 2016, 49-51), já tendo sido, inclusive, apreendidos narcossubmarinos totalmente elétricos, como na Colômbia em 2017, e totalmente submersíveis, como no Equador em 2010 e na Colômbia em 2011 e 2014 (CMCON 2022). Mas a evidência da capacidade dessas embarcações foi materializada em novembro de 2019, com a apreensão do primeiro narcossubmarino, no litoral da Espanha, oriundo da América do Sul, especificamente do Brasil (Romero 2022, 15-16).

Casos relacionados ao Brasil

Até o início de 2024, havia cinco casos envolvendo narcossubmarinos com relevância para estudo, análise e comparação, todos relacionados ao Brasil na "rota 'submersível' de drogas à Europa" (Soares 2023). O surgimento de um sexto caso, no final de fevereiro de 2024, com a apreensão de narcossubmarino na cidade de São Caetano do Odivelas, no Pará, região Norte do Brasil, intensificou ainda mais o alerta sobre o tema aqui apresentado. A sequência de eventos ganhou um novo patamar de complexidade com o sétimo caso, ocorrido mais recentemente, em 25 de março de 2025. Na Operação "Nautilus", a Polícia Judiciária Portuguesa interceptou, pela primeira vez, um narcossubmarino no Oceano Atlântico, próximo aos Açores, transportando entre 6,6 e 7 toneladas de cocaína. A operação, com colaboração internacional, resultou na prisão de cinco indivíduos, incluindo três brasileiros (CNN Portugal 2025).

Esses eventos não devem ser tratados isoladamente ou de forma restrita a uma análise meramente quantitativa. É importante analisá-los com cautela e preocupação, adotando uma análise essencialmente qualitativa, a fim de se compreender as nuances e complexidades envolvidas, como as motivações dos atores, os métodos utilizados e as consequências sociais e econômicas. Uma abordagem qualitativa permite exploração mais profunda dos fatores subjacentes e das implicações estratégicas, que não podem ser capturadas apenas por números e estatísticas.

A plausível hipótese de se estar diante de verdadeira cifra oculta marítimo-transatlântica não pode ser ignorada, representando uma nova ameaça à

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

segurança nacional do país e de seu entorno estratégico. Os sete casos envolvendo o Brasil, que constituem evidências significativas da existência de um ‘‘narcoeixo’’ submerso no Oceano Atlântico entre a América do Sul e Europa/África, estão explicitados a seguir:

1. Projetos de Construção (2010 a 2012).
    - Envolvimento de organizações criminosas do Centro-Oeste, cartéis e engenheiros colombianos.
    - Operação ‘‘Águas Profundas’’, deflagrada em 2014 pela Polícia Federal (PF) (Abreu 2021).
2. Apreensão em Vigia de Nazaré/PA (15 de dezembro de 2015).
    - Primeiro narcossubmarino apreendido no Brasil, em Vigia de Nazaré/Pará.
    - Envolvimento de organização criminosa transnacional colombiana, com um dos líderes preso em 2016 em Bogotá, Colômbia (CC 164457, STJ).
    - Vínculos com o cartel colombiano Clã do Golfo.
3. Apreensão no Suriname (fevereiro de 2018).
    - Narcossubmarino apreendido vazio no Suriname.
    - Motores adquiridos em Belém/PA em 2017 e 2018.
    - Operação ‘‘Flak’’, deflagrada em 2019 pela PF (IPL 069/2017 – DRE/DRCOR/SR/PF/TO).
4. Apreensão do ‘‘Che’’ na Espanha - Operação ‘‘Baluma’’ (24 de novembro de 2019).
    - Primeiro narcossubmarino apreendido na Europa (Operação ‘‘Baluma’’, na Espanha) proveniente da América do Sul, apelidado de ‘‘Che’’.
    - Piloto espanhol e dois tripulantes equatorianos presos (os três estiveram no Brasil).
    - Apreensão de carga superior a três toneladas de cocaína, com valor estimado em aproximadamente 140 milhões de euros.
    - Teria zarpado de Macapá/AP.
    - Vínculos com o cartel colombiano Clã do Golfo (Romero 2022).
5. Apreensão do ‘‘Poseidon’’ na Espanha (13 de março de 2023).
    - Segunda apreensão de narcossubmarino na Espanha (mesma região do ‘‘Che’’ de 2019).
    - Narcossubmarino já naufragado, sem tripulantes e drogas.
    - Vestígios encontrados no interior da embarcação indicam ligação com o Brasil.
    - Apelidado de ‘‘Poseidon’’, muito semelhante ao ‘‘Che’’ de 2019 (Sutton 2023).
6. Apreensão em São Caetano de Odivelas/PA (22 de fevereiro de 2024).
    - Segundo narcossubmarino apreendido no Brasil, nas proximidades do Farol do Itaipu em São Caetano de Odivelas/PA.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

- Pescadores da região informaram à polícia sobre a embarcação vazia à deriva.
- Apreendido com combustível e substância não identificada a bordo.

7. Primeira Apreensão de Narcossubmarino em Portugal – Operação "Nautilus" (25 de março de 2025).
    - Operação da Polícia Judiciária (PJ) portuguesa, denominada Operação "Nautilus", resultou na interceptação de um narcossubmarino no Oceano Atlântico, próximo aos Açores, transportando entre 6.6 e 7 toneladas de cocaína. Contou com a participação da Marinha e Força Aérea portuguesas, além da Guarda Civil da Espanha, DEA dos Estados Unidos e National Crime Agency (NCA) do Reino Unido.
    - A operação teve origem em informação compartilhada pela Guarda Civil da Espanha no Maritime Analysis and Operations Centre (Narcotics) (MAOC-N), com sede em Lisboa (EMFA 2025). A investigação está a cargo da Unidade Nacional de Combate ao Tráfico de Estupefacientes da PJ (Euronews 2025).
    - Presos cinco indivíduos: três brasileiros, um colombiano e um espanhol. Reportagens, alegadamente fundamentadas em investigações em curso, atestam que a embarcação partiu de Macapá/AP na foz do rio Amazonas, Brasil, tendo como destino o porto de Sines, em Portugal (Jozino 2025; Romero 2025).
    - As autoridades portuguesas não confirmaram, à época da apreensão, se há envolvimento de facções criminosas brasileiras na organização, tripulação e execução do transporte.

Ressalte-se que essa primeira apreensão em Portugal foi a quinta da Europa, sendo a quarta na Espanha, todas advindas da travessia do Oceano Atlântico. Além dos casos "Che" e "Poseidon", respectivamente de 2019 e 2023, em junho de 2024, quatro colombianos que tripulavam um narcosubmarino ao largo da costa da Espanha afundaram-no com a carga, após serem localizados pelos agentes aduaneiros, a cerca de 500 milhas a oeste de Cádiz, tendo sido posteriormente presos.

E, já em janeiro de 2025, um quarto narcossubmarino, de modelo distinto do "Che" e do "Poseidon" (Sutton 2025), foi encontrado nas águas da Costa da Morte, Galícia, na entrada do Estuário Camariñas-Muxía, onde foi deliberadamente afundado, após, provavelmente, sua carga ter sido descarregada. Nenhuma cocaína foi apreendida (Weerth 2025).

Com respeito às apreensões de 2015 em Vigia de Nazaré/PA e, nove anos após, a de 2024 em São Caetano do Odivelas/PA, ambas no Brasil, é pertinente ressaltar as observações de Chaves (2010), feitas cinco anos antes do evento em Vigia/PA na foz do rio Amazonas:

> [é] bastante possível que as conexões multimodais dessa logística da droga também envolvam, portanto, o problema dos narco-submersíveis,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

> que será trabalhado objetivamente nesta análise. Mas, afinal, o que são estes veículos de transporte da droga? Como eles afetam a segurança anti-narcóticos na América do Sul? Até que ponto o Brasil deve se preocupar com esta circulação ilícita?
>
> [...]
>
> PARA O BRASIL, IMPLICAÇÕES?
>
> Antes de qualquer crítica apressada a esta hipotetização, que se adianta aos fatos, é preciso sensibilidade para entender que o problema das chamadas 'novas ameaças' não necessariamente está relacionado a fatos ou ocorrências já presentes, mas a indisciplina nada coreografada dos vetores de agressão em um ambiente cada vez mais incerto, como é o mundo de hoje. Portanto, todo e qualquer exercício especulativo que venha a pensar ordenanças de defesa contra estas ameaças é de contribuição positiva para o debate sobre segurança nacional (Chaves 2010).

Bases constitucionais e infraconstitucionais

O tema ora tratado é pertinente para a Defesa e a Inteligência por possuir pontos de convergência com suas principais diretrizes normativas: Livro Branco de Defesa Nacional (LBDN), de 2020; Política Nacional de Defesa (PND), de 2024; Estratégia Nacional de Defesa (END), de 2024; Política Nacional de Inteligência (PNI), de 2016; e Estratégia Nacional de Inteligência (ENINT), de 2017.

Esses pontos de convergência se dão a partir da constatação de que o tema em estudo – narcossubmarinos e, por óbvio, as redes criminosas transnacionais complexas que desse modal se valem – deve ser analisado e enfrentado mediante uma interdependência entre os seguintes assuntos que constam do LBDN, da PND e da END: criminalidade organizada transnacional/transfronteiriça; defesa, soberania e securitização tanto da região Amazônica (abrangendo a Amazônia Legal/Verde e a Amazônia Azul[2]), assim como o entorno estratégico do país como um todo; e cooperação interagências, tanto em âmbito nacional quanto internacional.

É importante ressaltar que as normas e instrumentos legais que tratam do interesse da Defesa e da Inteligência também possuem pontos de contato com o Plano Estratégico da Marinha (PEM 2040), especialmente no que diz respeito ao combate à criminalidade organizada transnacional, à identificação de ameaças e à avaliação de conjunturas internas e externas.

Já a Inteligência permeia todas as esferas da segurança nacional, integrando-se de forma sinérgica com as políticas de defesa, soberania e segurança

2 Conforme a Marinha do Brasil (s.d.), "Amazônia Azul é a denominação do território marítimo brasileiro, que possui hoje aproximadamente de 3,6 milhões de km² referentes à soma da Zona Econômica Exclusiva (ZEE) com a Plataforma Continental (PC) do Brasil."

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

pública. Essa abordagem holística é essencial para enfrentar desafios emergentes, como o uso de narcossubmarinos por redes criminosas transnacionais, e promover a cooperação interagências, tanto em nível nacional quanto internacional.

Nessa esteira, denota-se perfeita aderência do tema às questões de soberania, defesa e segurança (nacional e pública), uma vez que, ocorrendo a incidência do ilícito, muito provavelmente se dará em área/região estratégica do país, no caso, na Amazônia Verde e/ou na Amazônia Azul (principal área de atuação do Poder Marítimo do Brasil), considerando-se os casos até aqui registrados. Dentre os Pontos-Chave do PEM 2040, encontra-se que

> [a] sociedade brasileira deve perceber o nosso entorno estratégico, que inclui o Atlântico Sul, como um ambiente onde nossa soberania e interesses no mar podem ser afetados por conflitos com outros Estados e ameaças multifacetadas, tais como terrorismo, pandemia, pirataria, crimes transnacionais e desastres ambientais (Brasil 2014).

No contexto brasileiro, em relação a esse "novo" fenômeno logístico-modal que consiste no envio de cocaína para o exterior via narcossubmarinos, Chaves (2010) já destacava em seu estudo que

> [...] não é de todo distante que pensemos a chegada (ou a tentativa de chegada) destes submersíveis no território nacional através do Amapá, extremo litoral norte do Brasil – ou até mesmo os diversos rios da nossa vasta bacia hidrográfica da Amazônia Ocidental, que conta com relativa expertise logística dos narcotraficantes em regiões de baixa densidade demográfica como a vasta fronteira com estes países acima listados e a Colômbia, uma das principais produtoras de cocaína do mundo.
>
> [...]
>
> De toda maneira, é de bom grado que estejamos atentos às novas possibilidades da logística do narcotráfico, que podem condicionar nossas políticas de segurança e as nossas fronteiras aos seus fluxos e rotas sazonais, com tecnologias disruptivas que forjam os mercados e os processos produtivos do crime transfronteiriço. Pretendeu-se aqui, modestamente, elencar um conjunto de fatores que se relacionam com um problema contemporâneo às águas da América do Sul, as quais o Brasil está emerso de modo indefectível. Um problema mútuo com ameaças que não distinguem nacionalidade; por sinal, uma questão sul-americana por excelência (Chaves 2010).

Por certo, outra ameaça que vem atrelada ao uso de narcossubmarinos no Atlântico é o domínio e o uso de determinada região fronteiriça do Brasil e seus países vizinhos por grupos criminosos articulados transnacionais. Destaca-se, ainda, o conceito de Defesa Nacional contido na PND e na END:

> DEFESA NACIONAL – É o conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do Território Nacional,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

> da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas (Brasil 2024, 77).

Na busca por uma atuação eficaz e eficiente no enfrentamento de ilícitos transfronteiriços e ambientais, especialmente na região Amazônica, cinco sistemas de monitoramento e controle, enfatizados no LBDN, são de extrema relevância: o Sistema de Gerenciamento da Amazônia Azul (SisGAAz); o Sistema Integrado de Monitoramento de Fronteiras (SISFRON); o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB); o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA); e o Sistema de Inteligência de Defesa (SINDE).

Dentre esses, destaca-se o SisGAAz para a ameaça dos narcossubmarinos. Coordenado e implementado pela Marinha do Brasil, o SisGAAz é uma ferramenta essencial para a governança e segurança marítima. Esse Programa Estratégico, operado em parceria com agências e órgãos governamentais, tem como missão monitorar e proteger continuamente as áreas marítimas de interesse e as águas interiores, portos, embarcações e infraestruturas, em face de ameaças, emergências, desastres ambientais, hostilidades ou ilegalidades, visando a segurança e a defesa da Amazônia Azul e o desenvolvimento nacional.

Além dos mecanismos de defesa, monitoramento, vigilância e controle da Amazônia já mencionados, o governo brasileiro instituiu em 2023 o Plano Amazônia: Segurança e Soberania (Plano AMAS) (Brasil 2023a), destinado ao desenvolvimento de ações de segurança pública que observem as necessidades e as especificidades dos 9 estados que compõem a Amazônia Legal (Acre, Amapá, Amazonas, Maranhão, Mato Grosso, Pará, Roraima, Rondônia e Tocantins) para o enfrentamento aos crimes na região, especialmente crimes ambientais e conexos.

O Plano AMAS foi um dos atos relativos à segurança pública no âmbito do Programa de Ação na Segurança (Brasil 2023b), lançado e apresentado na mesma data[3], no qual já havia expressa determinação de que o Decreto regulamentador do Plano AMAS deveria prever a implantação de 28 bases terrestres e 6 fluviais para combater crimes ambientais e infrações correlatas, totalizando 34 novas bases integradas de segurança (PF, PRF e Forças Estaduais).

3 Também como concretização de um dos eixos do PAS, o Ministério da Justiça e Segurança Pública (MJSP) lançou em 2 de outubro de 2023, o Programa Nacional de Enfrentamento às Organizações Criminosas (ENFOC) (Brasil 2023c), que envolve a participação da Secretaria Nacional de Segurança Pública (Senasp), Secretaria Nacional de Justiça (Senajus), Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos (Senad), Secretaria Nacional de Políticas Penais (Senappen), Polícia Federal (PF) e Polícia Rodoviária Federal (PRF).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

E, também, a instalação do Centro de Cooperação Policial Internacional da Amazônia, o CCPI – Amazônia (sede em Manaus), integrado com a Companhia de Operações Ambientais da Força Nacional de Segurança Pública, com sede em Manaus/AM.

Há, ainda, a previsão da implantação da Base da Coordenação de Aviação Operacional da Polícia Federal na Amazônia, da Força Integrada de Combate ao Crime Organizado no Amazonas, além da criação de duas delegacias descentralizadas da Polícia Federal nos municípios de Humaitá/AM e Tefé/AM.

No âmbito do AMAS ainda estão inseridos o Programa Estratégico de Segurança Pública da Amazônia (PESPAM) e os Planos Táticos Integrados (PTI) de Segurança Pública de cada estado integrante da Amazônia Legal brasileira. O PESPAM se destina ao estabelecimento dos princípios, missões, estratégias e ações de segurança pública a serem desenvolvidos pelas entidades que compõem a estrutura de governança do Plano AMAS.

As recentes ações e iniciativas visam a fortalecer a segurança na Amazônia, especialmente contra o crescente tráfico de drogas (cocaína e maconha, *creepy* ou *skunk*) pelas vias fluviais, utilizadas tanto para abastecer o mercado interno do Brasil quanto para alcançar os litorais e portos das regiões Norte e Nordeste do país, de onde são enviadas ao exterior. Essas medidas possibilitarão uma atuação mais eficaz no enfrentamento de ilícitos na região. Além disso, têm o potencial de ampliar o papel dos Núcleos de Polícia Marítima da Polícia Federal nos estados da Amazônia Legal. Em conjunto com os demais Órgãos de Segurança Pública estaduais e Forças Armadas, desempenharão papel crucial na segurança fluvial e lacustre, patrulhando portos e vias navegáveis, contribuindo significativamente para a melhoria da segurança na região.

Relações interagências em âmbito internacional

O combate ao tráfico de drogas transfronteiriço pelo Atlântico por meio de narcossubmarinos passa pelo contínuo esforço de cooperação entre agências nacionais e internacionais para – em conjunto – não só identificar, obstaculizar e neutralizar a ameaça aqui tratada, mas elucidar e prevenir crimes mediante oportuna, célere e eficiente cooperação jurídica, policial e de inteligência em âmbito internacional. Essa abordagem está alinhada com o que é preconizado pelo LBDN:

> [n]o âmbito do entorno regional, existe uma clara oportunidade de aprimoramento da cooperação no campo da defesa, por meio de instrumentos que promovam o desenvolvimento de um nível adequado de

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

> segurança regional na América do Sul, baseado na cooperação entre os países (Brasil 2020, 14-15).

O poder de cooperação internacional, embasado no princípio da troca de informações, fortalece tanto o desenvolvimento regional (na América do Sul) quanto extrarregional (nas Américas do Norte e Central, Europa e África), dentro de uma estrutura integrada de cooperação em inteligência estratégica. Essa estrutura conjunta, orientada pela cooperação entre serviços e sistemas de inteligência, contribui para a ampliação das capacidades dos países (Ribeiro 2006, 1). É relevante destacar o seguinte excerto do Capítulo 3 – Conceito Estratégico Marítimo Naval do PEM 2040:

> [a] ameaça ao tráfego marítimo e, por conseguinte, à estabilidade internacional pode provocar a formação de alianças estratégicas para sua proteção, cujas cargas, seguros, resseguros, tripulações e armadores foram, em grande medida, transnacionalizados. Tal forma de diplomacia naval converge com os interesses do Brasil, devendo ser adotada como uma oportunidade de projeção internacional pela presença naval, à luz do princípio jurídico da liberdade de navegação ou sob o amparo de organismos internacionais. Vale citar a participação brasileira com navios de guerra e no Comando da Força-Tarefa Marítima da Força Interina das Nações Unidas no Libano (FTM-UNIFIL) e em missões operativas combinadas no Golfo da Guiné com outros países, além da liderança em fóruns regionais, como a ZOPACAS, na busca por melhorar mecanismos de vigilância e defesa de suas linhas de comunicação marítimas no Atlântico Sul (Brasil 2014, 38).

Um dos exemplos de relação interagências em âmbito internacional é o *Maritime Analysis and Operations Centre (Narcotics)* – MAOC (N), com sede em Lisboa, Portugal. Foi criado em 2007 por iniciativa da Espanha, França, Holanda, Irlanda, Itália, Portugal e Reino Unido, para combater o tráfico transnacional de cocaína via Oceano Atlântico mediante uma cooperação internacional multilateral marítima e aérea.

Dentre as ações interagências exitosas no mar do Atlântico nos últimos anos empreendidas pelo MAOC (N), que resultaram em toneladas de cocaína apreendidas, destaque justamente para o caso do narcossubmarino "Che" (de 2019). Como salientado por Weerth (2022, 58),

> [t]alvez a apreensão mais marcante, que foi coordenada com sucesso com a participação e liderança do MAOC (N), tenha sido a apreensão do primeiro submarino transatlântico de drogas com cocaína da América do Sul, que atravessou o Atlântico e foi recolhido na costa espanhola, em novembro de 2019, com sua carga de 3,8 toneladas de cocaína (um primeiro caso comprovado).

Ainda sob esse contexto, é importante também o foco em uma contínua e sis-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

temática capacitação em procedimentos de análises prospectivas, bem como em ações de investigação conjunta (*joint investigation teams*), decorrente de sólida, efetiva e constante cooperação policial internacional, fundada em rede de compartilhamento de informações e inteligência (em níveis estratégico, tático e operacional). Com efeito, espera-se a promoção e o fortalecimento da interoperabilidade das forças de segurança governamentais – aperfeiçoando seus sistemas de comunicações, ações e capacitações –, com o propósito de mitigar formalidades e burocracias, derrubando barreiras no combate e enfrentamento à criminalidade transnacional.

Além do MAOC (N), outros exemplos significativos de cooperação internacional no combate ao crime organizado transnacional incluem:

- *Joint Interagency Task Force South* (JIATF *South*): força-tarefa interagências dos Estados Unidos dedicada ao combate ao tráfico de drogas e outras ameaças relacionadas na região da América Central e do Sul, por meio da coordenação de esforços entre diferentes agências governamentais.
- *European Union Agency for Criminal Justice Cooperation* (EUROJUST): agência da União Europeia responsável por fortalecer a cooperação judicial entre os Estados-Membros da UE no combate ao crime transnacional, facilitando a coordenação e troca de informações entre autoridades judiciais.
- *Seaport Cooperation Project* (SEACOP): implementado e financiado pela União Europeia (UE) como parte do Programa Global de Fluxos Ilícitos (*Global Illicit Flows Programme of the European Union*), a fim de combater o tráfico marítimo ilícito e redes criminosas associadas em países e regiões específicas da América Latina, Caribe e África Ocidental.
- d) Projeto I-CAN (*Interpol Cooperation Against ´Ndrangheta*): cooperação internacional da Interpol envolvendo Itália, Brasil e outros países, para enfrentamento às máfias italianas, em especial, a *´Ndrangheta*;
- Centros de Cooperação Policial Internacional da Polícia Federal (CCPIs): coordenados pela Polícia Federal do Brasil. Esses centros têm como objetivo agilizar o compartilhamento de informações e dados de inteligência entre polícias de diversos países. O primeiro centro foi implementado e está em pleno funcionamento desde 2018 na Superintendência da Polícia Federal no Rio de Janeiro. Em 2023, o Ministério da Justiça e Segurança Pública (MJSP), por meio da Portaria MJSP Nº 503, de 03/10/2023, definiu a competência da Diretoria da Amazônia e Meio Ambiente da PF (DAMAZ/PF) para planejar, instalar, dirigir, controlar e avaliar a atuação do Centro de Cooperação Policial Internacional da Amazônia, o CCPI - AMAZÔNIA, que buscará ampliar a cooperação policial e de inteligência entre os oito países integrantes da Amazônia Legal[4].

4 Nesse diapasão da cooperação internacional na região amazônica, convém destacar que a PF, desde 2003, conta com o Centro de Integração e Aperfeiçoamento em Meio Ambiente (CIAPA), localizado nas margens do rio Cuieiras, no município de Novo Airão/AM, onde agen-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

- Operação Guinex: operação conjunta no Golfo da Guiné com o objetivo de aumentar a segurança no Atlântico Sul, promovendo a interoperabilidade entre as Marinhas do Brasil e de Costa do Marfim, São Tomé e Príncipe, Camarões, Nigéria e Cabo Verde.
- 12º *Obangame Express*: maior exercício marítimo multinacional na África Ocidental e Central, realizado no início de 2023, no Golfo da Guiné e no Atlântico Sul.

Essas iniciativas representam esforços significativos na cooperação internacional para combater o crime organizado transnacional e promover a segurança em nível global.

Análise retrospectiva dos casos e possíveis tendências

Dada a crescente incidência de casos envolvendo narcossubmarinos nas últimas três décadas, principalmente na Colômbia (além de casos no Equador, Peru, Venezuela, Guiana, Suriname, países da América Central e do Norte, México e Estados Unidos), e considerando os sete casos conhecidos envolvendo o Brasil no período de 2010 a 2025, surgem algumas reflexões importantes para a Inteligência:

- A realidade envolvendo o Brasil seria exatamente essa limitada aos sete casos conhecidos?
- O Brasil possui conhecimento de dados não ostensivos sobre apreensões de narcossubmarinos por seus países vizinhos? Quantidades (narcossubmarinos, tipos/modelos e drogas), localidades (construção e apreensão), destino/rota, presos (números e nacionalidades), organizações criminosas envolvidas, e outros dados relevantes?
- A entrada de facções criminosas brasileiras em associação a organizações criminais internacionais na construção e lançamento de narcossubmarinos via Oceano Atlântico pode vir a ser uma tendência?
- Poderia ainda ser esse fenômeno acrescido de uma expansão para a faixa litorânea do Nordeste e Sudeste do Brasil, onde, além da menor distância até África e Europa, possam ser encontradas também vantagens operacionais e logísticas como as da foz do rio Amazonas?
- Considerando não apenas uma possível expansão geográfica de atuação, mas também a evolução e o emprego de novas tecnologias pelas organizações criminosas transnacionais na construção de narcossubmarinos (incluindo os totalmente submersíveis, elétricos e não tripulados operados remotamente), pode-se estar diante de um cenário disruptivo?

Cabe ressaltar que a instalação de estaleiros clandestinos para construção de

tes públicos são treinados para a defesa e preservação do meio ambiente e a repressão aos crimes ambientais, realizando cursos de piloto de embarcação, ambientação e sobrevivência na Amazônia, havendo, ainda, cooperação internacional educacional com forças públicas estrangeiras.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

narcossubmarinos requer uma série de condições, que incluem a escolha de regiões com baixa densidade populacional, de difícil acesso e com vegetação propícia ao acobertamento das ações criminosas, bem como aliciamento e cooptação de moradores locais. Além disso, a facilidade na aquisição de equipamentos náuticos e insumos para a construção das embarcações, juntamente com a presença de mão de obra qualificada, incluindo engenheiros e técnicos navais. Tais condições se tornam ainda mais favoráveis ao se considerar a histórica tradição do Brasil no contexto marítimo e de navegação.

Merece destaque o fato de que um único transporte bem-sucedido de narcossubmarino para a África ou a Europa apresenta potencial lucrativo bastante significativo, devido à sua capacidade de transportar grandes volumes de carga, normalmente entre duas e nove toneladas (UNODC 2010). Esse método, em apenas uma operação, pode superar consideravelmente várias outras formas de envio em termos de lucratividade, tais como: a contaminação de contêineres, *sea-chest* (caixa mares) ou cascos de navios por mergulhadores profissionais; a cooptação de tripulantes de navios (especialmente na modalidade conhecida como içamento); ou, até mesmo a depender do caso, o uso de veleiros, iates ou barcos pesqueiros, os quais frequentemente também resultam em apreensões volumosas (especialmente nos últimos anos). Exceto pelo uso de narcossubmarinos, todas as outras estratégias criminosas são dominadas por facções criminosas brasileiras.

A construção e o lançamento bem-sucedidos de narcossubmarinos representam um complexo esquema criminoso que amplifica significativamente a capacidade de retroalimentação global em diversos segmentos criminosos, incluindo o tráfico internacional de drogas, armas/munições e pessoas, bem como o terrorismo (narcoterrorismo), lavagem de dinheiro, biopirataria, contrabando, descaminho e outros crimes.

Ademais, outro fator a ser considerado que levaria a um potencial incremento do uso de narcossubmarinos pelo Oceano Atlântico é o aumento do comércio da cocaína da América Latina para a África (Delgado 2023), sendo o Brasil a principal zona de trânsito, armazenamento e consumo. Com efeito, conforme muito bem pontuado por Teles (2019),

> [e]ssa nova faceta de grande mercado consumidor se relaciona diretamente com preocupações de segurança do Brasil na medida em que afeta a dinâmica do tráfico internacional de drogas, particularmente no espaço setentrional da América do Sul e no Atlântico Sul. [...] É, portanto, notória a crescente importância do Brasil no fluxo de drogas ilícitas com destino à África.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Destarte, somente a possibilidade do uso de narcossubmarinos por organizações criminosas transnacionais atuantes em território brasileiro ou em outros países da América do Sul, Central e Norte, constitui-se em uma novel e significativa ameaça tanto à capacidade de patrulha e defesa da região, como ao espírito de paz e cooperação do Atlântico Sul, a denominada Zona de Paz e Cooperação do Atlântico Sul – ZOPACAS[5], representando importante desafio à estabilidade e à segurança no entorno estratégico brasileiro em suas projeções continentais e marítimas (Teles 2019).

Em entrevista ao InSight Crime, publicada em 21 de fevereiro de 2022, o jornalista espanhol Javier Romero, autor do livro *Operación Marea Negra*[6], respondendo a uma das perguntas na reportagem, destacou:

> [s]egundo a Marinha da Colômbia, pelo menos dois narcossubmarinos estão chegando à Europa pela Espanha e dois chegam à África a cada ano. A África está muito mais perto do Brasil do que da Europa. O aumento das safras nos países produtores inflou todas as rotas do narcotráfico no mundo, não apenas a transoceânica que tem como destino a Europa. Agora, toda a Costa Oeste Africana, desde o Golfo da Guiné até ao norte, atravessando todo o Magreb, é um grande armazém de cocaína a caminho da Europa (Saffon 2022).

Desafios e oportunidades

O tema em debate apresenta desafios não só para o Brasil, mas também para diversos países da América do Sul, Central e do Norte (México e EUA), além da Europa e da África, pois, como pontuado no início deste estudo, tais embarcações são praticamente invisíveis, indetectáveis em alto-mar. Nesse mesmo sentido, em reportagem publicada em abril de 2023, Antonio Martinez Duarte, Comissário-Chefe da Narco-Brigada da Polícia Nacional da Espanha, assim declarou:

> [h]á mais de 20 anos que os traficantes usam submarinos para chegar à África e à Europa, mas estes dois são os primeiros que apreendemos. Eles são muito difíceis de detectar (Beake 2023).

5 A ZOPACAS, estabelecida em 27 de outubro de 1986, é o principal foro para o tratamento de temas relativos à segurança do Atlântico Sul, consoante explicitado no LBDN, do qual ainda consta que, em termos geopolíticos, o Brasil prioriza o entorno estratégico, constituído pela América do Sul, Oceano Atlântico (Sul e parte do Atlântico Norte, onde encontra-se o estado do Amapá), costa ocidental da África e Antártida.

6 O livro intitulado *Operación Marea Negra* trata, em suma, da *Operación Baluma* deflagrada em 2019 na Espanha, que culminou na apreensão de carga superior a 3 toneladas de cocaína (152 fardos) retiradas de dentro do semissubmersível afundado (e, posteriormente, trazido à superfície), além de três presos (um espanhol, piloto da embarcação, e dois tripulantes equatorianos).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Na mesma reportagem, há ainda menção de se acreditar que, em pleno Oceano Atlântico, entre as Ilhas Canárias e os Açores, exista um cemitério de submarinos artesanais, afundados propositalmente após a carga ter sido descarregada com sucesso (Beake 2023):

> [e]m algum lugar entre as Ilhas Canárias e dos Açores, há um cemitério de submersíveis. Entre 15 e 20, que foram afundados por seus tripulantes uma vez realizada a entrega da cocaína a outra embarcação, asseguram os especialistas policiais (Zuloaga 2021).

Neste tópico, é relevante ressaltar a expertise dos narcotraficantes da Galícia, na Espanha, em trasladar cocaína de embarcações no mar dos Açores e Cabo Verde, no continente africano, para levar a carga até a terra por meio de pequenos barcos, veleiros ou barcos de pesca (UNODC 2023).

Assim, diante desse novo contexto apresentado, uma das primeiras oportunidades identificadas para lidar com esse risco (uso de narcossubmarinos no Atlântico) é estudá-lo e tratá-lo em nível estratégico, considerando-o como uma ameaça real e/ou potencial, tanto interna quanto externa, ao país. Pois, caso registre-se um novo evento envolvendo narcossubmarino no Atlântico envolvendo o Brasil, haverá impacto significativamente negativo na imagem do país e de suas instituições, tanto em âmbito nacional como internacional. Esse impacto é agravado pelo fato de o Brasil ser signatário de diversos acordos multilaterais e tratados internacionais relacionados à prevenção e repressão às drogas e ao crime organizado transnacional, com destaque para a Convenção de Palermo, assinada em 2000 no âmbito das Nações Unidas.

Dado que esse é um risco com alto potencial de impacto negativo, torna-se imperativo que a Inteligência estude as vulnerabilidades, oportunidades e desafios associados para neutralizá-lo ou mitigá-lo. Dentre uma série de desafios complexos, que exigem abordagem estratégica e integrada para serem enfrentados de maneira eficaz, estão:

1. Repressão e detecção: a dificuldade na repressão e detecção desses narcossubmarinos em alto-mar exige que o foco da fiscalização e busca seja direcionado às suas origens, ou seja, onde e como são construídos.
2. Controle de insumos e produtos: é necessário controlar insumos e produtos utilizados na construção de narcossubmarinos, como fibra de vidro e motores náuticos específicos.
3. Produção de conhecimento: deve-se produzir mais conhecimento acerca do tema, evitando dependência da produção de conhecimento extrarregional e reatividade a cada novo evento.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

4. Facções criminosas: avaliar a tendência de entrada de facções criminosas brasileiras, em parceria com narcocartéis colombianos e mexicanos, em esquemas que utilizam narcossubmarinos.
5. Vulnerabilidades de comunidades: tratar as vulnerabilidades enfrentadas por comunidades ribeirinhas e de pescadores ao longo do litoral brasileiro, que podem propiciar a instalação de pontos logísticos para o tráfico de drogas e armas.
6. Impacto nas pretensões transatlânticas: o crescimento de casos envolvendo narcossubmarinos pelo Atlântico pode impactar nas pretensões do Brasil de ser protagonista na região transatlântica e na ZOPACAS.
7. Ações intervencionistas: o aumento de casos de narcossubmarinos pode justificar ações ou políticas intervencionistas por parte de potências extrarregionais na América do Sul, além de pressão ambientalista e securitária internacional na Amazônia.

Apesar dos desafios, a situação também apresenta diversas oportunidades que podem ser exploradas para fortalecer a segurança e a soberania do Brasil. Entre as principais oportunidades estão as seguintes.

1. Potencialização de sistemas de segurança: potencializar o SisGAAz, o Centro Integrado de Segurança Marítima (CISMAR) e demais sistemas e programas da Marinha e de órgãos parceiros.
2. Integração de programas de fronteira: intensificar a integração e alcance do Programa de Proteção Integrada de Fronteiras (PPIF) e expandir os Gabinetes de Gestão Integrada de Fronteiras (GGFI).
3. Aperfeiçoamento do patrulhamento: aperfeiçoar, aprimorar e expandir o patrulhamento, policiamento, fiscalização e monitoramento das fronteiras e águas jurisdicionais brasileiras, aumentando a projeção internacional pela presença naval.
4. Criação de uma 2ª Esquadra: implementar uma 2ª Esquadra da Marinha do Brasil na região Norte/Nordeste.
5. Aquisição de equipamentos: adquirir mais aeronaves, navios, aeronaves remotamente pilotadas (ARPs) e veículos subaquáticos autônomos (AUVs) para busca, proteção, vigilância e monitoramento marítimo, aumentando o poder naval.
6. Potencialização de planos de segurança na Amazônia: potencializar o Plano Amazônia: Segurança e Soberania (Plano AMAS), o Programa Estratégico de Segurança Pública da Amazônia (PESPAM) e os Planos Táticos Integrados (PTI) de Segurança Pública dos estados da Amazônia Legal.
7. Fortalecimento da cooperação amazônica: fortalecer e efetivar a Declaração de Belém, consolidando a agenda comum entre os países signatários do Tratado de Cooperação Amazônica.
8. Exploração de petróleo na Foz da Bacia do Amazonas: a exploração de petróleo na Foz da Bacia do Amazonas pode trazer benefícios econômicos e de segurança, como geração de empregos, desenvolvimento econômico, aumento da receita fiscal, redução da dependência de importações, monitoramento e vigilância, infraestrutura de resposta a emergências e fortalecimento da segurança marítima.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Vale frisar que muitos dos desafios e oportunidades estão interligados, de modo que um mesmo tópico pode figurar tanto na lista de desafios quanto na de oportunidades, dependendo da perspectiva adotada na abordagem.

No futuro próximo, o uso dos modernos submarinos do Programa de Desenvolvimento de Submarinos (PROSUB), criado em 2008, será de grande utilidade no encalço de narcossubmarinos e outras ameaças no entorno estratégico brasileiro no Atlântico. Esse programa representa um grande avanço tecnológico e industrial naval brasileiro, fortalecendo a defesa e a soberania nacionais. Nesse mister, as marinhas norte-americana, no mar do Pacífico e do Caribe, e holandesa, no mar do Caribe, têm utilizado seus submarinos em operações antidrogas (Sutton 2020).

Em janeiro e março de 2024, a Marinha do Brasil lançou, respectivamente, os submarinos "Tonelero" (S-42) e "Humaitá" (S-41), segundo e terceiro dos quatro submarinos convencionais com propulsão diesel-elétrica previstos no PROSUB. O primeiro foi o "Riachuelo" (S-40) em setembro de 2022. O quarto submarino, o "Angostura" (S-43), está previsto para lançamento em 2025.

Esses novos submarinos contribuirão para aumentar o poder de dissuasão nos 5,7 milhões de km2 da Amazônia Azul. Soma-se, ainda, a construção futura do Submarino Convencionalmente Armado com Propulsão Nuclear (SCPN), batizado de "Álvaro Alberto" (SN-10), com previsão de entrega até 2033.

Conclusões e recomendações

Os narcossubmarinos no Oceano Atlântico representam uma ameaça contemporânea e emergente, devido à capacidade de transportar grandes cargas, evadir a fiscalização e integrar redes criminosas transnacionais, com possíveis impactos para o país. Este risco é agravado pela expansão da criminalidade organizada transnacional e pelo crescimento do modal narcomarítimo no Brasil e no mundo.

As evidências coletadas destacam a América do Sul, especialmente o Brasil, não só como um dos principais entrepostos de cocaína a caminho da Europa e da África por meio do transporte marítimo tradicional transatlântico, mas também, desde as apreensões dos narcossubmarinos em 2019 e 2023 na Espanha, e 2025 em Portugal, como palco de complexos esquemas criminosos transfronteiriços para construção e lançamento de narcossubmarinos capazes de transportar toneladas de cocaína.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Essa análise revela uma série de questões relevantes para a Inteligência, incluindo a escassez de trabalhos técnicos no Brasil sobre o tema e a falta de dados estatísticos específicos, especialmente no entorno estratégico brasileiro. Além disso, levanta-se a possibilidade da entrada de facções criminosas brasileiras nessa complexa cadeia de suprimentos para o envio, de uma só vez, de toneladas de cocaína a outros continentes via narcossubmarinos.

Portanto, é crucial que este tema seja compreendido, tratado e monitorado pela Inteligência, ao menos inicialmente, por meio de estudos comparativos de casos e estatísticas oficiais de outros países. Isso possibilitará abordagem e atuação mais eficazes e qualificadas no enfrentamento ao tráfico de drogas transnacional, principalmente no entorno estratégico transatlântico, onde o Brasil busca se tornar um ator regional relevante, exercendo papel de verdadeiro protagonista geopolítico.

Diante da natureza transnacional do tráfico de drogas por narcossubmarinos, a cooperação internacional se torna imperativa. É fundamental que o Brasil fortaleça suas parcerias com outros países (e organismos internacionais), especialmente aqueles localizados na América do Sul, Europa e África, para trocar informações de inteligência, compartilhar tecnologias de monitoramento marítimo e realizar operações conjuntas de combate ao crime organizado.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Referências

Abreu, Allan de. 2021. Cocaína - A Rota Caipira: o narcotráfico no principal corredor de drogas do Brasil. Record.

Beake, Nick. 2023. ''Cocaine-smuggling submarine reveals Europe's drug crisis,'' *BBC News*, 21 de abril de 2023. Acessado em 07 de maio de 2023. https://www.bbc.com/news/world-europe-65337215.

Brasil. 2016. *Política Nacional de Inteligência*. Gabinete de Segurança Institucional da Presidência da República. https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/politica-nacional-de-inteligencia.

Brasil. 2017. *Estratégia Nacional de Inteligência*. Gabinete de Segurança Institucional da Presidência da República. https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/ENINT.pdf.

Brasil. 2020. *Livro Branco de Defesa Nacional*. Ministério da Defesa. https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf.

Brasil. 2023a. *Plano Amazônia: Segurança e Soberania*. Ministério da Justiça e Segurança Pública. Decreto nº 11.614, de 21 de julho de 2023. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11614.htm.

Brasil. 2023b. *Plano de Ação na Segurança*. Ministério da Justiça e Segurança Pública. https://www.gov.br/mj/pt-br/assuntos/noticias/programa-de-acao-na-seguranca-pas-e-lancado-com-assinatura-dos-primeiros-atos-e-medidas-na-area-1.

Brasil. 2023c. *Programa Nacional de Enfrentamento às Organizações Criminosas*. Ministério da Justiça e Segurança Pública. https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/enfoc/Plano-de-Gerenciamento_Enfoc.pdf.

Brasil. 2024. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. Ministério da Defesa. Decreto Legislativo nº 61, de 23 de maio de 2024. https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf.

Delgado, Juan. 2023. ''Comércio de cocaína da América Latina para a África em ascensão,'' *Diálogo Américas*, 15 de fevereiro de 2023. Acessado em 27 de maio de 2023. https://dialogo-americas.com/pt-br/articles/comercio-de-cocaina-da-america-latina-para-a-africa-em-ascensao/.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Chaves, Daniel Santiago. 2010. "O Narcotráfico e seus Submarinos: um Novo Elemento na Logística do Crime na América do Sul," *Cadernos do Tempo Presente* 2. https://periodicos.ufs.br/tempo/article/view/2738.

CNN Portugal. 2025. "PJ e Marinha travam submarino com cerca de sete toneladas de cocaína a caminho dos Açores," 25 de março de 2025. Acessado em 25 de março de 2025. https://cnnportugal.iol.pt/submarinos/cocaina/pj-e-marinha-travam-submarino-com-sete-toneladas-de-cocaina-a-caminho-dos-acores/20250325/67e28b9ad34e3f0bae9c1570.

CMCON, Centro Internacional de Investigación y Análisis Contra Narcotráfico Marítimo. 2022. *Modalidades del Narcotráfico Marítimo 2022*. CMCON, nº 2. https://www.minjusticia.gov.co/programas-co/ODC/Documents/Publicaciones/Oferta/Trafico/Modalidades%20CMCON%202022.pdf.

Euronews. 2025. "PJ divulga imagens do submarino interceptado com quase sete toneladas de cocaína ao largo dos Açores." 25 de março de 2025. Acessado em 25 de março de 2025. https://pt.euronews.com/my-europe/2025/03/25/pj-interceta-submarino-carregado-de-cocaina-ao-largo-dos-acores.

G1. 2023. "Maior narcossubmarino da história da Colômbia é apreendido com 3 toneladas de cocaína," *G1*, 12 de maio de 2023. Acessado em 1º de maio de 2023. https://g1.globo.com/mundo/noticia/2023/05/12/maior-narcossubmarino-da-historia-da-colombia-e-apreendido-com-3-toneladas-de-cocaina.ghtml.

Gheller, Gilberto Fernando, Selma Lúcia de Moura Gonzales, e Laerte Peotta de Melo, orgs. 2015. *Amazônia e Atlântico Sul, Desafios e Perspectivas para a Defesa no Brasil*. Instituto de Pesquisa Econômica Aplicada - IPEA. https://repositorio.ipea.gov.br/handle/11058/4385.

Infopédia. s.d. "Narcossubmarino." Porto Editora. Acessado em 31 de março de 2025. https://www.infopedia.pt/dicionarios/lingua-portuguesa/narcossubmarino.

Jaramillo, Michelle Jacome. 2016. "The Revolutionary Armed Forces of Colombia (FARC) and the Development of Narco-Submarines." *Journal of Strategic Security* 9 (1): 49-69. https://doi.org/10.5038/1944-0472.9.1.1509.

Jozino, Josmar. 2025. "Submarino do Brasil transportava 6,6 toneladas de cocaína para Portugal," *UOL*, 25 de março de 2025. Acessado em 25 de março de 2025. https://noticias.uol.com.br/colunas/josmar-jozino/2025/03/25/submarino-do-brasil-transportava-66-toneladas-de-cocaina-para-portugal.htm.

Marinha do Brasil. 2020. *Plano Estratégico da Marinha* (PEM 2040). https://www.marinha.mil.br/publicacoes/pem2040.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Marinha do Brasil. s.d. "Amazônia Azul." Acessado em 25 de maio de 2023. https://www.marinha.mil.br/egn/spp_amazonia_azul.

O Globo. 2023a. "Narcossubmarino: embarcações são usadas para tráfico de drogas há 30 anos; veja evolução," *Jornal O Globo*, 1 de maio de 2023. Acessado em 1 de maio de 2023. https://oglobo.globo.com/mundo/epoca/noticia/2023/05/narcossubmarino-embarcacoes-sao-usadas-para-trafico-de-drogas-ha-30-anos-veja-evolucao.ghtml.

O Globo. 2023b. "Narcossubmarinos: Marinha da Colômbia capturou 19 embarcações do tipo apenas em 2023," *Jornal O Globo*, 7 de outubro de 2023. Acessado em 9 de outubro de 2023. https://oglobo.globo.com/mundo/epoca/noticia/2023/10/07/narcossubmarinos-marinha-da-colombia-capturou-19-embarcacoes-do-tipo-apenas-em-2023.ghtml.

O Globo. 2023c. "Narcossubmarino com 3,5 toneladas de cocaína é apreendido no México; vídeo," *Jornal O Globo*, 3 de junho de 2023. Acessado em 3 de junho de 2023. https://oglobo.globo.com/mundo/noticia/2023/06/narcosubmarino-com-35-toneladas-de-cocaina-e-apreendido-no-mexico-video.ghtml.

O Globo. 2024a. "Colômbia e Equador apreendem dois narcossubmarinos com quase 4 toneladas de cocaína," *Jornal O Globo*, 21 de janeiro de 2023. Acessado em 22 de janeiro de 2023. https://oglobo.globo.com/mundo/noticia/2024/01/21/colombia-e-equador-apreendem-dois-narcossubmarinos-com-quase-4-toneladas-de-cocaina.ghtml.

Ramirez, Byron. 2014. "Colombian Cartel Tactical Note #1: The Evolution of 'Narco-Submarines' Engineering," *Small Wars Journal*, 27 de fevereiro de 2014. Acessado em 6 de maio de 2023. https://archive.smallwarsjournal.com/jrnl/art/colombian-cartel-tactical-note-1.

Ribeiro, Fábio Pereira. 2006. "Cooperação Estratégica em Inteligência Formação da Defesa Regional: uma Contribuição dos Serviços de Inteligência," *Cadernos PROLAM/USP* 5 (8): 113-128. https://doi.org/10.11606/issn.1676-6288.prolam.2006.81802.

Romero, Javier. 2022. *Operación Marea Negra: La increíble historia del primer narcosubmarino que llegó a Europa con más de 3.000 kg de cocaína*. Penguin Random House.

Romero, Javier. 2025. "Un español, entre los cinco tripulantes detenidos a bordo de un narcosubmarino con 6.600 kilos de cocaína," *La Voz de Galicia*. 25 de março de 2025. Acessado em 25 de março de 2025. https://www.lavozdegalicia.es/noticia/galicia/2025/03/25/espanol-cinco-tripulantes-detenidos-bordo-narcosubmarino-7000-kilos-cocaina/00031742900843336119736.htm.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Soares, Rafael. 2023. ''Submarinos do tráfico: Brasil integra rota 'submersível' de drogas à Europa,'' *Jornal O Globo*, 1º de abril de 2023. Acessado em 1º de abril de 2023. https://oglobo.globo.com/mundo/noticia/2023/04/narcossubmarinos-brasil-integra-rota-submersivel-de-drogas-a-europa.ghtml.

Sutton, H.I. 2020. ''5 Ways The Military Hunts Narco Submarines You Don´t Hear About.''. *Forbes*, 4 de junho. Acessado em 6 de maio de 2023. https://www.forbes.com/sites/hisutton/2020/06/04/5-unseen-eyes--helping-the-navy-hunt-narco-submarines/.

Sutton, H.I. 2023. ''Latest Transatlantic Narco-Submarine in Europe Has Same Builder As Last One,'' *Covert Shores www.hisutton.com*, 13 de março de 2023. Acessado em 7 de maio de 2023. http://www.hisutton.com/Narco-Submarine-Spain-2023.html.

Sutton, H.I. 2025. ''Another Trans-Atlantic Narco Submarine Found in Europe,'' *Covert Shores www.hisutton.com*, 23 de janeiro de 2025. Acessado em 25 de março de 2025. http://www.hisutton.com/Transatlantic-Narco--Submarine-202501.html.

Teles, Matheus. 2019. ''Análises de Conjuntura: Inserção da África no mercado de drogas como consumidor e as implicações para o Brasil,'' GEPSI--UNB. http://gepsi.unb.br/index.php?option=com_content&view=article&layout=edit&id=35&Itemid=599.

UNODC, Escritório das Nações Unidas sobre Drogas e Crime. 2010. *The Globalization of Crime, a Transnational Organized Crime Threat Assessment*. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

UNODC, Escritório das Nações Unidas sobre Drogas e Crime. 2023. ''Cocaine trafficking diversifying through new hubs and groups, with global supply at record levels, says new report from the United Nations Office on Drugs and Crime,'' 16 de março de 2023. Acessado em 27 de maio de 2023. https://www.unodc.org/unodc/frontpage/2023/March/cocaine-trafficking-diversifying-through-new-hubs-nad-groups--with--global-supply-at-record-levels--says-new-report-from-the-united-nations-office-on-drugs-and-crime.html.

Weerth, Carsten. 2020a. ''Cocaine Smuggling by Help of Narco-Submarines from South America to Europe and Africa: A Proven Case – A Last Wake-Up Call for Customs Services Around the World,'' *Customs Scientific Journal* 1: 37-42. https://doi.org/10.32836/2308-6971/2020.1.5.

Weerth, Carsten. 2020b. ''Cocaine Smuggling by help of Narco-Submarines from South America to Africa and Europe: A Call for a higher awareness of an existing smuggling pathway,'' *Customs Scientific Journal* 2: 33-49. https://doi.org/10.32836/2308-6971/2020.2.5.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.255
ISSN 2595-4717

Weerth, Carsten. 2022. ''The Maritime Analysis and Operations Center (Narcotics) in Lisbon – a background paper on the foundation and successes of the EU´s prime law enforcement body for the prevention of transatlantic narcotic drug smuggling,'' *Customs Scientific Journal* 1: 55-59. https://doi.org/10.32782/2308-6971/2022.1.7.

Weerth, Carsten. 2025. ''Fourth proven case of a large Narco-Submarine crossing from the Americas to Africa/Europe and more LPV sightings: Raising awareness for a re-emerging smuggling route (West-Africa),'' ResearchGate. http://dx.doi.org/10.13140/RG.2.2.23480.05121.

Zuloaga, Jesús Maria. 2021. ''Oubiña confirma la existência de um 'cementerio' de narcosubmarinos en aguas canarias,'' *La Razón*, 19 de janeiro de 2021. Acessado em 30 de maio de 2023. https://www.larazon.es/espana/20210119/hfk2pg2opbgmvpv3nztpsmlhu4.html.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Artigo de pesquisa

Túlio Marcos Santos Cerávolo[1]
ORCiD 0009-0002-6347-7650

Cleber Modesto de Castro[2]
ORCiD 0009-0003-1192-4698

A APLICAÇÃO DAS TÉCNICAS DE ANÁLISE ESTRUTURADAS NO PROCESSO DE ANÁLISE DE INTELIGÊNCIA

https://doi.org/10.58960/rbi.2025.20.257

Cerávolo, Túlio Marcos Santos, e Cleber Modesto de Castro. 2025. "A aplicação das técnicas de análise estruturadas no processo de análise de inteligência". *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.257. https://doi.org/10.58960/rbi.2025.20.257.

Recebido em 30/10/2024
Aprovado em 17/12/2024
Publicado em 16/04/2025

1 Coronel de Infantaria do Exército Brasileiro, bacharel em Ciências Militares - Academia Militar das Agulhas Negras (AMAN), pós-graduado em Operações Militares – Escola de Aperfeiçoamento de Oficiais (EsAO), mestre em Ciências Militares - Escola de Comando e Estado Maior do Exército (ECEME), mestre em Segurança Nacional – *Colegio de Defensa Nacional* (México), possui os cursos Básico, Intermediário e Avançado de Inteligência da Escola de Inteligência Militar do Exército (EsIMEx) e o Curso Básico de Inteligência no Uruguai. Atualmente é o Comandante da EsIMEx.

2 Tenente-Coronel de Infantaria do Exército Brasileiro. Bacharel em Ciências Militares - Academia Militar das Agulhas Negras, bacharel em Educação Física – Escola de Educação Física do Exército, pós-graduado em Ciências Militares - Escola de Comando e Estado-Maior do Exército. Atualmente serve como Assessor de Inteligência Prospectiva do Centro de Inteligência do Exército (CIE). Possui o Curso Avançado de Inteligência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

A APLICAÇÃO DAS TÉCNICAS DE ANÁLISE ESTRUTURADAS NO PROCESSO DE ANÁLISE DE INTELIGÊNCIA

Resumo

Este artigo analisa o emprego das técnicas de análise estruturadas (TAE) na Inteligência. O estudo explora a Metodologia para a Produção do Conhecimento do Sistema de Inteligência do Exército Brasileiro e destaca categorias de TAE que melhor atendem demandas contemporâneas. Com base em um questionário aplicado a profissionais de inteligência, analisam-se as TAE consideradas mais adequadas para utilização em diferentes situações: trabalho em equipe com disponibilidade de tempo, trabalho individual com disponibilidade de tempo e trabalho individual com tempo exíguo. Conclui-se que a aplicação adequada das TAE mais relevantes pode melhorar a precisão analítica e a agilidade na tomada de decisões, contribuindo para a eficiência e eficácia da análise de Inteligência.

Palavras-chave: análise de inteligência, metodologia de produção do conhecimento, técnicas de análise estruturadas.

THE APPLICATION OF STRUCTURED ANALYTICAL TECHNIQUES IN THE PROCESS OF INTELLIGENCE ANALYSIS

Abstract

This article examines the use of structured analytical techniques (SATs) in Intelligence. The study explores the Knowledge Production Methodology of the Brazilian Army's Intelligence System and highlights categories of SATs that best meet contemporary demands. Based on a questionnaire administered to intelligence professionals, the SATs considered most suitable for use in different situations are analyzed: team work with time availability, individual work with time availability, and individual work with limited time. It is concluded that the appropriate application of the most relevant SATs can improve analytical accuracy and decision-making agility, contributing to the efficiency and effectiveness of Intelligence analysis.

Keywords*: intelligence analysis, knowledge production methodology, structured analytical techniques.*

LA APLICACIÓN DE LAS TÉCNICAS DE ANÁLISIS ESTRUCTURADAS EN EL PROCESO DE ANÁLISIS DE INTELIGENCIA

Resumen

Este artículo analiza el empleo de las técnicas de análisis estructuradas (TAE) en la Inteligencia. El estudio explora la Metodología para la Producción del Conocimiento del Sistema de Inteligencia del Ejército Brasileño y destaca categorías de TAE que mejor atienden las demandas contemporáneas. Con base en un cuestionario aplicado a profesionales de inteligencia, se analizan las TAE consideradas más adecuadas para su uso en diferentes situaciones: trabajo en equipo con disponibilidad de tiempo, trabajo individual con disponibilidad de tiempo y trabajo individual con tiempo limitado. Se concluye que la aplicación adecuada de las TAE más relevantes puede mejorar la precisión analítica y la agilidad en la toma de decisiones, contribuyendo a la eficiencia y eficacia del análisis de Inteligencia.

Palabras clave*: análisis de inteligencia, metodología de producción del conocimiento, técnicas de análisis estructuradas.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Introdução

A Era da Informação, entendida como a mudança social, política e econômica impulsionada pelos avanços tecnológicos na computação e nas telecomunicações (Teitelbaum 2004), tem como produto a própria informação. Essa Era se expande e se dissemina em um ritmo sem precedentes, oferecendo aos indivíduos uma quantidade e variedade crescente de dados. Segundo Artner et al. (2016), o analista de Inteligência na Era da Informação tem que estar preparado para lidar com os problemas perenes da área, como a complexidade dos cenários internacionais, informações incompletas e ambíguas, além das limitações inerentes à mente humana.

Para Liaropoulos (2006), essa revolução da informação impactou cada etapa do ciclo de Inteligência, acrescentando novas questões à agenda da Inteligência, alterando as questões antigas e trazendo mudanças organizacionais e culturais na arte da Inteligência. Além disso, alterou a relação entre a Inteligência e os decisores políticos, influenciando a forma como os clientes de Inteligência interagem com a informação.

A análise de Inteligência permaneceu por muito tempo nas sombras. As empresas e instituições não falavam sobre seus esforços de Inteligência e o tema não aparecia na mídia popular. Recentemente, essa situação passou por uma transformação significativa, principalmente devido à comercialização da Inteligência – que ampliou o acesso a dados fornecidos por empresas privadas, como imagens de satélites e drones – e devido à globalização da disciplina, que extrapolou suas origens nacionais e militares para adquirir crescente relevância nas áreas de segurança interna, aplicação da lei e nas organizações comerciais (Clark 2022). Essa transformação também impulsionou avanços metodológicos e ampliou o alcance e a eficácia da análise de Inteligência.

Apesar dessas transformações e avanços, a análise de Inteligência ainda enfrenta desafios significativos, e erros continuam a ocorrer. Estudos de Clark (2022), Heuer e Pherson (2021) e Coulthart (2017) destacam que os analistas tendem a aprender mais com os fracassos do que com os sucessos, como evidenciado pelas falhas significativas da Inteligência americana no século XXI: o ataque de 11 de setembro de 2001 e o erro de estimativa de 2002 sobre as armas de destruição em massa do Iraque.

As falhas de Inteligência sobre as armas de destruição em massa iraquianas também foram vistas por Artner et al. (2016) e Coulthart (2016). Eles observaram que a Agência Central de Inteligência (CIA) dos Estados Unidos da

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

América (EUA) promoveu vigorosamente formatos alternativos de análise estruturada nos anos seguintes a essas falhas. Isso incluiu, por exemplo, geração sistemática e revisão rigorosa de hipóteses alternativas. Outras organizações também promoveram mudanças na direção das técnicas de análise estruturada (TAE), como a Inteligência do Corpo de Fuzileiros Navais dos EUA, que desenvolveu um conjunto de 28 modelos, abordagens e técnicas estruturadas. Da mesma forma, o Escritório do Diretor de Inteligência Nacional (ODNI) promoveu o treinamento de analistas em pensamento crítico TAE. Especialistas de Inteligência americanos observaram que as TAE ganharam popularidade em parte porque abordavam especificamente armadilhas cognitivas que têm sido associadas a falhas recorrentes de Inteligência.

Ao analisar erros cometidos pela Inteligência americana, Clark (2022) identificou três tipos de fracasso cometidos por profissionais de Inteligência: falha no compartilhamento de informações, falha em analisar o material coletado de forma objetiva e falha do cliente em agir com base na Inteligência. Para evitar esses três fracassos, o autor propôs uma abordagem para a análise de inteligência centrada no alvo.

Nesse contexto, Clark (2022) explica que o sucesso desse processo depende, em parte, do uso eficaz de ferramentas analíticas, incluindo técnicas de análise estruturadas. Entretanto, algumas críticas são realizadas quanto ao uso dessas técnicas pela comunidade de Inteligência:

> [o] problema é que muitas TAE atrapalham o pensamento amplo e o tipo de análise que os formuladores de políticas querem. Ao mesmo tempo, a atenção obstinada à técnica corre o risco de reduzir as análises a processos mecânicos que exigem apenas o processamento dos dados "certos" para atender às necessidades dos formuladores de políticas (Haines e Leggett 2001 *apud* Clark 2022, tradução nossa).

Além disso, como observou um oficial sênior de Inteligência, "a confiança em técnicas analíticas estruturadas não produz necessariamente melhores resultados" e "a fé cega nas TAE não é mais redentora do que qualquer outra fé cega" (Gartin 2019).

Apesar das críticas, as TAE podem ter valor na análise se usadas no ponto certo do processo. O desafio é que os novatos podem se sentir sobrecarregados com o grande número de TAE disponíveis e com a incerteza sobre como e onde aplicá-las. Além disso, muitas dessas técnicas não são amplamente utilizadas por analistas de Inteligência, principalmente devido à sua complexidade e ao tempo necessário para implementá-las (Clark 2022).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

A Metodologia para a Produção do Conhecimento (MPC) utilizada pelo Sistema de Inteligência do Exército (SIEx), consolidada no Manual Técnico Produção do Conhecimento de Inteligência (EB70-MT-10.401), propõe a análise estruturada para permitir que o analista exponha seu pensamento e permita que seu trabalho possa ser revisto, discutido e criticado por partes ou passo a passo por outros profissionais (Brasil 2019).

Diante do cenário apresentado, formulamos a seguinte pergunta de pesquisa: Quais as categorias de TAE mais relevantes a serem aplicadas durante a Metodologia para a Produção do Conhecimento do SIEx para contribuir de maneira mais efetiva no processo de análise de Inteligência?

Visando a responder a essa pergunta, apresentamos a Metodologia para a Produção do Conhecimento do SIEx, expondo a "sequência ordenada de procedimentos executados pelo analista, com vista à produção de um conhecimento de Inteligência de forma racional e com melhores resultados" (Brasil 2019), com foco nos objetivos a serem atingidos e nos desafios a serem alcançados por ele em cada etapa do processo.

Na sequência, são examinadas as categorias de análise estruturada, baseadas nos conceitos mais recentes de classificação de técnicas bem como em conselhos para a escolha de uma técnica mais adequada, seguindo orientações de Heuer e Pherson (2015), no sentido de que as TAE são organizadas em grupos relacionados com base em algum fator comum a cada técnica. Essa primeira parte foi baseada em uma pesquisa bibliográfica, que consistiu na revisão e análise de obras e artigos científicos.

Diante desse quadro, foram aplicados questionários utilizando o Método Delphi. Um grupo de especialistas, possuidores do Curso Avançado de Inteligência da Escola de Inteligência Militar do Exército (EsIMEx), foi selecionado para responder a duas rodadas de perguntas, com o objetivo de atingir um consenso sobre o tema abordado. Os questionários foram estruturados de forma a permitir a coleta de dados quantitativos e qualitativos, com perguntas fechadas e abertas, visando a explorar as percepções, experiências e previsões dos especialistas. Na segunda rodada, os participantes receberam um resumo das respostas anteriores, permitindo-se a revisão de suas opiniões e a oportunidade de ajustar suas respostas com base nas contribuições do grupo. Com isso, foi possível refinar os resultados, gerando dados mais precisos e *insights* mais robustos e fundamentados para a análise final do estudo.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Discussão teórica

A Metodologia para a Produção do Conhecimento utilizada pelo SIEx consiste em uma sequência ordenada de procedimentos executados pelo analista para produzir conhecimento de Inteligência de forma racional e com melhores resultados (Brasil 2019). Clark (2022) propõe uma nova abordagem, centrada no alvo, que se diferencia do modelo tradicional linear e sequencial. Essa abordagem mais interativa e colaborativa envolve todas as partes interessadas, incluindo os analistas, as fontes de obtenção e os decisores, permitindo uma interação dinâmica e adaptativa.

O Departamento de Defesa dos EUA apresentou uma concepção de metodologia para a produção do conhecimento que destaca a interação de diferentes partes do ciclo de Inteligência, oferecendo um modelo útil para facilitar a compreensão. Esse modelo sugere que o processo não deve ser visto como uma sequência rígida, mas como um fluxo contínuo de interação entre os diversos elementos do ciclo de Inteligência: planejamento e direção, coleta, processamento e exploração, análise e produção e, por fim, difusão e integração. Todas essas etapas são realizadas de forma interativa em função da missão e são objeto de avaliação constante. Essa abordagem permite maior flexibilidade e adaptabilidade, características essenciais em um ambiente de Inteligência cada vez mais complexo e dinâmico (EUA 2017).

A MPC utilizada no SIEx compartilha com a abordagem de Robert Clark e o modelo do Departamento de Defesa (DoD) a concepção de que "as cinco fases do método não implicam procedimentos rigorosamente ordenados e não têm limites precisos. São fases que se interpenetram, inter-relacionam e interdependem" (Brasil 2019). No entanto, a MPC não incorpora as inovações apresentadas por Clark, como a interação dinâmica e adaptativa entre os diversos atores envolvidos no processo de Inteligência — analistas, fontes de obtenção e decisores. Essas interações, fulcrais à abordagem centrada no alvo de Clark, promovem um modelo colaborativo que permite maior flexibilidade e adaptabilidade, características fundamentais para atender aos desafios contemporâneos da atividade de Inteligência.

A primeira fase da MPC inicia com o planejamento, quando é essencial envolver todas as partes interessadas, incluindo os decisores, para criar uma imagem compartilhada do alvo ou problema. Clark (2022) sugere que essa abordagem colaborativa permite que todos contribuam com seus conhecimentos e extraiam os elementos necessários para suas tarefas. A aproximação dos analistas com as fontes de coleta e os decisores, os quais possuem

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

insights valiosos, é um desafio crucial para garantir que as ideias relevantes sejam incorporadas no produto analítico, aumentando a probabilidade de uso dos resultados da Inteligência.

O planejamento centrado no alvo considera o problema como um sistema, analisando sua estrutura, função e processo. A estrutura envolve os componentes e suas relações, a função refere-se aos resultados produzidos e o processo à sequência de eventos que produzem esses resultados (Clark 2022). Drell (1993) enfatiza a necessidade de uma análise minuciosa do problema, formulando um esboço preliminar dos aspectos a serem conhecidos. Clark (2022) reforça a necessidade de entender, definir, decompor e modelar (EDDM) o alvo. Já a MPC do SIEx (Brasil 2019) destaca a importância de determinar o período de tempo relevante para a análise. Ao final da fase do planejamento, o analista de Inteligência está em condições de compreender o alvo e a questão-problema identificando as lacunas de conhecimento a preencher, formulando suas Necessidades de Inteligência (NI).

Na fase de Reunião ou Gestão da Obtenção, o analista determina o valor dos dados reunidos, verificando sua pertinência e credibilidade, e integra esses dados em um conjunto coerente (Brasil 2019; Hendrickson 2018). O guia da Agência Central de Inteligência dos Estados Unidos (CIA 2009) enfatiza a importância da verificação contínua da qualidade das informações. A integração prioriza as NI em elementos essenciais de Inteligência com alto grau de credibilidade, ajustando os aspectos essenciais estabelecidos na fase de planejamento.

Após a gestão da obtenção, inicia-se a fase de análise. Neste momento emprega-se a Inteligência Descritiva, usada para entender sistemas complexos, comportamentos e tendências. O analista deve identificar atores e variáveis relevantes, refinando a modelagem do alvo, e apresentar o que está acontecendo ao decisor (Clark 2022). A análise de atores e variáveis oferece *insights* valiosos sobre as relações e possíveis ações futuras dos envolvidos. Hendrickson (2018) e Clark (2022) destacam a importância de formular hipóteses com base em conhecimentos prévios e evidências iniciais.

Após o decisor tomar conhecimento da situação atual, inicia-se a análise focada em compreender o que acontecerá a seguir, caso o cliente manifeste interesse. Nesse contexto, recorre-se à Inteligência Diagnóstica. De acordo com Clark (2022), essa abordagem oferece observações valiosas aos tomadores de decisão, permitindo que se preparem de maneira mais segura e eficaz para lidar com eventos futuros. Para isso, o analista realiza a

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

validação das hipóteses, define atores e variáveis relevantes e conduz uma avaliação detalhada de causa e efeito para responder por que os eventos estão ocorrendo (Hendrickson 2018).

Dessas observações, conclui-se que a MPC apresenta objetivos claros, porém coloca desafios significativos para o analista de Inteligência em cada uma de suas fases. A correta aplicação da metodologia requer planejamento colaborativo, integração eficaz dos dados obtidos e análise precisa de atores, variáveis e sistemas complexos, elementos indispensáveis para oferecer ao decisor tanto uma compreensão abrangente da situação atual quanto uma visão das possíveis ações futuras. Contudo, os desafios relacionados à incorporação das perspectivas de decisores e fontes de coleta, além da necessidade de refinar hipóteses e modelos, destacam a importância do domínio das TAE e de uma abordagem adaptativa. A próxima seção apresentará as categorias de TAE, com o objetivo de auxiliar a escolha da técnica mais apropriada para aprimorar a eficácia das análises de Inteligência.

As categorias de TAE

Historicamente, analistas de Inteligência baseavam suas opiniões exclusivamente em seu próprio conhecimento e experiência, usando um quadro de referência pessoal. Contudo, a explosão de informações disponíveis e as características modernas do combate tornaram esse método obsoleto e propenso a erros graves, como demonstrado pelos ataques de 11 de setembro de 2001 (Clark 2022).

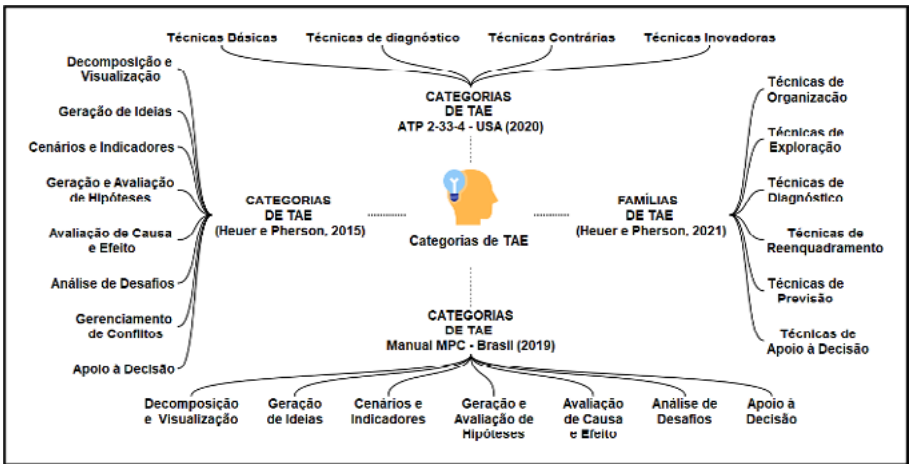
Heuer e Pherson (2021) destacam que, em uma era marcada pela complexidade crescente e pela abundância de dados, a capacidade de aplicar técnicas de análise estruturada é crucial para uma tomada de decisão eficaz. Essas técnicas ajudam a evitar armadilhas comuns, como o viés de confirmação, e são fundamentais tanto para o trabalho individual quanto para equipes de analistas.

A Figura 1 apresenta quatro classificações de técnicas analíticas estruturadas. Observa-se que o Manual Técnico Produção do Conhecimento de Inteligência EB70-MT-10.401 (Brasil 2019) adotou as mesmas sete categorias propostas por Heuer e Pherson (2015), exceto pela ausência da categoria "Gerenciamento de Conflitos". Além disso, as definições dessas categorias no Manual coincidem integralmente com aquelas apresentadas por Heuer e Pherson, refletindo a mesma abordagem conceitual e prática para a classificação das TAE.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Em 2020, o Exército Americano (EUA 2020) agrupou as técnicas em apenas quatro categorias. Em 2021, seis anos após a última edição de sua obra, Heuer e Pherson revisaram e reorganizaram as técnicas, adotando uma nova classificação.

Figura 1
Visão geral de classificações de TAE



Fonte: elaboração própria (2025).

A seguir serão descritas as categorias de TAE com suas respectivas técnicas segundo classificação do Manual EB70-MT-10.401 (Brasil 2019) e segundo Heuer e Pherson (2015).

Descrição das categorias de TAE

Heuer e Pherson (2015) categorizaram as TAE em oito grupos principais para fornecer uma estrutura organizada e sistemática que facilitasse seu uso por analistas de Inteligência. Cada categoria agrupa técnicas com objetivos ou abordagens semelhantes, tornando mais fácil escolher a técnica mais apropriada para um problema específico. Os autores recomendam que analistas iniciantes comecem com um número pequeno de técnicas fundamentais, pois essas técnicas são usadas com frequência e aplicadas a vários tipos de análise.

> a) Decomposição e Visualização: essa categoria decompõe problemas complexos em partes gerenciáveis e permite visualizar esses componentes para facilitar a compreensão e análise, apoiando a identificação de soluções eficazes e a tomada de decisões. Exemplos incluem Cronologia, Linha do Tempo e Mapas Mentais/Conceituais (Heuer e Pherson 2015).
>
> b) Geração de Ideias: fundamental para estimular a criatividade e explorar uma ampla gama de possibilidades. Reúne diversas perspectivas e

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

experiências para enriquecer o processo analítico. Técnicas como *Brainstorming*, *Starbursting* e Matriz de Impacto Cruzado são úteis no início de projetos ou quando métodos tradicionais enfrentam limitações diante da complexidade dos dados (Heuer e Pherson 2015).

c) Cenários e Indicadores: destinada a prever e monitorar mudanças em ambientes complexos e incertos, essa categoria é crucial para construir cenários futuros e desenvolver indicadores que sinalizem alterações significativas ou tendências emergentes. Exemplos incluem Análise de Cenários Simples e Geração, Validação e Avaliação de Indicadores (Heuer e Pherson 2015).

d) Geração e Avaliação de Hipóteses: foca no desenvolvimento e teste de hipóteses para entender melhor as situações analisadas e prever possíveis resultados. Técnicas como Geração de Múltiplas Hipóteses e Análise de Hipóteses Concorrentes ajudam a identificar a hipótese mais provável, refutando as menos sustentáveis com base nas evidências disponíveis (Heuer e Pherson 2015).

e) Avaliação da Causa e do Efeito: esta categoria examina relações causais em diferentes cenários, ajudando analistas a entenderem conexões entre variáveis e seus impactos resultantes. Técnicas como Pensamento de Fora para Dentro e Análise do Chapéu Vermelho identificam causas subjacentes e avaliam os efeitos de ações ou condições, proporcionando uma base sólida para ações futuras (Heuer e Pherson 2015).

f) Análise de Desafios: foca em testar e desafiar o entendimento e as suposições em análises para garantir sua robustez, especialmente em contextos de incerteza elevada ou informações contraditórias. Técnicas como Advogado do Diabo e Análise Pré-Mortem promovem pensamento crítico e preparam melhor os analistas para lidar com o inesperado e mitigar riscos significativos (Heuer e Pherson 2015).

g) Apoio à Decisão: fornece técnicas que auxiliam os tomadores de decisão a escolherem entre diferentes alternativas com base em uma análise rigorosa e dados sólidos. Exemplos incluem Matriz de Decisão e Matriz SWOT, que estruturam o processo de tomada de decisão e garantem que todas as opções sejam avaliadas e os riscos compreendidos (Heuer e Pherson 2015).

h) Gerenciamento de Conflitos: projetada para resolver desacordos dentro de equipes de análise ou entre partes interessadas, garantindo que os conflitos não prejudiquem o processo analítico ou os resultados. Técnicas como Colaboração Confrontada e Debate Estruturado facilitam a comunicação eficaz e a resolução de conflitos, promovendo um ambiente colaborativo (Heuer e Pherson 2015).

O Manual EB70-MT-10.401 apresenta sete categorias de TAE, excluindo a categoria de Gerenciamento de Conflitos mencionada por Heuer e Pherson (2015).

As categorias de TAE DE 2020 do Exército Americano

O Exército Americano, em 2020 (EUA 2020), categorizou as técnicas em três seções principais: básicas, diagnósticas e avançadas, sendo que as avançadas são subdivididas em contrárias (*contrarian*) e inovadoras (*imaginative*).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

As TAE básicas fornecem *insights* para a resolução de problemas, incluindo Ordenação, Cronologias, Análise de Rede e Mapeamento de Eventos. Elas são geralmente usadas no início do esforço de Inteligência para obter um diagnóstico inicial do problema, revelando padrões (EUA 2020).

As técnicas de diagnóstico focam em tornar argumentos analíticos, suposições e lacunas de Inteligência mais transparentes, analisar a qualidade da informação e identificar indicadores de mudança. Essas técnicas são frequentemente usadas junto com outras para fortalecer avaliações e conclusões analíticas, como Verificação dos Pressupostos-Chave (EUA 2020).

As técnicas avançadas são divididas em técnicas contrárias (*contrarian*) e técnicas inovadoras (*imaginative*). As contrárias desafiam suposições vigentes e ampliam resultados possíveis, examinando preconceitos e suposições quanto à relevância e consequência. Exemplos incluem Análise de Hipóteses Concorrentes, Advogado do Diabo, Time A e Time B, Análise de Alto Impacto/Baixa Probabilidade e Análise "E se?" (EUA 2020).

As técnicas avançadas inovadoras ajudam os analistas a abordar problemas de múltiplas perspectivas, facilitando a previsão de eventos e a geração criativa de ideias. Exemplos incluem *Brainstorming*, Pensamento de "fora para dentro" e Técnica de Análise do Time Vermelho, auxiliando na identificação de diferentes perspectivas e suposições entre membros da equipe de análise (EUA 2020).

As categorias de TAE na edição de 2021 de Heuer e Pherson

Na 3ª edição do livro *Structured analytic techniques for intelligence analysis*, de 2021, Heuer e Pherson reorganizaram as oito categorias originais em seis famílias de técnicas para simplificar e tornar seu uso mais prático. Essas famílias incluem:

> a) Técnicas de Organização: estruturam e organizam informações de maneira clara e lógica, ajudando a desenvolver listas de eventos críticos, fatores-chave e variáveis importantes. Exemplos incluem Ordenação, Classificação, Pontuação e Priorização, Mapas de Processos e Gráficos de Gantt, que facilitam a visualização de cronogramas e fluxos de trabalho (Heuer e Pherson 2021).
>
> b) Técnicas de Exploração: ajudam os analistas a expandirem o entendimento e gerarem novas ideias e abordagens. Incluem métodos como *Brainstorming*, *Starbursting*, Mapas Mentais e Conceituais, Técnica de Grupo Nominal e Análise de Rede (Heuer e Pherson 2021).
>
> c) Técnicas de Diagnóstico: identificam e avaliam as causas subjacentes ou variáveis que influenciam um problema. Exemplos incluem Verificação

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

> das Premissas-Chave, Cronologia e Linha do Tempo e Matriz de Impacto Cruzado. Essa categoria também abrange técnicas para gerar e testar hipóteses, como Geração de Hipóteses Simples e Múltiplas, e Matriz de Hipóteses Concorrentes (Heuer e Pherson 2021).
>
> d) Técnicas de Reenquadramento: ajudam os analistas a ver o problema sob diferentes perspectivas e questionar abordagens existentes. Mitigam limitações cognitivas comuns e aumentam as chances de acerto na análise. Divididas em técnicas de Causa e Efeito, Análise de Desafios e Gerenciamento de Conflitos (Heuer e Pherson 2021).
>
> e) Técnicas de Prospecção: utilizadas para antecipar futuros desenvolvimentos e cenários potenciais, ajudando os decisores a estruturar problemas e antecipar o imprevisto. Incluem cenários simples, geração de múltiplos cenários e raciocínio contrafactual, ajudando a alertar sobre perigos futuros e revelar oportunidades (Heuer e Pherson 2021).
>
> f) Técnicas de Apoio à Decisão: auxiliam na tomada de decisões, para avaliar opções e determinar a melhor linha de ação. Apresentam todas as opções e inter-relações de forma gráfica, ajudando os analistas a testar resultados de opções alternativas. Incluem Análise SWOT, Matriz de Decisão e Análise Bowtie (Heuer e Pherson 2021).

Cada família de técnicas tem um papel único no processo de análise, permitindo que os analistas abordem desafios de maneira abrangente e metódica, garantindo uma análise rigorosa e minimizando vieses, resultando em ações mais informadas e confiáveis (Heuer e Pherson 2021).

Os analistas frequentemente manifestam incertezas quanto à seleção da técnica mais adequada a ser empregada. Para isso, Heuer e Pherson (2021) propuseram um guia para selecionar as TAE mais adequadas, que inclui uma lista de doze tarefas possíveis que os especialistas realizam durante uma análise. O guia combina a tarefa com várias técnicas analíticas, proporcionando velocidade na escolha e utilização apropriada. As doze tarefas são:

> 1. Iniciar um projeto, obter dados, expandir o pensamento: técnicas como Verificação dos Pressupostos-Chave, *Brainstorming*, *Starbursting* e Pensamento de Fora para Dentro.
>
> 2. Buscar o sentido dos dados, procurar por conexões, por agrupamentos, procurar os limites entre os dados e procurar por lacunas: técnicas como Cronologias e Linha do Tempo, *Brainstorming* Estruturado, Mapas Conceituais e Análise de Venn.
>
> 3. Explorar as ideias, procurar por relações, comparações e causalidade: técnicas como Mapas Mentais, Análise de Venn e Mapas Conceituais.
>
> 4. Explicar eventos, providenciar respostas, identificar hipóteses prováveis e oferecer alternativas: técnicas como Geração de Múltiplas Hipóteses, Análise de Hipóteses Concorrentes e Localizador de Inconsistências.
>
> 5. Avaliar a possibilidade de engano: técnicas como Análise de Detecção de Engano, Análise de Hipóteses Concorrentes, Geração de Hipótese Múltiplas e Análise do Time Vermelho.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

6. Questionar noções preconcebidas, estabelecidas e mentalidades fixas (mindset): técnicas como Verificação dos Pressupostos-Chave, Análise Pré-Mortem e Autocrítica Estruturada.

7. Reformular seus problemas e considerar um ponto de vista diferente: técnicas como Pensamento de Fora para Dentro, Análise do Chapéu Vermelho e Análise "E se?".

8. Visualizar os eventos sob a perspectiva de um adversário: técnicas como Análise do Time Vermelho, Geração de Hipóteses Múltiplas e Análise SWOT.

9. Identificar os fatores-chave dos eventos, realizar uma análise prospectiva e rastrear trajetórias futuras: técnicas como Geração de Fatores-Chave, Identificador de Incertezas-Chave, Geração de Cenários Múltiplos e Indicadores.

10. Evitar surpresa, fornecer aviso antecipado de eventos que possam afetar interesses críticos: técnicas como Indicadores, Detecção de Negação, Análise "E se?" e Análise de Alto Impacto/Baixa Probabilidade.

11. Apoiar um decisor na formulação de conclusões e escolher linhas de ação: técnicas como Matriz de Decisão, Análise SWOT, Vantagens, Inconvenientes, Vulnerabilidade e Soluções, Matriz de Impacto e Análise de Campo de Força.

12. Apresentar os dados em formato visual: técnicas como Linhas do Tempo, Análise de Venn, Mapas Mentais, Indicadores, Vantagens, Inconvenientes, Vulnerabilidade e Soluções e Análise de Campo de Força.

Conclui-se parcialmente que o analista de Inteligência se beneficia de um vasto leque de técnicas de análise estruturada, permitindo a escolha da ferramenta mais adequada para cada situação. O domínio aprofundado dessas categorias e a compreensão das tarefas e desafios específicos da MPC facilitam a busca pela técnica ideal, otimizando o desempenho e a qualidade do trabalho.

Metodologia: a convergência das categorias de TAE com a MPC

Para validar a aplicabilidade das TAE nas diferentes fases da MPC, comparou-se a opinião de analistas de Inteligência do SIEx com as características das TAE e com os desafios da MPC. Dessa forma, tornou-se possível obter um conjunto de TAE consideradas mais adequadas ao dia a dia e às demandas dos analistas. Com o objetivo de promover a transparência e facilitar a replicação do questionário, esta seção oferece um resumo das etapas metodológicas seguidas.

Foram aplicados dois questionários a analistas utilizando o método Delphi, uma TAE de Análise de Desafio. O primeiro formulário foi enviado a um grupo de quarenta analistas com formação no Curso Avançado de Inteligência da EsIMEx, os quais responderam individualmente, sem qualquer viés de influ-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

ência ou pressão de grupo. Após a coleta das respostas, os dados foram consolidados por meio de processos de ordenação, classificação e priorização das soluções propostas. Conforme prescrito pela metodologia, uma segunda rodada de questionamentos foi encaminhada aos mesmos analistas, com perguntas mais focadas, estimulando a reflexão e facilitando a convergência de opiniões. Nesta segunda etapa, trinta e sete analistas participaram, contribuindo para o refinamento das conclusões.

Três situações distintas foram apresentadas aos especialistas. Na primeira, o analista foi colocado em um cenário de trabalho em equipe com tempo disponível (Quadro 1).

Quadro 1
Modelo do questionário 1ª situação – questões fechadas

Fase	Objetivo	Desafio	Opções
1ª fase Planejamento	Compreender o alvo/ problema	1. Modelagem do alvo 2. Interação com o decisor 3. Linha do tempo 4. Levantamento das NI	Múltipla escolha
2ª fase Gestão da Obtenção ou Reunião	Confeccionar documentos de requisitos de inteligência	1. Priorização das NI	Múltipla escolha
3ª fase Análise e Síntese (Inteligência Descritiva)	Apresentar ao decisor o que está acontecendo	1. Levantar os atores 2. Levantar as variáveis 3. levantar as hipóteses	Múltipla escolha
4ª fase Análise e Síntese (Inteligência Diagnóstica)	Apresentar ao decisor o "porquê" de algo estar acontecendo	1. Validar as hipóteses 2. Definir atores e variáveis relevantes 3. Avaliação de causa e efeito	Múltipla escolha

Fonte: elaboração própria (2025).

Na segunda situação (Quadro 2), o especialista desempenharia a tarefa de forma individual, mantendo disponibilidade de tempo. Foi apresentada uma situação hipotética e solicitado ao especialista que indicasse quais TAE utilizaria para solucionar a questão-problema proposta.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Quadro 2
Modelo do questionário 2ª situação – questão aberta

Situação	Prazo disponível	Questão-problema	TAE utilizada
Analista trabalhando de forma individual	Prazo suficiente	Situação hipotética	Solução livre

Fonte: elaboração própria (2025).

Na terceira situação (Quadro 3), solicitou-se ao analista que considerasse um cenário no qual a análise deveria ser realizada sob restrição de tempo, com prazos exíguos.

Quadro 3
Modelo do questionário 3ª situação – questão aberta

Situação	Prazo disponível	Questão-problema	TAE utilizada
Analista trabalhando de forma individual	O mais rápido possível	Situação hipotética	Solução livre

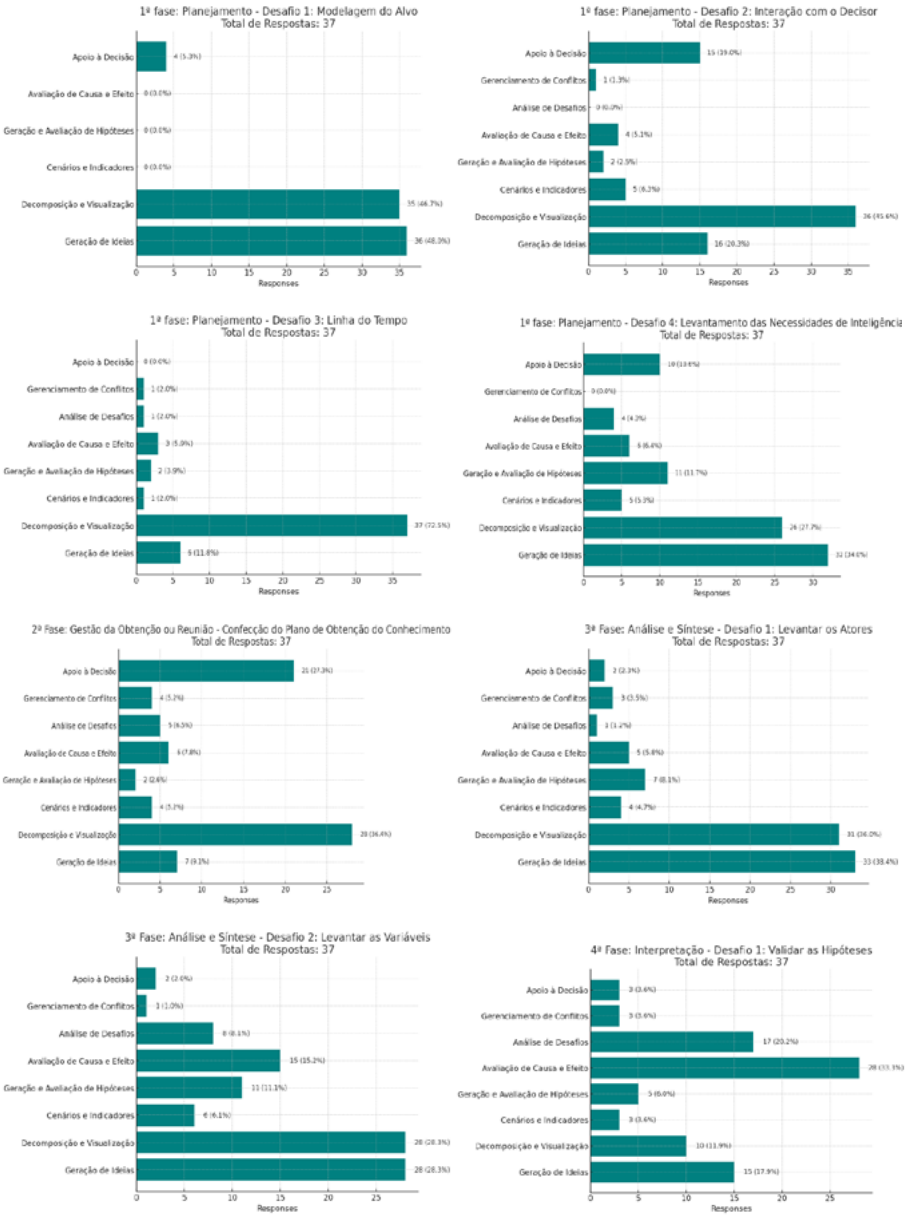
Fonte: elaboração própria (2025).

Resultados

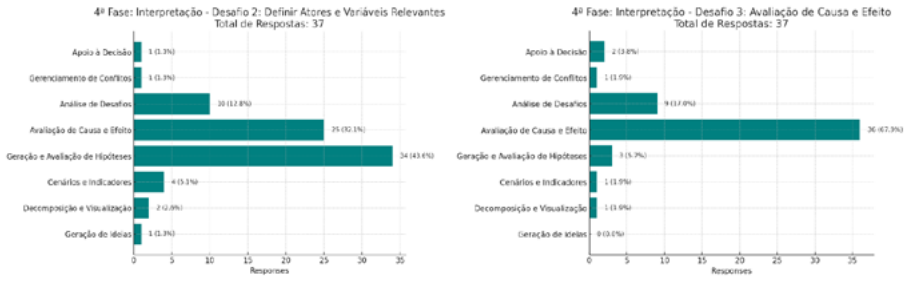
Dessa forma, ao final da primeira rodada de questionamentos, as respostas dos especialistas foram ordenadas, classificadas e analisadas conforme os princípios do método Delphi, que visa obter um consenso progressivo a partir da interação entre os participantes em múltiplas etapas. Na segunda rodada, os especialistas tiveram a oportunidade de revisar e reavaliar suas opiniões, com base no *feedback* consolidado da primeira fase, contribuindo para o refinamento das propostas e a convergência de suas respostas. Considerando-se as respostas dos analistas a respeito da primeira situação (solução em grupo com tempo disponível), e após o refinamento obtido na segunda rodada de questionários, obtiveram-se os conjuntos de técnicas considerados mais adequados pelos analistas para enfrentar cada um dos desafios compreendidos nas diferentes fases da análise de inteligência. Os resultados são apresentados no Gráfico 1.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Gráfico 1
Resultados para a Situação 1 (Solução em grupo com tempo disponível), após a segunda rodada



Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717



Fonte: elaboração própria (2025).

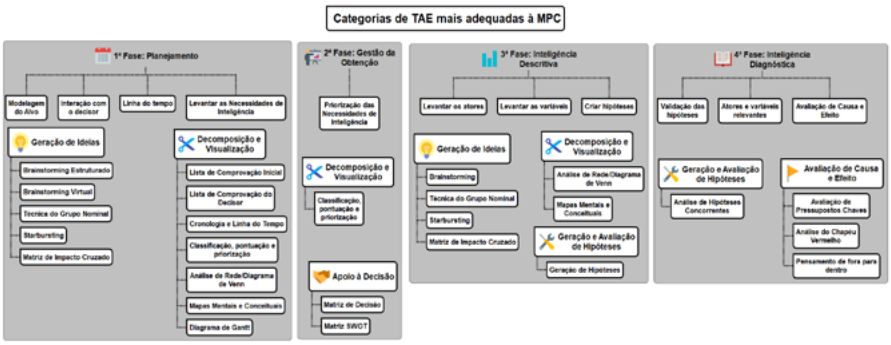
Com base na pesquisa e nas contribuições dos especialistas, foram apontadas as categorias de técnicas analíticas estruturadas mais indicadas para apoiar a análise de Inteligência em cada uma das etapas da Metodologia de Produção de Conhecimento. A utilização apropriada dessas técnicas destacadas tem o potencial de aumentar de forma expressiva a exatidão das análises realizadas e de acelerar o processo decisório, fortalecendo tanto a qualidade quanto a efetividade das operações de análise de Inteligência.

O trabalho em grupo, considerado na primeira situação apresentada no questionário, é essencial para a abordagem de problemas complexos na análise de Inteligência, pois permite a combinação de diferentes habilidades, conhecimentos e perspectivas. Quando direcionado pelo uso das TAE mais relevantes, esse esforço coletivo se torna ainda mais eficaz, garantindo que as energias do grupo sejam canalizadas de forma produtiva. A seleção adequada das TAE não apenas organiza o raciocínio e promove maior clareza no processo, mas também potencializa a colaboração, criando sinergia entre as capacidades dos integrantes e as ferramentas analíticas utilizadas. Essa integração é decisiva para alcançar o objetivo proposto, assegurando que o trabalho em grupo, aliado às técnicas apropriadas, resulte em análises precisas e soluções bem fundamentadas.

Nesse contexto, a Figura 2, abaixo, apresenta uma proposta de categorias e técnicas mais adequadas para cada fase da MPC a partir dos resultados obtidos no questionário (resumidos no Gráfico 1). Essas categorias e técnicas foram identificadas por um grupo de especialistas em Inteligência para serem aplicadas por analistas que disponham de tempo suficiente para o processamento.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Figura 2
Categorias de TAE mais adequadas a cada fase da MPC



Fonte: elaboração própria (2025).

Na segunda situação incluída no questionário, solicitou-se aos especialistas que indicassem as TAE mais adequadas para a solução de uma situação hipotética, considerando que, nesse cenário, o analista realizaria o trabalho de forma individual e ainda contaria com tempo disponível para o desenvolvimento do processo.

Mesmo contando com tempo disponível, o analista que trabalha individualmente enfrenta o desafio de selecionar criteriosamente as TAE mais adequadas. Essa escolha cuidadosa é fundamental para garantir que o processo atenda aos objetivos propostos, permitindo uma abordagem sistemática e eficiente que maximize a precisão dos resultados e a relevância das conclusões obtidas.

O Quadro 4 apresenta as TAE consideradas mais adequadas pelos analistas nessa situação, a partir das respostas do questionário.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

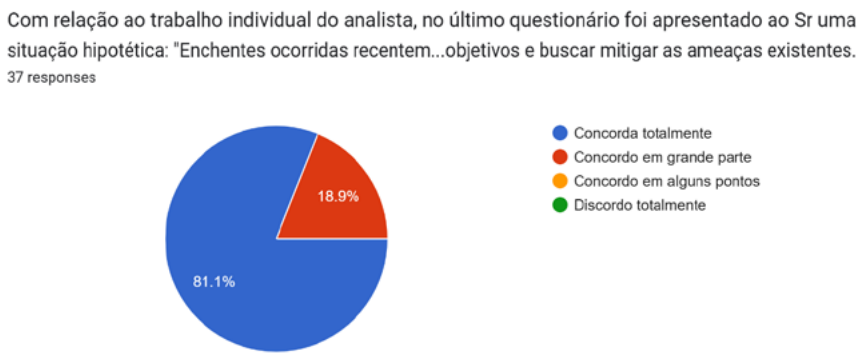
Quadro 4
TAE consideradas mais adequadas para a situação 2 (trabalho individual com tempo disponível)

TAE	Finalidade
Brainstorming Estruturado	Gerar o máximo de ideias
Starbursting	Entender, decompor e modelar a questão-problema
Cronologia e Linha do Tempo	Encadeaar os fatos, contextualizar o problema e suas origens
Mapa Mental	Organizar as ideias levantadas
Matriz de Impacto Cruzado	Identificar a motricidade e dependência de atores e variáveis e priorizar os mais relevantes
Geração de Hipóteses	Entender melhor as situações analisadas e prever possíveis impactos
Análise de Cenários	Identificar os possíveis cenários que podem impactar a situação-problema
Matriz SWOT	Levantar quais ações ou tarefas terão maior impacto para alcançar os objetivos e buscar mitigar as ameaças existentes

Fonte: elaboração própria (2025).

Na segunda rodada, os analistas manifestaram alto nível de concordância com o resultado consolidado da primeira rodada (Quadro 4), o que pode ser verificado no Gráfico 2.

Gráfico 2
Concordância com o resultado consolidado da primeira rodada para a situação 2 (trabalho individual com tempo disponível), após a segunda rodada



Fonte: elaboração própria (2025).

Na terceira e última situação do questionário, foi apresentada a mesma si-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

tuação hipotética. Entretanto, dessa vez, foi colocada a premissa de tempo como fator primordial para o cumprimento da missão. Segundo Clark (2022), o tempo é um problema comum enfrentado pelos analistas, que precisam equilibrar a precisão e a profundidade de suas análises com as restrições de tempo impostas pela necessidade de fornecer informações eficientes rapidamente. O mesmo é pontuado no manual de análise de Inteligência do Exército dos Estados Unidos da América (EUA 2020): as restrições no tempo são impostas frequentemente pelos prazos de planejamento operacional e execução, exigindo que os analistas produzam Inteligência com limitação de profundidade e completude. Assim, Heuer e Pherson (2021) ressaltam a necessidade de métodos que possam ser executados eficientemente dentro das limitações de tempo típicas da profissão de analista de Inteligência.

Dessa forma, as TAE mais recomendadas para a solução do problema hipotético em tempo exíguo constam no Quadro 5.

Quadro 5
TAE consideradas mais adequadas para a situação 3 (trabalho individual com tempo exíguo)

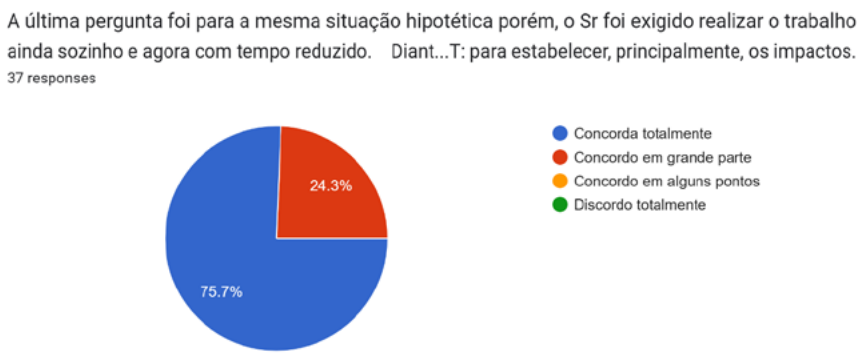
TAE	Finalidade
Brainstorming/Starbursting	buscar perceber diretamente de forma rápida os principais impactos.
Cronologia e Linha do Tempo	para permitir melhor visualização do problema, inclusive por parte da autoridade.
Mapa Mental	organizar as ideias e podendo utilizar no briefing para a autoridade.
Matriz SWOT	identificar e analisar os fatores internos e externos, desafios e oportunidades e formular estratégias eficazes para a questão/problema.

Fonte: elaboração própria (2025).

Assim como na situação anterior, para a situação 3 os analistas também manifestaram alto nível de concordância com o resultado consolidado da primeira rodada (Quadro 5), o que pode ser verificado no Gráfico 3.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Gráfico 3
Concordância com o resultado consolidado da primeira rodada para a situação 3 (trabalho individual com tempo exíguo), após a segunda rodada



Fonte: elaboração própria (2025).

Os resultados apresentados demonstram que as TAE desempenham um papel importante na organização, visualização e solução de problemas complexos na atividade de Inteligência sob restrições de tempo e recursos. A seleção dessas técnicas pelos analistas reflete a necessidade de ferramentas versáteis que os auxiliem tanto na estruturação do raciocínio quanto na comunicação eficaz com tomadores de decisão. Analisando individualmente cada técnica escolhida, revela-se que essas TAE não apenas melhoram a clareza e a precisão das análises, mas também podem ter papel decisivo no engajamento com autoridades favorecendo a qualidade das decisões em cenários de Inteligência.

Considerações finais

O raciocínio para analistas de Inteligência na Era da Informação enfrenta três desafios principais: erros internos; erros externos; e problemas de insuficiência, irrelevância, indeterminação e insignificância (Hendrickson 2018). Um bom analista deve adotar novos métodos, técnicas e pensamento crítico. É essencial identificar o que se precisa saber e buscar esse conhecimento, além de entender os obstáculos cognitivos ao pensamento crítico e saber como reduzi-los (Smith 2017).

Neste trabalho, um diferencial significativo foi o acesso direto a profissionais de Inteligência, o que permitiu realizar análise empírica e incorporar suas perspectivas e experiências práticas à análise. Essa interação possibilitou a coleta de *insights* valiosos sobre a aplicação de técnicas de análise estruturadas no dia a dia da atividade de Inteligência, especialmente em contextos

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

marcados por restrições de tempo e incertezas.

Heuer e Pherson (2021) destacam, por exemplo, a eficácia de utilizar duas técnicas distintas para conduzir a mesma análise, prática que, conforme relatado por alguns profissionais entrevistados, pode reduzir significativamente erros e aumentar a confiança nos resultados obtidos. Ao mesmo tempo, Hendrickson (2018) reforça a importância de desenvolver métodos e estratégias que conciliem precisão e agilidade, um desafio constante em um ambiente onde o "relógio implacável" molda decisões.

As TAE desempenham um papel essencial na análise de Inteligência, especialmente em cenários onde um grupo de analistas dispõe de tempo adequado para a entrega do produto final. Após a análise dos resultados obtidos da pesquisa, concluiu-se que as categorias de TAE mais adequadas para esse contexto foram: Geração de Ideias, Decomposição e Visualização, Apoio à Decisão, Geração e Avaliação de Hipóteses e Avaliação de Causa e Efeito. A aplicação criteriosa dessas técnicas contribui para o aprimoramento dos processos analíticos, promovendo uma maior eficiência no uso dos recursos disponíveis e uma maior eficácia na entrega de produtos de Inteligência mais precisos e bem fundamentados.

Comparando os resultados das duas primeiras situações, constatou-se que as técnicas mais adequadas para o trabalho individual com tempo disponível pertencem às mesmas categorias de TAE selecionadas para o contexto de trabalho em grupo. Observou-se que as técnicas *Brainstorming* Estruturado, *Starbursting*, Cronologia e Linha do Tempo, Mapa Mental, Matriz de Impacto Cruzado, Geração de Hipóteses, Análise de Cenários e Matriz SWOT se destacam como as mais apropriadas para o analista atuar de forma individual quando dispõe de tempo suficiente para desenvolver seu trabalho.

Com a redução do tempo disponível para o analista realizar seu trabalho, a escolha das TAE mais adequadas foi diretamente impactada, exigindo soluções mais rápidas e direcionadas. Conforme indicado pelos especialistas e apresentado no Quadro 5, as técnicas recomendadas refletem a necessidade de otimização do tempo sem comprometer a qualidade da análise. O *Brainstorming* Estruturado destaca-se por gerar rapidamente um grande volume de ideias iniciais, facilitando a identificação dos principais aspectos do problema. O *Starbursting* ajuda a decompor a questão-problema de maneira eficiente, utilizando perguntas direcionadoras para alcançar um entendimento rápido. A Cronologia e Linha do Tempo organiza os eventos de forma sequencial, permitindo uma visualização clara e ágil dos fatos críticos. O Mapa Mental

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

contribui para organizar as informações de forma visual e sintética, facilitando a estruturação lógica do raciocínio do analista. Por fim, a Matriz SWOT oferece uma abordagem eficaz para identificar rapidamente forças, fraquezas, oportunidades e ameaças associadas à situação analisada, possibilitando uma avaliação estruturada dos elementos internos e externos mesmo em um contexto de tempo limitado.

As condições impostas aos analistas, como trabalho em equipe ou individual com tempo disponível, e trabalho individual com tempo exíguo, influenciam diretamente a seleção das TAE mais adequadas ao processo de análise, como exemplificado no presente artigo. Cada cenário apresenta desafios e demandas específicos, exigindo que as TAE escolhidas sejam compatíveis com as limitações e oportunidades do contexto.

Nesse sentido, a pesquisa realizada com especialistas em Inteligência oferece subsídios valiosos para a escolha das técnicas mais eficazes, ajudando os analistas a atingirem seus objetivos com precisão e relevância. A adequada integração entre as condições de trabalho, as TAE selecionadas e o suporte proporcionado pela pesquisa contribuem significativamente para a missão dos analistas de Inteligência no assessoramento aos processos decisórios.

Assim, o acesso a esses profissionais enriqueceu a compreensão dos desafios e práticas da Inteligência contemporânea, trazendo contribuições práticas e teóricas ao campo. Recomenda-se que estudos futuros investiguem como esses aprendizados podem ser aplicados para aprimorar a formação de analistas e desenvolver técnicas que atendam às demandas da Era da Informação. Essa abordagem contribuirá para fortalecer o papel da Inteligência na tomada de decisão estratégica, dotando-a de maior eficácia e relevância.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

Referências

Artner, Stephen, Richard S. Girven e James Bruce. 2016. Assessing the value of structures analytic techniques in teh U.S. Intelligence Community. Santa Monica, CA: RAND Corporation. Acesso em 17 de abril de 2024. https://rand.org/pubs/research_reports/RR1408.html.

Brasil. 2019. Manual Técnico – Produção do Conhecimento de Inteligência (EB-70-MT-10.401). 1. ed. Brasília: Comando de Operações Terrestres, Exército Brasileiro. https://bdex.eb.mil.br/jspui/handle/123456789/3270.

Clark, Robert. 2022. Intelligence analysis: A target centric approach. 7. ed. SAGE.

Coulthart, Stephen J. 2017. "An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques," International Journal of Intelligence and CounterIntelligence 30 (2): 368–91. https://doi.org/10.1080/08850607.2016.1230706.

Drell, Bernard. 1993. "Intelligence research – Some suggested approaches," Studies in Intelligence (CIA), 22 de setembro de 1993. Acesso em 20 de março de 2024. https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-1-no-4/intelligence-research-some-suggested-approaches.

Hendrickson, Noel. 2018. Reasoning for Intelligence Analysts - A Multidimensional Approach of Traits, Techniques, and Targets. Rowman & Littlefield.

Heuer, Richards J. e Randolph H. Pherson. 2015. Structured analytic techniques for intelligence analysis. 2. ed. CQ Press.

Heuer, Richards J. e Randolph H. Pherson. 2021. Structured analytic techniques for intelligence analysis. 3. ed. CQ Press.

Liaropoulos, Andrew. 2006. A (r)evolution in intelligence affairs? In search of a new paradigm (Research paper n. 100). Atenas: Research Institute for European and American Studies. https://www.files.ethz.ch/isn/31740/rieas100.pdf.

Smith, Michael. 2017. "A good intelligence analyst," International Journal of Intelligence and CounterIntelligence 30 (1): 181-185. Acesso em 5 de maio de 2024. https://doi.org/10.1080/08850607.2016.1230708.

Teitelbaum, Lorne. 2005. The Impact of the Information Revolution on Policymakers' Use of Intelligence Analysis. Dissertation. Santa Monica, CA: Rand. https://www.rand.org/pubs/rgs_dissertations/RGSD186.html.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.257
ISSN 2595-4717

EUA (Estados Unidos da América). 2017. Joint and national support to military operations (DoD Joint Publication 2-01). Washington: Joint Chiefs of Staff, Department of Defense. https://www.usna.edu/Training/_files/jp2_01_20170705v2.pdf.

EUA (Estados Unidos da América). 2009. A tradecraft primer: Structured analytic techniques for improving intelligence analysis. Washington: Central Intelligence Agency (CIA). Acesso em 20 de março de 2024. https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf.

EUA (Estados Unidos da América). 2020. Intelligence analysis (ATP 2-33.4). Washington: Department of Army.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Artigo de pesquisa

Bruno Martini[1]
ORCiD 0009-0001-8379-5405

Jamille Secchi[2]
ORCiD 0009-0000-3936-5881

Lívia Aparecida de Almeida e Sousa[3]
ORCiD 0000-0001-6421-1614

FORMALIZANDO A INCLUSÃO DA NEURODIVERSIDADE NA INTELIGÊNCIA E NA DEFESA NACIONAL DO BRASIL

https://doi.org/10.58960/rbi.2025.20.260

Martini, Bruno, Jamille Secchi e Lívia Aparecida de Almeida e Sousa. 2025. "Formalizando a inclusão da neurodiversidade na inteligência e na defesa nacional do Brasil." *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.260. https://doi.org/10.58960/rbi.2025.20.260.

Recebido em 26/11/2024
Aprovado em 07/05/2025
Publicado em 30/05/2025

1 Doutorando em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA), mestre em Dinâmica de Sistemas Costeiros e Oceânicos (UFPR). Acadêmico Visitante no Instituto de Política Espacial (SPI) da George Washington University (2023-2024). Membro do Laboratório de Simulação e Cenários Prospectivos (UNIFA), do Grupo de Astronomia e Física de Concórdia/SC (GAFC) e da International Academy of Space Studies (IASS).

2 Clínica Corpus Lab. Mestre em Saúde e Gestão do Trabalho (UNIVALI).

3 Universidade da Força Aérea (UNIFA). Doutora em Linguística Aplicada (UFRJ) e mestre em Ciência da Literatura (UFRJ). Pesquisadora do Laboratório de Simulação e Cenários Prospectivos (UNIFA) e revisora do Instituto Histórico-Cultural da Aeronáutica (INCAER).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

FORMALIZANDO A INCLUSÃO DA NEURODIVERSIDADE NA INTELIGÊNCIA E NA DEFESA NACIONAL DO BRASIL

Resumo

A neurodiversidade, incluindo autismo, TDAH e dislexia, oferece grandes benefícios para a inteligência e defesa do Brasil. Em vez de ser vista como deficiência, deve ser reconhecida como uma fonte de riqueza e potencial. Integrar a neurodiversidade nesses setores pode ampliar perspectivas, criar vantagens competitivas, aproveitar habilidades únicas e melhorar a análise de ameaças e oportunidades. Exemplos práticos no Brasil incluem análise de dados, desenvolvimento de IA e cibersegurança. Entretanto, desafios como estigma, preconceito, necessidade de mudança cultural e falta de infraestrutura devem ser enfrentados. Para promover a inclusão da neurodiversidade, é essencial aumentar o conhecimento, revisar métodos de contratação, implementar políticas inclusivas e criar ambientes de trabalho acolhedores.

Palavras-chave: autismo, inteligência de Estado, neurodivergência, vantagem neurodiversa.

FORMALIZING THE INCLUSION OF NEURODIVERSITY IN BRAZIL´S NATIONAL INTELLIGENCE AND DEFENSE

Abstract

Neurodiversity, including autism, ADHD and dyslexia, offers great benefits for Brazil's intelligence and defense. Rather than being seen as a disability, it should be recognized as a source of wealth and potential. Integrating neurodiversity into these sectors can broaden perspectives, create competitive advantages, harness unique skills and improve threat and opportunity analysis. Practical examples in Brazil include data analysis, AI development and cybersecurity. However, challenges such as stigma, prejudice, the need for cultural change and a lack of infrastructure must be addressed. To promote the inclusion of neurodiversity, it is essential to increase knowledge, review hiring methods, implement inclusive policies and create welcoming work environments.

***Keywords**: autism, state intelligence, neurodivergency, neurodiverse advantage.*

FORMALIZAR LA INCLUSIÓN DE LA NEURODIVERSIDAD EN LA INTELIGENCIA Y LA DEFENSA NACIONAL BRASILEÑAS

Resumen

La neurodiversidad, incluidos el autismo, el TDAH y la dislexia, ofrece grandes ventajas para la inteligencia y la defensa de Brasil. En lugar de ser vista como una discapacidad, debería ser reconocida como una fuente de riqueza y potencial. Integrar la neurodiversidad en estos sectores puede ampliar las perspectivas, crear ventajas competitivas, aprovechar habilidades únicas y mejorar el análisis de amenazas y oportunidades. Ejemplos prácticos en Brasil son el análisis de datos, el desarrollo de la IA y la ciberseguridad. Sin embargo, hay que hacer frente a retos como la estigmatización, los prejuicios, la necesidad de un cambio cultural y la falta de infraestructuras. Para promover la inclusión de la neurodiversidad, es esencial aumentar el conocimiento, revisar los métodos de contratación, aplicar políticas inclusivas y crear entornos de trabajo acogedores.

***Palabras clave**: autismo, inteligencia estatal, neurodivergencia, ventaja neurodiversa.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Introdução

Em 19 de fevereiro de 2024, o engenheiro espacial Danilo Miranda (2024) postou na rede social profissional LinkedIn um currículo recebido de um garoto brasileiro de 8 anos, que se autodenominou "autista com Altas Habilidades e Superdotação". Além de estar cursando o Nível Fundamental 1, o garoto incluiu em sua formação acadêmica cinco cursos online concluídos pela Agência Espacial Brasileira (AEB) e Astrofísica 1 pela Universidade Federal de Santa Catarina (UFSC). Outro colega, engenheiro em microeletrônica e empreendedor, sugeriu que o garoto fosse mentorado por Miranda para aprender a "navegar" em um mundo ultra diverso e de interesses distintos, para que tivesse as condições de sobreviver, florescer e fazer a diferença no mundo que tanto busca. Ele expressou preocupação ao ver que muitos talentos fora do padrão, na fase adulta, sofrem discriminação e até mesmo punição por seu brilhantismo, perdendo oportunidades profissionais e relegando suas capacidades diferenciadas a hobbies ultrassofisticados.

Semanas antes, em 7 de fevereiro de 2024, um dos autores deste artigo havia participado do evento "AI and Neurodiversity" no think tank Center for Strategic & International Studies (CSIS) em Washington D.C., Estados Unidos da América (EUA), onde se discutiu um tema relacionado. Durante um debate, Lakshmi Raman, diretora de Inteligência Artificial da Central Intelligence Agency (CIA), Courtney Weinbaum, cientista sênior da RAND, Peter Kant, CEO da Enabled Intelligence e Kiersten Todt da Cybersecurity and Infrastructure Security Agency (CISA) debateram como líderes em inovação tecnológica, cibersegurança e inteligência artificial precisam incorporar mais indivíduos neurodiversos para criar forças de trabalho com maior diversidade de pensamento capazes de resolver problemas complexos e construir soluções mais eficazes.

Ainda não há uma definição clara para a palavra "neurodiversidade". Segundo Abreu (2022), o conceito foi elaborado pela socióloga australiana especialista em autismo Judy Singer e pelo jornalista estadunidense Harvey Blume a partir de trocas de correspondências em 1996. O think tank estadunidense RAND (Weinbaum *et al.* 2023) descreveu neurodiversidade como "um termo genérico que abrange uma ampla gama de diagnósticos cognitivos, incluindo (mas não exclusivamente) Transtorno do Espectro do Autismo (TEA), Transtorno do Déficit de Atenção (TDA) e Transtorno do Déficit de Atenção/Hiperatividade (TDAH), dislexia, discalculia e síndrome de Tourette", com a ressalva de que não é um termo médico e inclui diagnósticos cognitivos e de desenvolvimento. Sadzinski Junior *et al.* (2021) evidenciaram que ainda há pouca produção de estudos com o termo neurodiversidade no Brasil.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

É importante ressaltar que o termo neurodiversidade refere-se à ideia de que diferenças neurológicas como autismo, TDAH, dislexia, entre outros, são variações naturais do funcionamento cerebral e devem ser compreendidas, respeitadas e valorizadas. Indivíduos neurodivergentes compreendem a realidade e os problemas por prismas diferentes, contribuindo assim para suas resoluções. Muitos possuem habilidades especiais como resolver enigmas, hiperfoco, hiperconcentração, atenção aos detalhes, memorização, raciocínio matemático e lógico, identificação de padrões, pensamento visual e lateral, além da disposição para ousar e experimentar opções não convencionais.

Este artigo propõe discutir a abertura das instituições de defesa e inteligência brasileiras à neurodiversidade, reconhecendo o potencial de indivíduos com autismo, TDAH e outras condições neurológicas para contribuir significativamente para a defesa nacional. Ao visar especificamente a defesa nacional do Brasil, prioritariamente contra ameaças externas e diferenciando-se da segurança contra ameaças internas, consideram-se as três forças armadas singulares: o Exército Brasileiro (EB), a Força Aérea Brasileira (FAB) e a Marinha do Brasil (MB), além da agência de inteligência de Estado da Presidência da República, a Agência Brasileira de Inteligência (ABIN). Contemplando também a iniciativa privada, incluem-se as empresas que compõem a Base Industrial de Defesa (BID). O tema torna-se ainda mais instigante ao considerar o significativo aumento no diagnóstico de algumas dessas condições em crianças, como o TDAH (Xu et al. 2018) e o TEA[1] (Salgado et al. 2022), cujas causas ainda são incertas. Segundo Martins (2022), via Ministério da Saúde, entre 5 a 8% da população mundial possui TDAH.

Esta pesquisa é de natureza exploratória e qualitativa, fundamentada em uma revisão bibliográfica narrativa. Foram analisados documentos técnicos, relatórios institucionais, artigos acadêmicos e fontes jornalísticas sobre neurodiversidade, inteligência e defesa nacional. As fontes foram selecionadas por sua relevância contemporânea e por abordarem diretamente os temas de empregabilidade de neurodivergentes e inovação organizacional em setores estratégicos. A análise concentrou-se na identificação de padrões de aplicação prática, desafios institucionais e propostas de políticas públicas inclusivas.

Com base na revisão da literatura, argumenta-se aqui a proposição original e exploratória de que a neurodiversidade é uma fonte inexplorada de benefícios para a inteligência e defesa do Brasil. A neurodiversidade amplia as

1 Importante destacar que o Transtorno do Espectro Autista apresenta três níveis de suporte, conforme o Manual Estatístico e Diagnóstico de Transtornos Mentais DSM-5-TR (APA 2022). Nem todos os autistas possuem habilidades cognitivas compatíveis com as funções de inteligência, sendo necessário avaliar caso a caso.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

perspectivas, pois a diversidade de pensamento e abordagens na resolução de problemas aumenta as chances de gerar soluções inovadoras e criativas. Além disso, os países que valorizam e aproveitam melhor a neurodiversidade poderão obter uma vantagem estratégica sobre aqueles que não o fizerem (Austin *et al.* 2017; Davis 2021). Indivíduos neurodivergentes frequentemente percebem detalhes, padrões e tendências que outros podem não notar, o que pode ser extremamente útil na identificação de ameaças e oportunidades táticas e estratégicas. Portanto, este artigo destaca a importância de reconhecer a neurodiversidade como uma fonte de potencial e não como uma deficiência.

Metodologia

Este estudo adota uma abordagem exploratória e qualitativa, centrada na análise teórica e documental sobre a inclusão da neurodiversidade nos setores de inteligência e defesa nacional. A investigação fundamenta-se em uma revisão narrativa da literatura, associada à análise crítica de documentos oficiais, relatórios institucionais e iniciativas públicas e privadas tanto no Brasil quanto no exterior. Optou-se por essa estratégia metodológica em razão da escassez de dados empíricos sobre o tema no contexto brasileiro e da natureza inovadora da proposta.

Foram analisadas fontes primárias como editais públicos da Agência Brasileira de Inteligência (ABIN), normativas das Forças Armadas, diretrizes ministeriais e documentos internacionais emitidos por instituições como a Central Intelligence Agency (CIA), National Security Agency (NSA), RAND Corporation e Secret Intelligence Service (SIS) do Reino Unido. Complementarmente, foram incluídas fontes secundárias de natureza acadêmica, como artigos científicos sobre neurodivergência, empregabilidade e inclusão organizacional, além de publicações jornalísticas e depoimentos em mídias sociais que ilustram a percepção pública e institucional sobre o tema.

A análise foi guiada por três questões orientadoras: (1) De que forma a neurodiversidade pode ser integrada produtivamente nas estruturas de inteligência e defesa do Brasil? (2) Quais barreiras normativas, estruturais e culturais dificultam essa integração? (3) Quais estratégias e políticas podem promover uma inclusão eficaz, ética e segura da população neurodivergente nesses setores?

Essa abordagem permite mapear práticas já existentes e apontar lacunas estruturais que impedem avanços concretos. Além disso, articula evidências internacionais com o contexto nacional, buscando oferecer proposições iniciais para políticas públicas mais inclusivas e inovadoras. Ao integrar elementos

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

normativos, técnicos e sociocognitivos, a metodologia adotada fortalece a consistência argumentativa e amplia o potencial de contribuição da presente pesquisa para os debates sobre diversidade e inovação no campo da defesa e da inteligência sem perder o foco na produtividade e eficiência dos serviços de defesa e inteligência para os interesses do Brasil.

As limitações desta abordagem concentram-se na ausência de dados quantitativos sistematizados, o que reforça a necessidade de estudos empíricos futuros. No entanto, o caráter exploratório permite levantar hipóteses, mapear direções de pesquisa e propor caminhos institucionais com base nas melhores evidências disponíveis.

Com a finalidade de tornar o percurso metodológico mais claro e didático, o quadro abaixo (Quadro 1) visa facilitar a compreensão dos dados analisados.

Quadro 1
Quadro do Percurso Metodológico

Tema	Fonte	Método de análise	Observações
Políticas públicas	Documentos da ABIN, MD, etc.	Análise documental	Normas de acesso e inclusão
Práticas internacionais	CIA, RAND, CSIS, empresas	Revisão de relatórios	Modelos referenciais
Aspectos sociocognitivos	Literatura acadêmica	Revisão bibliográfica	Neurodiversidade, TEA, TDAH, dislexia etc.

Fonte: elaboração dos autores (2025).

No próximo tópico, as vantagens competitivas neurodiversas são discutidas. Identificam-se as dificuldades para a incorporação da mão de obra neurodiversa na defesa e inteligência. E, então, são apresentadas as considerações finais com proposições de possíveis soluções e a recomendação de estudos futuros.

Incorporando a vantagem neurodiversa

Para além do TEA e TDAH, outras formas de neurodivergência – como dislexia, discalculia e síndrome de Tourette – também merecem atenção, especialmente se associadas a trajetórias educativas e socioeconômicas diversas. Iniciativas inclusivas devem considerar, por exemplo, a interseccionalidade entre neurodiversidade, gênero, raça, e classe social, ampliando o escopo de representatividade e impacto em prol da eficiência dos setores da defesa e inteligência nacional.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Segundo James A. Lewis, vice-presidente da CSIS, "a diversidade proporciona vantagem". Afinal, as inteligências neurotípicas (que representam a vasta maioria da população) são mais previsíveis e mais facilmente antecipadas pelos adversários (CSIS 2024). A diversidade de pensamentos e perspectivas contribui para a geração de soluções inovadoras e a resolução de problemas de maneira mais criativa. Diferentes padrões de pensamento envolvidos na solução de um problema aumentam a probabilidade de serendipidades, ou seja, descobertas feitas por acaso. Conjuntos de soluções diferentes e inovadoras para um mesmo problema oferecem opções mais abrangentes para abordar uma situação, potencialmente levando a resultados mais eficazes. Segundo Raman (CSIS 2024), a CIA até tem usado o termo "neurodiverse advantage" ("vantagem neurodiversa"). Pessoas que veem o mundo de forma diferente são valiosas exatamente por isso.

Na defesa, aproveitar a vantagem neurodiversa pode levar a soluções alternativas, mais criativas e mais difíceis de serem antecipadas pelo adversário. Essa antecipação pode ser ainda mais necessária quando se considera que certos competidores estrangeiros já podem estar se utilizando desses benefícios. Ao menos algumas empresas dos EUA (CAI 2024) e agências de inteligência já estão declaradamente fazendo isso (CSIS 2024). A National Security Agency, em seu plano de recrutamento de 2020 (EUA 2020), informa como seus Gerentes do Programa para Recrutamento de Portadores de Deficiência participam de diversos eventos buscando pessoas com certas características desejáveis, incluindo condições neurodivergentes. A CIA, em sua estratégia de inclusão e diversidade (EUA 2022), coloca o aumento da taxa de contratação de neurodivergentes como seu segundo objetivo estratégico. No Reino Unido, o Intelligence Community's Design System (ICDS) descreve como tornar conteúdos mais acessíveis ao público neurodivergente em benefício da comunidade de inteligência britânica, como o Security Service (MI5), Secret Intelligence Service (SIS/MI6), Government Communications Headquarters (GCHQ) e seus parceiros (Reino Unido 2024).

Alguns neurodivergentes possuem capacidades que os colocam em vantagem em relação aos neurotípicos em certas atividades. O autismo, por exemplo, é caracterizado como um transtorno neurológico que afeta a comunicação, o comportamento e a capacidade de interação social. A condição não define nem limita a capacidade geral da pessoa com autismo, pois há habilidades específicas evidenciadas nas pessoas com espectro autista; dentre elas: a habilidade de se atentar a detalhes específicos que passam facilmente despercebidos por pessoas neurotípicas, memória excepcional, hiperfoco e capacidade analítica aguçada que facilita a identificação de padrões e o

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

processamento eficiente de informações complexas (Adams 2020; Baron-Cohen 2006; 2012; Baron-Cohen *et al.* 2009). Na Austrália, Austin *et al.* (2017) relataram como a Australian Defence Organization (ADO), em parceria com empresas especializadas, estava recrutando analistas cibernéticos dentro do espectro autista que dificilmente se candidatariam às vagas. Morgan McCardell deu entrevista relatando como seu autismo a ajudou a ser uma analista da National Geospatial-Intelligence Agency (NGA) dos EUA, identificando padrões em imagens satelitais no atual conflito na Ucrânia (CBS 2023).

Isso já abre um panorama que mostra como a inclusão de pessoas neurodivergentes pode ser benéfica nos ambientes de trabalho, podendo contribuir de forma significativa em operações, desde as mais simples até as mais complexas. Outro exemplo são os casos de pessoas diagnosticadas com TDAH, que normalmente são vistas como desatentas e agitadas, conforme seu diagnóstico, mas que possuem habilidades interessantes. Se exploradas, essas habilidades podem contribuir nos ambientes de trabalho, incluindo a segurança nacional. Por exemplo, criatividade (Boot *et al.* 2020), hiperfoco em determinadas tarefas (Ashinoff e Abu-Akel 2021), capacidade de multitarefas e pensamento rápido e capacidade de adaptação (WildAlaskanRed 2022, LethalityJane 2023).

Han *et al.* (2019), em uma revisão da literatura, reportaram como o TDAH pode ser mais frequente em atletas de alto rendimento em certos esportes, afetando seu rendimento positivamente em alguns aspectos e moldando suas escolhas por tais atividades físicas. Sua intensa dedicação nos treinamentos frequentemente resulta até em uma maior taxa de contusões e um tempo mais prolongado para sua recuperação. Atletas olímpicos como Michael Jordan e Michael Phelps já declararam ter TDAH (Vlad e Lungu 2017).

É possível recorrer e demonstrar, segundo pesquisas e estudos recentes, as mais variadas habilidades e capacidades diferenciadas associadas a alguns indivíduos diagnosticados com cada uma das condições abarcadas pela neurodiversidade. No entanto, tal detalhamento não é o objetivo deste artigo. A intenção é apenas enfatizar que, embora as dificuldades e "limitações" sejam frequentemente ressaltadas quando se pensa em neurodivergentes, há inúmeras habilidades e capacidades raras inerentes a essas pessoas. É preciso trazer à tona essas qualidades para que elas possam contribuir com todo seu potencial e serem vistas de maneira integral e produtiva pela sociedade, e não apenas como alguém "diferente".

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Os obstáculos autoimpostos para a seleção de pessoal na defesa e inteligência

Nem todos os neurodivergentes possuem habilidades especiais úteis aos setores da defesa e inteligência ou são aptos a exercer essas atividades, exatamente da mesma forma que ocorre com os neurotípicos. O argumento aqui defendido é evitar desperdiçar certos talentos úteis apenas por não se enquadrarem nos métodos de recrutamento tradicionais atuais. E, a partir daí, buscar soluções inteligentes que aproveitem todo o potencial latente para o desenvolvimento do Brasil no cenário globalizado e altamente competitivo.

Historicamente e globalmente, as comunidades de defesa e inteligência podem ter restringido a qualidade de suas atividades por limites autoimpostos, como não recrutar mulheres, pessoas fora dos limites máximos e mínimos de altura, peso ou em certas condições de saúde para determinadas funções que poderiam ser realizadas com alto desempenho. Muitas dessas limitações já se mostraram improdutivas e foram alteradas nos métodos de contratação e alistamento de pessoal. Somente em tempos mais recentes as Forças Armadas têm se aberto a novas possibilidades de inclusão social. Em 1980, a Marinha permitiu o ingresso oficial de mulheres pela primeira vez nas Forças Armadas do Brasil, e até hoje o fazem apenas por meio das escolas preparatórias de oficiais (Lombardi *et al.* 2009) ou concursos públicos. Entretanto, planeja-se que em 2025 mulheres poderão se alistar, inclusive como soldados de infantaria, com ingresso previsto para 2026 (Feitoza 2024). A partir de 2011, quando o Supremo Tribunal Federal (STF) equiparou casais homossexuais aos heterossexuais, alguns militares passaram a declarar cônjuges do mesmo sexo como dependentes no cadastramento previdenciário e no sistema de saúde militar, sendo o primeiro caso oficializado em 2013 no Exército (Stochero 2013).

Segundo os "índices mínimos de aptidão de conscritos para o Serviço Militar nas Forças Armadas", a altura mínima exigida é de 1,55m e para alturas acima de 1,95m a admissão está condicionada à proporcionalidade biotipológica. Há ainda requisitos mínimos de acuidade visual, senso cromático e capacidade auditiva (Brasil 1992). A Instrução Normativa nº 8 de 2017 estabelece critérios para a prova de capacidade física para os concursos públicos para ingresso nos cargos de Agente de Inteligência e Oficial de Inteligência da ABIN, que prevê provas de corrida e natação, salvo em certos casos de comprovada deficiência física compatível com a função (Brasil 2017a).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

As avaliações psicológicas nos concursos públicos são regidas pela Instrução Normativa nº 11 de dezembro de 2017, conforme testes psicológicos aprovados pelo Conselho Federal de Psicologia (CFP), que determinam se o candidato preenche os requisitos ou apresenta as habilidades necessárias para atuar no cargo em questão (Brasil 2017b). Um diagnóstico neurodivergente não é critério de eliminação desde que o candidato apresente as habilidades necessárias para atuar no cargo do Plano de Carreiras e Cargos da ABIN. Mesmo assim, a avaliação quanto ao cumprimento dessas demandas poderia ser revista à luz da ativa inclusão da vantagem neurodiversa para funções específicas ainda não regulamentadas.

De acordo com todos os editais de contratação da ABIN (Brasil 2018), certos conhecimentos obrigatórios, como especificidades do Direito Administrativo, são fatores limitantes questionáveis, não apenas para o público neurodiverso, mas também para muitos outros perfis intelectuais não afeitos a esta ou outras disciplinas. Tais editais tendem a ser excessivamente padronizantes e intelectualmente excludentes, enquanto a atividade de inteligência demanda cada vez mais diversidade intelectual para resolver os complexos desafios contemporâneos.

Diante do avanço científico e tecnológico disruptivo - como nas atividades de guerra e inteligência eletrônica e cibernética, operações espaciais, IA e robótica - e das crescentes demandas analíticas, é válido questionar se os critérios atuais de seleção em defesa e inteligência contemplam adequadamente o potencial de profissionais com perfis cognitivos diversos, inclusive aqueles que, mesmo dentro dos espectros neurodiversos, demonstrem habilidades compatíveis e até altamente adequadas a tais funções. Por exemplo, nem todos os soldados precisam estar fisicamente aptos para correr empunhando fuzis; alguns precisam apenas estar atualizados com os últimos avanços tecnológicos e científicos ou, até mesmo, apenas possuir uma capacidade natural de pensar de forma distinta da média. Da mesma forma, nem todos os Oficiais Técnicos de Inteligência e Agentes de Inteligência da ABIN precisam ser nadadores habilitados em direito e geografia; basta que sejam altamente competentes em funções específicas de grande relevância para a inteligência de Estado.

Pode ser necessário transcender a rigidez dos requisitos estabelecidos no alistamento militar e nos concursos públicos, incluindo o ainda em planejamento para a carreira civil do Ministério da Defesa (Rodrigues e Ribeiro 2023). As Forças Armadas, a ABIN e as empresas da Base Industrial de Defesa (BID) precisam repensar seus métodos de seleção de pessoal para atrair e recrutar

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

essas pessoas. E após o recrutamento, é essencial criar um ambiente que permita a integração e o desenvolvimento desses indivíduos. Como discutido no evento da CSIS (2024), uma das abordagens pode ser simplesmente perguntar-lhes o que necessitam em seu local de trabalho ou se precisam de um escritório físico quando podem realizar suas tarefas remotamente, com horários flexíveis e metas ou prazos de produtividade definidos. Para alguns membros da comunidade neurodiversa, até mesmo o acesso convencional ao prédio pode ser um desafio ou um impedimento, como dirigir até o local, usar crachás, senhas ou interagir com recepcionistas ou seguranças. Outras vulnerabilidades comuns a muitos indivíduos neurodivergentes podem incluir problemas de adequação social, possíveis falhas de expressão verbal, hipersensibilidade a estímulos sensoriais, entre outras.

Estudar a diversidade neurológica auxilia na compreensão de como o cérebro sustenta a mente (Nobre e Van Ede 2020). Diferentes tipos de cérebros oferecem mais percepções e ampliam a compreensão sobre o funcionamento da mente humana. Por isso, embora se reconheça o valor da integração entre IA e humanos, pouco se discute sobre a consideração da multiplicidade de intelectos humanos. Peter Kant (CSIS 2024), um desenvolvedor privado de IA, ressalta a importância de integrar o intelecto neurodiverso à IA e ao aprendizado de máquinas para uma representatividade mais fiel da inteligência humana. Afinal, se a IA busca simular o funcionamento do cérebro humano, a neurodiversidade é uma parte historicamente negligenciada desse processo.

Historicamente, as diferenças neurológicas foram estigmatizadas e mal compreendidas. Contudo, à medida que pesquisas evidenciam e as empresas reconhecem o valor da inclusão e diversidade, muda-se lentamente o padrão social de compreender a neurodivergência, abrindo espaço para a atuação profissional dessas pessoas (de Freitas 2016). Indivíduos neurodivergentes têm muito a oferecer às organizações, desde habilidades únicas até perspectivas inovadoras. Investir na inclusão e apoio a essas pessoas promove justiça social e impulsiona inovação e sucesso organizacional a longo prazo. A CAI, por exemplo, é uma empresa de soluções tecnológicas que se diferencia no mercado pelo pioneirismo no emprego ativo da comunidade neurodiversa como estratégia de marketing (CAI 2024). Empresas comprometidas com inclusão e diversidade são vistas mais positivamente por clientes, parceiros e colaboradores potenciais.

Empresas da Base Industrial de Defesa (BID) encontrariam maior flexibilidade que o Estado para fazer adaptações normativas e logísticas. A defesa e inteligência do Brasil certamente já contam com indivíduos neurodiversos que

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

podem esconder sua condição para evitar rótulos prejudiciais. O dilema da acomodação, como descrito por Weinbaum *et al.* (2023), ocorre quando um funcionário poderia se beneficiar de adaptações específicas às suas necessidades, mas hesita em se declarar deficiente devido ao possível impacto em sua reputação. Contribui para essa mudança de paradigma na sociedade o fato de um número crescente de celebridades declararem publicamente suas condições neurodiversas (Budryk 2021).

Para exemplificar a aplicação da neurodiversidade na inteligência e defesa, destacam-se as áreas como análise de dados e cibersegurança. Alguns indivíduos com autismo, por exemplo, podem ter habilidades notáveis para analisar grandes volumes de dados e identificar padrões (Austin *et al.* 2017; CBS 2023). Na cibersegurança, algumas pessoas com TDAH podem se sobressair pela capacidade de multitarefa e pensamento rápido, qualidades valiosas na defesa contra ataques cibernéticos (LethalityJane 2023). Além disso, indivíduos hiperfocados podem acelerar a conclusão de projetos específicos. Assim, enfatiza-se a importância de integrar a vantagem neurodiversa nas estratégias da comunidade de defesa e inteligência do Estado.

Considerações Finais

Embora desafiadora, a inclusão de neurodivergentes no local de trabalho pode dinamizar a cultura organizacional e fomentar inovação. Essa diversidade estimula a criatividade e a resolução de problemas, promovendo um ambiente mais inclusivo e equitativo, valorizando pessoas historicamente subestimadas pelo mercado e aproveitando suas raras e até únicas particularidades em prol da produtividade institucional.

É essencial que iniciativas para incorporar a neurodiversidade se estendam além das instituições federais e privadas da BID. Para propósitos de defesa nacional brasileira, precisam ser também pensadas iniciativas pelo próprio Ministério da Defesa (MD), Ministério de Ciência, Tecnologia e Inovação (MCTI), entre outros ministérios relacionados e seus órgãos componentes, em especial os órgãos de segurança pública. Cada um desses precisa fomentar discussões internas e externas sobre revisar seus métodos de contratação, condições de trabalho e planos de carreira à luz do potencial para vantagem competitiva pela inclusão da comunidade neurodiversa. Isso implica repensar requisitos para servidores, focando nos desafios contemporâneos em vez de se restringir aos sistemas atuais de alistamento e concursos. Novos estudos para a realidade de cada órgão ou realidade profissional precisam ser estimulados e fomentados. Isso abriria mais uma possibilidade para interações interdisciplinares entre

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

profissionais de defesa, inteligência, psicologia e psiquiatria.

Promover conhecimento sobre neurodiversidade é crucial para superar estigmas. Sem esforços para mudar paradigmas, aumentam-se os estereótipos sociais e as dificuldades de interação. Políticas inclusivas são fundamentais antes da contratação proativa de neurodivergentes, garantindo igualdade de oportunidades e suporte necessário. Oferecer treinamentos e material informativo aos servidores contribui para a conscientização. Ambientes acolhedores aumentam o engajamento dos servidores, reduzindo rotatividade e custos com recrutamento e treinamento. A identificação de servidores neurodiversos existentes é vital para mapear obstáculos e facilitadores institucionais, encorajando-os a romper com o dito dilema da acomodação.

Algumas vagas deveriam ser reservadas para contratar pessoal com qualidades analíticas específicas. Por exemplo, testes online para certas funções poderiam ser mais realistas e inclusivos do que concursos públicos, adaptados para diferentes estímulos mentais, tais como através de textos imagéticos, áudios, ilustrações, vídeos, linguagem matemática etc. (Reino Unido 2024). No Exército (EB), Força Aérea (FAB) e Marinha (MB), vagas para Oficiais Temporários poderiam ter maior flexibilidade para funções que exigem habilidades especiais, como em criptografia, metadados, robótica, programação, operações espaciais, cibernéticas, etc. E assim como as Forças Armadas estabeleceram Oficiais Temporários, poderia ser pensado para a ABIN cargos de Oficiais Técnicos de Inteligência Temporários (OTIT) e Agentes Técnicos de Inteligência Temporários (ATIT), que estivessem sujeitos a um plano de carreira mais curto, sem direito à aposentadoria na função, desonerando o Estado, desobrigando-o de sua responsabilidade quanto a potenciais inadequações de saúde dos aprovados, protegendo-o por contratos de confidencialidade e ainda aproveitando habilidades especiais que de outra forma seriam desperdiçadas pelo Estado, tornando-o mais inclusivo, oferecendo ao acompanhamento de saúde, psicológico, condicionamento físico e/ou fisioterapia e oportunidades de trabalho e capacitação de alto nível.

Futuras pesquisas científicas precisam investigar tais demandas institucionais para a variabilidade do espectro de mentes neurodiversas, possivelmente priorizando de início as mais comuns e com maior potencial de retorno produtivo, como (talvez) o TEA, TDA e TDAH. A proposta é mudar a cultura de contratação e retenção, criando ambientes de trabalho empáticos e inclusivos, com segurança psicológica e a promoção de um diálogo aberto e transparente. A inclusão visa não só ao bem-estar dos indivíduos marginalizados, mas também à competitividade e à produtividade das instituições e, em última análise, à

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

qualidade da inteligência de Estado e da defesa nacional.

A neurodiversidade pode trazer benefícios significativos, como a ampliação da perspectiva, vantagem competitiva e melhor compreensão de ameaças e oportunidades. Exemplos práticos de sua aplicação no Brasil incluem a análise de dados, desenvolvimento de IA e a cibersegurança, onde as habilidades únicas de indivíduos neurodivergentes podem ser aproveitadas. Estes autores defendem que os desafios contemporâneos são demasiadamente complexos e difíceis para não incluírem a neurodiversidade.

De forma propositalmente introdutória, este artigo demonstra a importância de se explorar a vantagem neurodiversa na inteligência e defesa nacionais para se obter vantagens estratégicas e competitivas. A neurodiversidade, compreendida como um espectro de variações neurológicas, é vista não como uma deficiência, mas como uma riqueza natural do funcionamento cerebral que pode tornar as instituições de inteligência e defesa mais eficientes, eficazes e inovadoras diante dos complexos e dinâmicos desafios globais contemporâneos.

Conforme o Centro de Controle e Prevenção de Doenças dos Estados Unidos, cerca de 1 em cada 36 crianças no país está dentro do espectro autista. E como publicou Martins (2022), no Brasil, estima-se que o TDAH afete entre 5% a 8% da população. No entanto, ainda há escassez de dados nacionais sobre a inserção de neurodivergentes em funções estratégicas como as de inteligência. De maneira semelhante, não existem estatísticas públicas sobre a quantidade de profissionais neurodiversos nas Forças Armadas ou na ABIN. Pesquisas futuras podem preencher essa lacuna e apoiar o desenho de políticas baseadas em evidências quantitativas. Outra possível linha seria mapear os perfis cognitivos mais frequentes em concursos de inteligência e defesa, a fim de propor adequações mais inclusivas, assim como identificar atuais servidores com algum diagnóstico neurodivergente. Entrevistas com esses servidores podem apontar possíveis caminhos para as melhorias requeridas nos métodos de seleção de pessoal para a defesa e a inteligência, no ambiente de trabalho e nos processos internos.

É esperado que este artigo seja prolífero, atraindo a atenção de mais profissionais para o assunto da neurodivergência, da neurotipia e de seus processos cognitivos e neurológicos, estimulando a colaboração acadêmica multidisciplinar de profissionais da ABIN e MD com psicólogos, psiquiatras e outros pesquisadores também nesta temática de vanguarda.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Agradecimentos

Este estudo contou com financiamento da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) na forma de uma bolsa de estudos do Programa de Doutorado Sanduíche no Exterior (PDSE) concedida ao primeiro autor para estudar de novembro de 2023 a agosto de 2024 na George Washington University em Washington, D.C., Estados Unidos da América (EUA). Agradecemos também ao Grupo de Pesquisa Ensino Militar: Estratégias Formativas e Prospectivas, inserido no Laboratório de Simulações e Cenários (LSC) do Centro de Estudos Estratégicos (CEE) da Universidade da Força Aérea (UNIFA).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Referências

Abreu, Tiago. 2022. *O que é neurodiversidade?* Goiânia: Cânone Editoração Ltda.

Adams, Carol A. 2020. "Neurodiversity at Work Benefits Everyone – Why Companies Are Hiring Autistic People." *The Conversation*, 24 de setembro de 2020. https://theconversation.com/neurodiversity-at-work-benefits-everyone-why-companies-are-hiring-autistic-people-146788.

APA (American Psychiatric Association). 2022. *Diagnostic and statistical manual of mental disorders*. 5ª edição. Washington: American Psychiatric Association.

Ashinoff, Brandon K., e Ahmad Abu-Akel. 2021. "Hyperfocus: the forgotten frontier of attention." *Psychological Research* 85 (1): 1–19. https://doi.org/10.1007/s00426-019-01245-8.

Austin, Robert D., Michael Fieldhouse, Aiyaswami Mohan, and Peter Quinn. 2017. "Why the Australian Defence Organization is recruiting cyber analysts on the autism spectrum." *Harvard Business Review*, 7 de dezembro de 2017.

Baron-Cohen, Simon. 2006. "The hyper-systemizing, assortative mating theory of autism." *Progress in Neuro-Psychopharmacology and Biological Psychiatry* 30 (5): 865–872. https://doi.org/10.1016/j.pnpbp.2006.01.010.

Baron-Cohen, Simon. 2012. "Autism and the technical mind: children of scientists and engineers may inherit genes that not only confer intellectual talents but also predispose them to autism" *Scientific American* 307 (5).

Baron-Cohen, Simon, Emma Ashwin, Chris Ashwin, Teresa Tavassoli e Bhismadev Chakrabarti. 2009. "Talent in autism: hyper-systemizing, hyper-attention to detail and sensory hypersensitivity." *Philosophical Transactions of the Royal Society B: Biological Sciences* 364 (1522): 1377–1383. https://doi.org/10.1098/rstb.2008.0337.

Boot, Nathalie, Barbara Nevicka e Matthijs Baas. 2020. "Creativity in ADHD: goal-directed motivation and domain specificity." *Journal of Attention Disorders* 24 (13): 1857–1866. https://doi.org/10.1177/1087054717727352.

Brasil. 1992. Decreto nº 703 de 22 de dezembro de 1992. https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d703.htm.

Brasil. 2017a. Instrução Normativa nº 8 ABIN/GSI/PR de 28 de dezembro 2017. Agência Brasileira de Inteligência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Brasil. 2017b. Instrução Normativa nº 11 ABIN/GSI/PR de 28 de dezembro 2017. Agência Brasileira de Inteligência.

Brasil. 2018. Edital nº 1 do Concurso Público para Provimento de Vagas nos Cargos de Oficial de Inteligência, de Oficial Técnico de Inteligência e de Agente de Inteligência. Agência Brasileira de Inteligência, 2 de janeiro de 2018.

Budryk, Zack. 2021. "More Celebrities Are Coming Out as Autistic. That Makes a Huge Difference." Washington Post, 8 de setembro de 2021.

CAI. 2024. "CAI Neurodiverse Solutions." https://www.cai.io/neurodiverse-solutions/overview.

CBS. 2022. "Autistic Analysts Help U.S. Spy Agency." CBS This Morning, 21 de abril de 2022. https://www.cbs.com/shows/video/_XCOWqlrt7c6xXBE6GC0xIiHGTQlWhhx/.

CSIS (Center for Strategic and International Studies). 2024. "AI and Neurodiversity. Strategic Technologies Program, Diversity and Leadership in International Affairs Project." Acessado em 7 de fevereiro de 2024. https://www.csis.org/events/ai-and-neurodiversity.

Davis, Tre. 2021. "Airman Advocates for Neurodiversity in Military." U.S. Air Force, 6 de agosto de 2021.

De Freitas, Ana Beatriz Machado. 2016. "Da concepção de deficiência ao enfoque da neurodiversidade." *Revista Científica de Educação* 1 (1): 86–97.

EUA (Estados Unidos da América). 2020. *FY2020 National Security Agency Affirmative Action Plan*. National Security Agency (NSA). https://www.nsa.gov/Portals/75/documents/about/diversity/2020_AAP_External_Web_Report_ACCESSIBLE.pdf.

EUA (Estados Unidos da América). 2022. *2022-2023 CIA Diversity and Inclusion Strategy*. Central Intelligence Agency. https://www.cia.gov/static/c26da464843c5aee8217ef3919b19638/2020-2023-DI-Strategy.pdf.

Feitoza, Carlos. 2024. "Forças Armadas vão permitir o alistamento militar feminino pela primeira vez em 2025." Folha de São Paulo, 1º de junho de 2024. https://www1.folha.uol.com.br/poder/2024/06/forcas-armadas-vao-permitir-alistamento-militar-feminino-pela-1a-vez-em-2025.shtml.

Han, Doug H., David McDuff, Donald Thompson, Mary E. Hitchcock, Claudia L. Reardon e Brian Hainline. 2019. "Attention-Deficit/Hyperactivity Disorder in elite athletes: A Narrative Review." *British Journal of Sports Medicine* 53 (12). http://dx.doi.org/10.1136/bjsports-2019-100713.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

LethalityJane. 2022. "It's Pretty Much Common Knowledge in a Lot of Technical Military MOS's That a Bunch of Our Peers Have Undiagnosed ADHD or Autism." Twitter (postagem de usuário), 23 de junho de 2022. https://twitter.com/LethalityJane/status/1540119983849558016.

Lombardi, Maria Rosa, Cristina Bruschini e Cristiano M. Mercado. 2009. "As Mulheres nas Forças Armadas Brasileiras: A Marinha do Brasil." *Textos FCC* 30.

Martins, Fran. 2022. "Entre 5% e 8% da população mundial apresenta Transtorno de Déficit de Atenção com Hiperatividade." Ministério da Saúde. https://www.gov.br/saude/pt-br/assuntos/noticias/2022/setembro/entre-5-e-8-da-populacao-mundial-apresenta-transtorno-de-deficit-de-atencao-com-hiperatividade.

Miranda, Danilo. "Recebi hoje esse belo currículo!" LinkedIn (postagem de usuário). https://www.linkedin.com/feed/update/urn:li:activity:7165301119810834433/.

Nobre, Anna Christina, e Freek Van Ede. 2020. "Under the mind's hood: what we have learned by watching the brain at work." *Journal of Neuroscience* 40 (1): 89-100. https://doi.org/10.1523/JNEUROSCI.0742-19.2019.

Reino Unido. 2024. "The UK Intelligence Community Design System (ICDS)." Version 2.21.0. Secret Intelligence Service (SIS). https://design.sis.gov.uk/accessibility/needs/neurodiversity.

Rodrigues, Larissa e Leonardo Ribeiro. 2023. "Defesa quer criar carreira própria para diminuir dependência de militares na estrutura do ministério." CNN Brasil, 12 de abril de 2023.

Sadzinski Junior, Anastácio, Sheila Wayszceyk e Andrea Soares Wuo. 2021. "Neurodiversidade: levantamento das produções nacionais." *Revista Humanitaris* 2 (2): 156-166.

Salgado, Nathalia, Jessica Pantoja, Rafael Viana e Rodrigo Varotti Pereira. 2022. "Transtorno do espectro autista em crianças: uma revisão sistemática sobre o aumento da incidência e diagnóstico." *Research, Society and Development* 11 (13): e512111335748. http://dx.doi.org/10.33448/rsd-v11i13.35748.

Stochero, Tahiane. 2013. "Justiça manda Exército reconhecer companheiro de sargento gay." G1, 8 de agosto de 2013. https://g1.globo.com/pernambuco/noticia/2013/08/justica-manda-exercito-reconhecer-companheiro-de-sargento-gay.html.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.260
ISSN 2595-4717

Vlad, Alexandru Robert e Andreea Ioana Lungu. 2017. "Can a person with attention deficit hyperactivity disorder be an athlete?" *Acta Marisiensis-Seria Medica* 63 (3): 110-114. https://doi.org/10.1515/amma-2017-0030.

Weinbaum, Cortney, Omair Khan, Teresa D. Thomas e Bradley D. Stein. 2023. *Neurodiversity and National Security: How to Tackle National Security Challenges with a Wider Range of Cognitive Talents*. RAND Corporation, RR-A1875-1. https://www.rand.org/pubs/research_reports/RRA1875-1.html.

WildAlaskanRed. 2022. "Add to That My Ability to Hyper-Focus. EOD Is the Perfect Job for Someone with ADHD." Twitter (postagem de usuário), 24 de junho de 2022. https://twitter.com/WildAlaskanRed/status/1540431593138839552.

Xu, Guifeng, Lane Strathearn, Buyun Liu, Binrang Yang e Wei Bao. 2018. "Twenty-year trends in diagnosed attention-deficit/hyperactivity disorder among US children and adolescents, 1997–2016." *JAMA Network Open* 1 (4): e181471. https://doi.org/10.1001/jamanetworkopen.2018.1471.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Artigo de pesquisa

José Fernando Moraes Chuy[1]
ORCiD https://orcid.org/0000-0003-3831-9300

A INADEQUAÇÃO DA ESTRATÉGIA DA DETERRENCE DIANTE DA RADICALIZAÇÃO VIRTUAL TERRORISTA

https://doi.org/10.58960/rbi.2025.20.262

Chuy, José Fernando Moraes. 2025. "A inadequação da estratégia da *deterrence* diante da radicalização virtual terrorista." *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.262. https://doi.org/10.58960/rbi.2025.20.262.

Recebido em 05/12/2024
Aprovado em 27/05/2025
Publicado em 18/06/2025

1 Delegado de Polícia Federal. Doutor em Direito e Segurança pela Universidade Nova de Lisboa; Mestre em Ciências Policiais (com especialização em Criminologia e Investigação Criminal) pelo Instituto Superior de Ciências Policiais de Portugal; Especialista em Ciências Penais pela Universidade do Sul de Santa Catarina. Professor do Programa de Pós-Graduação da Academia Nacional de Polícia, onde é Coordenador do grupo de pesquisa Rede de Pesquisa em Terrorismo.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

A INADEQUAÇÃO DA ESTRATÉGIA DA DETERRENCE DIANTE DA RADICALIZAÇÃO VIRTUAL TERRORISTA

Resumo

A temática do terrorismo é catalizadora do sentimento de insegurança na sociedade global e de risco, demandando profunda reciclagem dos sistemas estatais, especialmente nas áreas da segurança e da inteligência. O artigo aborda o atual cenário de radicalização virtual terrorista e busca avaliar a possibilidade de seu enfrentamento através da aplicação de uma histórica e clássica estratégia. Largamente utilizada ao longo da Guerra Fria, a deterrence (dissuasão) permanece com alcance em face de determinadas ameaças contemporâneas, especialmente no campo militar. Explorando a base conceitual e as características da deterrence, o artigo acaba por concluir pela sua inaplicabilidade no aspecto de prevenção da radicalização de indivíduos com propensão ao fanatismo e ao encantamento do terror propagado pelas redes sociais.

Palavras-chave: terrorismo, dissuasão, radicalização, redes sociais, Inteligência.

THE INADEQUACY OF THE DETERRENCE STRATEGY IN THE FACE OF VIRTUAL TERRORIST RADICALIZATION

Abstract

The theme of terrorism is a catalyst for the feeling of insecurity in global society and risk, requiring a profound recycling of State systems, especially in the areas of security and intelligence. The article addresses the current scenario of virtual terrorist radicalization and seeks to evaluate the possibility of confronting it through the application of a historical and classic strategy. Widely used throughout the Cold War, deterrence remains with a large scope, in the face of certain contemporary threats, especially in the military field. Exploring the conceptual basis and characteristics of deterrence, the article concludes that it is not applicable in the aspect of preventing the radicalization of individuals with a propensity for fanaticism and enchantment caused by the terror propagated by social networks.

Keywords*: terrorism, deterrence, radicalization, social networks, Intelligence.*

LA INSUFICIENCIA DE LA ESTRATEGIA DE DETERRENCE ANTE LA RADICALIZACIÓN VIRTUAL TERRORISTA

Resumen

La temática del terrorismo es catalizadora del sentimiento de inseguridad en la sociedad global y de riesgo, demandando un profundo reciclaje de los sistemas estatales, especialmente en las áreas de la seguridad y la inteligencia. El artículo aborda el actual escenario de radicalización virtual terrorista y busca evaluar la posibilidad de su enfrentamiento a través de la aplicación de una histórica y clásica estrategia. Ampliamente utilizada a lo largo de la Guerra Fría, la deterrence (disuasión) permanece con alcance frente a determinadas amenazas contemporáneas, especialmente en el campo militar. Explorando la base conceptual y las características de la deterrence, el artículo concluye que esa no es aplicable en el aspecto de prevención de la radicalización de individuos con propensión al fanatismo y al encantamiento causados por el terror propagado por las redes sociales.

Palabras clave*: terrorismo, disuasión, radicalización, redes sociales, Inteligencia.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Introdução

Conforme Beck (2015, 70), os riscos não devem ser tratados como fatalidades decorrentes de fatores externos. Os riscos são decorrentes da ação humana e de seus respectivos resultados destrutivos, em tempo e lugar distantes de onde a ação incialmente se desenvolveu. Tal circunstância, agravada pelo fenômeno da globalização, desencadeia o surgimento da "teoria da sociedade de risco mundial", quando a segurança passa a ser priorizada em todos os aspectos da vida social. Pois exatamente na atual sociedade de risco mundial, a temática do terrorismo é catalizadora do sentimento de insegurança em termos globais.

O combate militar ao fenômeno resultou na formação de uma segunda geração de terroristas, fortalecendo a ideologia extremista das organizações, especialmente no espaço virtual (Crenshaw 2010, 44-45). O caráter comunicacional pulverizado na internet pelas organizações terroristas se apresenta como perigoso risco, na medida em que resulta na efetivação de recrutamentos e em processos de radicalização (Chuy 2018).

A radicalização virtual é realidade global que atinge inclusive países sem aparente relação com o terrorismo (Queiroz 2013, 75). Em um contexto de terrorismo disseminado em redes sociais, uma moderna prestação social protetiva estatal se mostra necessária, demandando o prévio estudo de estratégias e, ainda uma profunda reciclagem da forma de atuar das forças de segurança e dos serviços de inteligência.

Alternativas de enfrentamento, antes de colocadas em prática de forma açodada, devem ser devidamente pesquisadas, avaliadas e calibradas, dando posterior subsídio à atuação dos órgãos estatais. É exatamente esse o objetivo deste artigo, que busca avaliar academicamente uma alternativa diante de um terrorismo espraiado, que se vale de todas as vantagens tecnológicas do processo de globalização para a propagação e publicidade de ideologias.

O artigo parte de estratégia largamente utilizada ao longo da Guerra Fria. A *deterrence* pontuou as atividades estatais, tendo significativa influência para a paz mundial, com notada importância no Direito Internacional e nos organismos de inteligência (Correia 2018). Perfeitamente abordada por Schelling (2008; 2011), tal estratégia foi inovadora no âmbito das relações internacionais, dos estudos estratégicos e ainda no processo de tomada de decisões, sendo sintetizada pelo recurso à coerção por via diplomática justamente para evitar o conflito ("diplomacia da violência"). Para o notável autor, agraciado em

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

2005 com o Prêmio de Ciências Econômicas em Memória de Alfred Nobel, os verdadeiros protagonistas de um evento conflitivo comportar-se-iam a partir de um denominador comum de racionalidade diante de ameaças plausíveis.

A *deterrence* teria aplicabilidade em face do terrorismo? Seria possível as forças de segurança e de inteligência aplicarem a teoria em face de organizações não estatais envolvidas com o terrorismo internacional, que muitas vezes não possuem bens vulneráveis, tampouco um regime a ser confrontado? Ancorado nos ensinamentos de Schelling, buscou-se analisar a possibilidade de adaptar a *deterrence* no âmbito contemporâneo da segurança e da inteligência e utilizá-la no enfrentamento preventivo ao "encantamento do terror" propagado na internet.

Dentro de uma abordagem multidisciplinar, o artigo percorre um trilho exploratório de conceitos estratégicos relacionados à deterrence, conjugado com a análise da evolução da temática terrorista. É apresentado um exame bibliográfico com entendimentos e referências doutrinárias com posicionamentos bastante distintos (e conflitantes) acerca da aplicabilidade da deterrence em relação ao campo de estudo ainda lacunoso da radicalização virtual.

A partir da interação entre os conteúdos coletados, por meio de uma construção argumentativa a parte final do artigo apresenta uma série de fundamentos que, a nosso ver, evidenciam que a dissuasão, apesar de seu riquíssimo e exitoso legado, não demonstra aplicabilidade no aspecto de prevenção de segmentos com propensão ao fanatismo e ao "encantamento do terror" propagado pelas redes sociais.

A radicalização, as redes sociais e a transnacionalização do terrorismo

A radicalização decorre de um processo que acaba por transformar psicologicamente um determinado segmento, fazendo com que pessoas ou grupos se distanciem de antigas práticas, passando a apoiar ideologias sociais, políticas e religiosas extremas. A radicalização não constitui prática criminosa, a não ser quando se torna violenta (El-Said 2015, 9).

Pois a radicalização terrorista é justamente o processo que conduz uma pessoa a aceitar atos violentos como se legítimos fossem (OSCE 2014, 19). Daí deriva a radicalização virtual terrorista, que apresenta características bastante perigosas:

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

> [r]adicalizing and recruiting online has great advantages over the traditional (and riskier) public communications. Terrorist groups can reach out to an incalculably vast audience. With no travel required, cost is minimal, no logistics or transportation support is needed, and the odds of detection are low. And the newly radicalized need not necessarily pack up and head for the Middle East—jihadi groups encourage attacks at home to avoid the risk of infiltration while traveling.
>
> The threshold for engaging in cyber jihad is markedly lower than for someone who gives up a familiar, comfortable life to travel to an actual battle zone and risk death or capture. If the notion of online activism as a proper, respectable, and sufficient form of jihad wins wide acceptance within radical circles, we can expect ever-increasing efforts in online propaganda and cyber attacks. This could further inspire yet more individuals, facilitating both radicalization and recruitment, and lead to a new cycle of attacks (Alarid 2016, 320-321).

Demant (2010) refere um terrorismo cada vez mais transnacional, com a veiculação de eventos facilitada pelas comunicações instantâneas que acabam por promover a adesão de integrantes vulneráveis (em sua maioria jovens) a uma ideologia radical.

A Al-Qaeda deu início à transnacionalização do terrorismo através do alargamento de ataques externos a regiões de conflito e do aproveitamento das inovações tecnológicas. Importante notar que desde a década de 1980 os jihadistas já produziam programas de debate em estilo televisivo, revistas a cores, palestras em cassetes. Lançado em 2001, o vídeo "The State of the Ummah" trazia propaganda da Al-Qaeda "requintadamente produzida", tendo definido o grupo para os meios de comunicação ocidentais. O vídeo apresentava claro incitamento ideológico, servindo como recrutamento e ainda como suporte para apologistas (Stern e Berger 2015, 129-130).

Após a Al-Qaeda, o Estado Islâmico (ISIS) soube perceber os proveitos da globalização, utilizando novos recursos de comunicação disponibilizados pela rede mundial de computadores (Chuy 2021). Por meio de técnicas altamente profissionais e com robusto volume de publicações, no intuito de inundar as redes sociais, a organização adaptou e desenvolveu uma série de narrativas com viés de propaganda adaptada a cada tipo de público-alvo (Fonseca e Lasmar 2017, 178). Percebendo que a violência atrai e gera propaganda revertida em recrutamentos, o Estado Islâmico passou a se utilizar de cenas brutais editadas em filmes modernos, promovendo alargada divulgação (McCants 2016, 42-43).

Conhecido como "gestão da selvageria" (the management of savagery), a estratégia do ISIS, por intermédio de poderosa mistura de "carnificina chocante" com ideais utópicos, alcançou vasta audiência global, resultando em

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

manipulação e recrutamento (Stern e Berger 2015, 25; 144).

O ISIS foi eficiente em observar a utilidade do uso das redes sociais e de videogames para efetivar a radicalização de número gigantesco de pessoas, das mais variadas regiões e continentes, obtendo vasto quadro de recrutas (Alarid 2016). De forma impressionante o grupo otimizou a utilização de novas tecnologias e de mídias sociais, desencadeando verdadeira "terceirização midiática", fazendo com que inclusive indivíduos externos à organização disseminassem suas manifestações oficiais (crowdsourcing) (Barrett 2014).

Napoleoni observa que "o crescente número de seguidores ao redor do mundo, pessoas induzidas a abraçar a prática da violência pela propaganda do Estado Islâmico, confirma o caráter fascinador global da sua mensagem" (Napoleoni 2015, 71). A estratégia do ISIS conseguiu atrair milhares de "recrutas" de todas partes do mundo, que queriam "se juntar à batalha antes do apocalipse final" (Beck 2015, 21-27).

O terror hodierno se vale de antigas práticas, combinando estas com avançada tecnologia da informação e de comunicação do mundo global e informatizado, mistura que além de permitir a obtenção de recursos e a coordenação dos grupos operativos, acaba por desenvolver a difusão de propaganda política e o recrutamento de voluntários (Fraga Iribarne 2004, 179). Usada para uma segura comunicação pelas organizações terroristas, a internet tem grande valia para espalhar mensagens, disseminar propaganda e chamar outros para a ação (Berntsen 2008, 52-53).

A popularização das redes sociais é sobremaneira útil para as organizações terroristas que passaram a personalizar sua mensagem para específicos nichos de audiência, operacionalizando a radicalização "online" de pessoas com pouco conhecimento dos aspectos religiosos ou ideologicos dos grupos (Weimann, 2014).

Além de espalhar o medo e o terror nos inimigos, o material compartilhado nas redes sociais resulta em robusta fonte de marketing, operando proselitismos entre possíveis seguidores (Napoleoni 2015, 70). O universo globalizado favorece a fluidez e a velocidade da informação, que instantaneamente é transmitida e recebida. Nesse contexto, as práticas do terror chegam imediatamente à sociedade, centralizando a atenção do público (Callegari 2016, 16; 23).

A internet se transformou na plataforma ideal para transmissão da mensagem para uma ampla audiência. Além dos extremistas religiosos, organizações

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

separatistas, nacionalistas, racistas e outras se aproveitam do fácil acesso à rede mundial de computadores, além de seu custo ínfimo e da sua insuficiente e falha regulação (Carvalho 2016, 34-35). Dessa forma, a

> mutação dos efeitos da propaganda clássica causada pelas atrocidades itinerantes de organizações armadas representa uma ameaça sem igual para os países ocidentais. Assim como os improvisados homens-bomba dos primeiros anos de 2000, os degoladores alfabetizados pelas cartilhas virtuais do faça-o-mal-você-mesmo dos dias atuais são difíceis de identificar e localizar, pois não pertencem a nenhum grupo terrorista consagrado, de vida relativamente longa, e sua radicalização nasceu da gestação de apenas alguns cliques do mouse (Napoleoni 2015, 71).

Valendo-se das ''benesses'' tecnológicas, os atos de terror contemporâneo apresentam robusto escopo de danos e baixo custo para as organizações que muitas vezes simplificam processos buscando dificultar a detecção pelas forças policiais (Ramos 2009, 27-37).

A disseminação de ações extremistas e de ideologias de radicalização violenta por meio da internet e das redes sociais tem resultado em discussões da comunidade internacional no que tange exatamente à sua correta interpretação e aplicação (Koschade 2006).

Globalização do terrorismo e seu ineficiente enfrentamento militar

Em 1976, Laqueur já afirmava que os meios de comunicação seriam os melhores amigos dos terroristas e que o ato terrorista em si nada seria sem o apoio da publicidade (Laqueur 1976, 99-104).

Iñigo Alvarez (2016) constata uma evolução do fenômeno terrorista, que passa a ser globalizado. Hodiernamente a internet acaba por fornecer as ferramentas para a referida globalização do terror, permitindo que indivíduos baseados em qualquer local do planeta acessem sites de grupos radicais, assistam propagandas e se comuniquem com esses grupos (Richardson 2006, 134).

Com a ''revolução tecnológica terrorista'', passa a ser notada a participação de novos personagens, de perfil mais impulsivo. Com notado desconhecimento das demandas das organizações, esses novos atores são muito menos ideológicos, passando a agir sem conexão direta com as lideranças (Chuy 2018).

Atos de ''*home-grown*'' são executados por sujeitos autorradicalizados pelas redes sociais, muitas das vezes sem o conhecimento dos grupos. A alteração do perfil terrorista é representada pelo maior envolvimento de jovens, de mulheres e ainda de atores estrangeiros (*foreign fighters*) em ações solitárias

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

(Crenshaw e Lafree 2017, 74).

Percebendo que a radicalização deve ser encarada como um processo e não como um fenômeno isolado, Ares observa a tendência de perpetração de atentados por indivíduos nacionais autorradicalizados sem ligação direta com grupos terroristas exteriores, simplesmente ''inspirados'' pela propaganda ideológica de radicalização (Ares 2015). Tomé nota um ''número impressionante de 'jihadistas express' mais ou menos autorradicalizados nascidos e criados no Ocidente'' (Tomé 2015).

Carvalho (2016, 52) observa a incapacidade das sociedades de enfrentar a ''globalização do terrorismo''. As tradicionais estratégias de ''combate militar'' insistemente executadas não se mostram efetivas no que tange à continuidade das organizações e de seus nefastos atos. Nesse sentido,

> não se pode dizer que a ''guerra contra o terrorismo'' é uma guerra dentro dos padrões históricos e conceituais. Não há nenhum inimigo a conquistar, nenhuma terra a capturar, nenhuma maneira de saber quando a guerra foi ganha ou não, ou muito menos se haverá ou não uma negociação ou um acordo de paz que colocará fim ao conflito (Nasser 2021, 15).

Como observado por Crenshaw, a Guerra ao Terror trouxe como marca a rejeição do terrorismo como crime, promovendo recurso excessivo à força militar. Tal contexto, além de não produzir democracia nem estabilidade, acabou por desencadear a formação de uma segunda geração de líderes terroristas e provocar ''mais terrorismo''. Como já referido, a superada estratégia ''de guerra'', acabou por fortalecer a ideologia extremista das organizações, permitindo a utilização do espaço virtual para radicalização e recrutamento de novos agentes (Crenshaw 2010, 44-45).

Guerra Fria e dissuasão

Interessante destacar que a tradução de *deterrence* para a língua portuguesa corresponde a ''dissuasão'', tradução esta que, a nosso ver, causa significativa confusão de ordem semântica, na medida em que a palavra ''dissuasão'' tem um alcance bastante abrangente.

Cabe referir que não estamos a tratar da dissuasão no âmbito do desenvolvimento das teorias de punição criminal (*criminal deterrence teory*). A esse respeito, embora nos ajudem a compreender o significado da palavra deterrence, trabalhos antológicos de filósofos como Hugo Grotius, Thomas Hobbes, John Locke, dentre outros, são clássicos sob o prisma da teoria psicológica e sociológica.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Derivado do latim (“*deterre*”), “*deterrence*” é assim definido no Penguin Dictionary of International Relations:

> [d]eterrence is a conditional commitment to retaliate, or to exact retribution if another party fails to behave in a desired, compliant manner. [...] [It] concentrates exclusively on negative sanctions, or threats, and upon preventing undesirable behavior (Evans e Newnham 1998, 126-127).

Caracteriza-se como um processo de influenciar as escolhas de uma parte adversa e influenciar essa mesma parte em relação ao que se espera de nosso comportamento. Portanto, não se trata de uma teoria de aplicação de violência, de agressão e nem de guerra. Limita-se, pois, a influenciar outra parte para que acredite que o nosso comportamento (chamado de comportamento estratégico) dependerá exatamente do seu comportamento (Schelling 2011, 16). A *deterrence* busca influir no processo decisório de terceiros, persuadindo-os no sentido de não adotarem determinada ação (Gray 2003, 32). A teoria tem sua lógica baseada em persuadir uma parte (um alvo), demonstrando que os custos de uma determinada ação superam os possíveis benefícios que esta ação pode proporcionar (Wilner 2011).

A configuração da *deterrence* requer um conflito e um interesse comum entre as partes envolvidas, não tendo aplicabilidade em casos de puro e completo antagonismo de interesses (Schelling 2011, 16). Schelling defendia o recurso à coerção pela via diplomática justamente para evitar o conflito (“diplomacia da violência”), fazendo com que uma parte optasse por uma ação contrária à sua vontade, em razão da ameaça de uso da força (*armed suasion*). Assim, os verdadeiros protagonistas de um evento conflitivo comportar-se-iam a partir de um denominador comum de racionalidade diante de ameaças plausíveis (Correia 2018). Portanto, os dissuadidos devem ser capazes de tomar decisões racionais. A racionalidade da parte adversa é pertinente à ameaça desenvolvida, razão pela qual a deterrence não teria aplicabilidade frente a pessoas transtornadas ou menores de idade (Schelling 2011, 16).

Para que a deterrence funcione, a parte “dissuasora” deve fazer uma ameaça contra algo valioso para os dissuadidos, caso contrário, a ameaça não terá sentido. Nos confrontos tradicionais entre Estados, esse critério pode ser mais ou menos facilmente satisfeito (Wagner 2004). A estratégia se apresenta como uma “variável relacional”, um produto de determinada relação (ou relacionamento), razão pela qual não pode ser criada ou administrada artificialmente por apenas um personagem (Gray 2000).

A Guerra Fria consistiu em uma “rivalidade entre dois sistemas político-eco-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

nômicos mutuamente excludentes acerca do futuro da sociedade industrial'' (Buzan 1997). A ''Primeira Era Nuclear'' restou marcada pela polarização entre duas superpotências, dentro de um antagonismo econômico que derivava para os campos da indústria armamentista e para a energia atômica (Kajibanga 2016). Largamente manejada ao longo da Guerra Fria, a dissuasão trabalhava a ''persuasão'' dos adversários, de forma que percebessem que os custos de uma possível agressão excederiam os eventuais ganhos, detendo, assim, agressões. Baseada nos princípios da comunicação, da capacidade e da credibilidade e, ainda, na intenção de materializar uma ameaça, de forma a incutir na mente do adversário o receio de um ataque (Correia 2018), ao longo dos mais de 40 anos da Guerra Fria a *deterrence* se caracterizou como elemento fundamental.

Acerca da ''comunicação'', Wagner destaca que canais que possibilitem às partes se comunicar precisam existir. Em relação à ''capacidade'', a dissuasão ''depende do que se pode fazer, não do que se fará'' (Wagner 2004). A ''credibilidade'' é a percepção que o desafiado detém da parte dissuasora, ou seja, conseguir fazer com que o adversário acredite que a ameaça de dissuasão será realizada em caso de não cooperação (Schelling 2011, 16).

Enquanto estratégia de imputação ao adversário do cálculo de custo/benefício de suas ações, a dissuasão foi utilizada de forma robusta durante os anos 1950, tendo a bipolaridade da Guerra Fria sido o momento de maior aplicabilidade, definindo as relações exteriores entre os Estados Unidos e a antiga União Soviética. Por meio da dissuasão foi evitado um conflito militar e nuclear direto entre as duas superpotências.

O fim da Guerra Fria conduziu a um quadro de desequilíbrio internacional e, de certa forma, de declínio da dissuasão. Especialmente nos Estados Unidos, o conceito perdeu aceitação, na medida em que remeteria à questionável estratégia nuclear relacionada à possibilidade real de destruição massiva de toda a humanidade.

Dissuasão e ameaças contemporâneas

Knopf ressalta que após o fim da Guerra Fria emergiu uma nova linha de pesquisas sobre a dissuasão, que ganhou ainda mais volume após o 11 de setembro, sendo classificada pelo autor como a quarta onda na pesquisa da dissuasão . Tal (re)classificação decorre exatamente da circunstância relacionada à mudança de uma situação relativamente simétrica de dissuasão mútua, que caracterizou a Guerra Fria, para as ameaças assimétricas que

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

dominam o ambiente de segurança atual (Knopf 2010).

Knopf sustenta que a dissuasão permanece desempenhando importante papel, muito embora atualmente com menor abrangência. Hodiernamente o autor trata da adoção de um conceito mais amplo de dissuasão, que não seja exclusivamente militar. Knopf destaca que não apenas os veteranos teóricos da dissuasão (Colin Gray, Patrick Morgan, Lawrence Freedman e Robert Jervis), mas toda a literatura que pesquisa a quarta onda está de acordo que a dissuasão continua relevante e potencialmente útil contra ameaças contemporâneas (Knopf 2010).

De fato, Gray refere que a dissuasão permanece absolutamente essencial como elemento da grande estratégia, muito embora apresente acentuada dificuldade de aplicação nas diferentes condições do século XXI (Gray 2003).

Quinlan (2004) explica que os instrumentos militares, enquanto instrumentos para executar destruição física, não são as únicas possibilidades de dissuasão. Instrumentos políticos, econômicos, sociais, judiciais e até religiosos ou similares podem contribuir com o processo.

Embora sejam uma constante histórica, os relacionamentos envolvidos pela *deterrence* não são modelos estáticos e lineares. Suas circunstâncias, detalhes e forma de implementação estão constantemente a mudar. A teoria permaneceria aplicável, mas os estrategistas devem determinar quem deter, como deter, quando e por quê (Gray 2000). Conforme Knopf (2010), não se está a confiar em uma postura dissuasora única, devendo a estratégia ser adaptada a cada caso individual com fulcro em uma compreensão detalhada da parte adversa. Assim, muitas pesquisas passaram a abordar maneiras de obter alguma vantagem com a estratégia.

Dentre as pesquisas, Quinlan (2004) constata que no período hodierno podem ser criadas diferentes e variadas estruturas de *deterrence*, com base mais ampla e eventualmente mais multifacetada do que durante a Guerra Fria (e suas percepções bilaterais concentradas em energia nuclear). O conceito subjacente de *deterrence* permanece válido e relevante. Precisaria ser explorado de forma mais flexível, com uma gama mais ampla de instrumentos, uma relação mais bem calibrada com a natureza de determinados atores e, sempre que possível, uma base mais ampla de legitimidade e apoio internacional.

Ao criticar o que chama de ‘‘estigmatização e centralização da dissuasão no meio militar’’, Hopf (1994, 241) destaca justamente que a teoria deve au-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

mentar seu raio de atuação, buscando identificar vários outros instrumentos de dissuasão.

Dissuasão e terrorismo

A dissuasão teria aplicabilidade em face do terrorismo? A pesquisa identificou posições conflitantes.

Parte da doutrina especializada entende que a dissuasão demanda que os atores envolvidos (ambos) compartilhem algum nível de comprometimento na relação entre "perdas e ganhos." Tal circunstância demanda das partes igualmente uma racionalidade comum. Diante de tal correlação, Suarez (2013, 41-42) sustenta não haver possibilidade de encaixe da teoria da dissuasão em relação às organizações terroristas. Para Knopf, os terroristas são dispostos a cometer suicídio pela causa, estando mais interessados nas recompensas celestiais do que nas terrenas (Knopf 2010).

Em discurso proferido em 2002 na academia militar de West Point, o ex-presidente dos Estados Unidos George W. Bush referiu opinião bastante forte a respeito do declínio da *deterrence* e de sua não aplicação frente ao terrorismo (Bush 2002). Em outra ocasião o antigo mandatário norte-americano foi ainda mais direto, referindo que, diferentemente da URSS, os adversários terroristas escondem-se em cavernas e sombras, não tendo mais fronteiras para proteger ou capital para defender, razão pela qual não poderiam ser dissuadidos (Bush 2006). As organizações não estatais não teriam um "endereço de retorno", um alvo territorial contra o qual ameaças podem ser feitas e cumpridas (Wilner 2011).

Nesse sentido, a Estratégia Nacional de Segurança dos Estados Unidos de 2002 assevera que após o colapso da URSS e o fim da Guerra Fria, o ambiente de segurança passou por profunda transformação e que os conceitos tradicionais de deterrence não se prestariam a enfrentar um inimigo terrorista cuja táticas declaradas consistem em destruir e tomar como alvo pessoas inocentes (EUA 2002).

Importante, no entanto, identificar segmentos da doutrina e da pesquisa com entendimento de que a dissuasão teria aplicabilidade no período contemporâneo, especialmente em relação ao terrorismo.

Nesse aspecto, Wilner nota, após o 11 de setembro, um crescente "ceticismo" acerca da aplicabilidade da dissuasão. Tal desconfiança decorreria primor-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

dialmente da religiosidade fundamentalista, especialmente da Al-Qaeda, que acaba por negar qualquer tomada de decisão racional. Além disso, este fanatismo faz eclodir contextualizações divergentes e uma tendência para aceitação de riscos, por meio de comportamento maximalista e resoluto. Assim, um indivíduo que idealiza uma vida esplêndida após a morte não temeria retaliação nem punição. Contudo, Wilner (2011) critica o ceticismo relacionado à dissuasão, referindo que tal ceticismo é baseado no "instinto", sendo desprovido de uma argumentação teórica rigorosa e tão somente representa artigos de opinião, em vez de avaliações obstinadas.

Ao referir que a dissuasão é provavelmente tão antiga quanto o próprio conflito, Wagner (2004) pondera que a estratégia poderia ter aplicabilidade em um confronto não tradicional entre um Estado e um oponente abstrato, como o terrorismo. Em contexto diferente do da Guerra Fria, a principal dificuldade seria executar a ação apropriada na medida em que a *deterrence* contemporânea deveria ser dirigida a um alvo assimétrico, na maioria das vezes um ator não-estatal. O autor conclui que, embora possa ser possível impedir ações terroristas individuais, o próprio terrorismo não pode ser dissuadido por meios exclusivamente militares, como referido na retórica usada na guerra contra o terrorismo. Assim, a *deterrence* teria uma aplicação bastante ampla, sendo o enfrentamento do terrorismo uma delas. Entretanto, a sua aplicabilidade ao terrorismo necessitaria de ajustes, pois uma ameaça de dissuasão só pode ser feita contra algo que a pessoa a ser dissuadida preza, o que se torna bastante complexo diante de terroristas preparados para o sacrifício pessoal (Wagner 2004).

Puchades Navarro (2011), comentando a nova teoria econômica do crime, nota que a grande maioria dos delinquentes, excetuado um número limitado de psicopatas, reagem de forma racional e previsível a estímulos e incentivos materiais (rendimentos). Da mesma forma, racionalizam as consequências dos seus atos e da probabilidade de punição. A partir dessa constatação, o autor pontua que ao terrorismo, enquanto atividade criminosa, devem ser aplicados os modelos econômicos de crime com adaptações. Considerando que os atores do terror respondem racionalmente à análise dos custos e benefícios de suas atividades, eles podem ser dissuadidos por meio de ações que diminuam os benefícios esperados de suas ações.

Nesse aspecto, Trager e Zagorcheva (2005) referem que além da parte adversária ter necessariamente que compreender a ameaça (implícita ou explícita), a sua tomada de decisão deve ser suficientemente influenciada justamente por cálculos de custos e benefícios.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Knopf (2010) entende que a dissuasão continua viável e relevante, especialmente no trato com o terrorismo contemporâneo. Assim, uma dissuasão unidirecional ganharia força no contexto internacional hodierno, na medida em que as potências, especialmente os Estados Unidos, esperam deter organizações terroristas, sem que esses atores não estatais modernos sejam capazes de também dissuadir tais potências. Consequentemente, o grande desafio vivenciado nos dias atuais é o de evitar a dissuasão mútua, tentando dissuadir os outros atores para que não lancem ataques e, principalmente, não adquiram capacidades como armas nucleares que poderiam ser usadas para dissuadir os atores estatais. E nesse aspecto, a assimetria contemporânea se apresentaria vantajosa às entidades estatais pois permitiria um critério menos exigente para medir o valor da dissuasão (diferentemente do período da Guerra Fria em que a dissuasão nunca poderia falhar, pois o seu fracasso poderia significar a aniquilação nuclear mútua). Assim, face às ameaças contemporâneas, seria percebida a aplicabilidade positiva da dissuasão marginalmente para a redução do número de ataques.

Wilner (2011) afirma que uma compreensão mais robusta do terrorismo, acompanhada de apreciação mais matizada da lógica em que se baseia a teoria da dissuasão, evidencia que uma variedade de medidas dissuasivas pode ser aplicada frente às organizações terroristas, exigindo significativa expansão do escopo da teoria, que supere o foco no aspecto da punição e do armamento nuclear. Seria necessária uma adaptação estatal com o escopo de fazer uso da dissuasão para influenciar o comportamento de grupos terroristas. O autor reconhece que dissuadir terroristas é mais complexo que dissuadir adversários estatais, constatando, entretanto, que ambos os processos compartilham uma mesma lógica: a manipulação do comportamento de um adversário por meio de alavancagens coercitivas, diplomáticas ou ideológicas contra seus ativos, objetivos e crenças. No sentido, Davies e Jenkins afirmam que

> [i]t is a mistake to think of influencing al Qaeda as though it were a single entity; rather, the targets of US influence are the many elements of the al Qaeda system, which comprises leaders, lieutenants, financiers, logisticians and other facilitators, foot soldiers, recruiters, supporting population segments, and religious or otherwise ideological figures. A particular leader may not be easily deterrable, but other elements of the system (e.g., state supporters or wealthy financiers living the good life while supporting al Qaeda in the shadows) may be (Davis e Jenkins 2002).

Cumpre observar que muitas das abordagens propostas para a dissuasão são de natureza indireta (dissuasão indireta), destinadas a pressionar terceiros que facilitam o terrorismo, ao invés dos próprios terroristas (Davis e Jenkins 2002). Esse tipo de dissuasão volta-se a terceiros cujas ações podem afetar a ação a ser desencadeada por uma organização. Seria uma forma preventiva

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

que não acaba por dissuadir diretamente os agentes terroristas, mas setores de assessoramento e apoio de grupos.

A predileção dos Estados ocidentais no que tange a uma resposta repressiva ao terrorismo baseada na força, por meio da justiça criminal ou através do engajamento militar, denota a dominação de um modelo de dissuasão, em muito lastreado na negação ou na punição. A dissuasão por negação, conforme Snyder (1961), é relacionada à tentativa de convencimento acerca da disposição estatal de não aceitar concessões e, assim, desencorajar potenciais agentes terroristas, diminuindo suas chances de sucesso ou convencendo-os a perseguir seus objetivos políticos de outra maneira. A dissuasão por punição ocorreria quando o Estado pune o ator não estatal caso uma ação não desejada seja realizada, tornando o custo de cometer um ataque muito superior aos benefícios do ataque.

Dissuasão e radicalização virtual terrorista

Como alhures abordado, a *deterrence* é concebida justamente no aspecto de exploração do potencial de força, de maneira a persuadir uma parte adversa (potencial inimigo) a evitar certas ações (Schelling 2011, 9).

Concordamos com Gray (2010) no sentido de ser mais difícil ter sucesso com uma estratégia de *deterrence* hoje do que na Guerra Fria. Em praticamente todas as circunstâncias contemporâneas, não se pode mais impedir algo ameaçando simplesmente infligir danos sociais maciços. No período contemporâneo assimétrico resta alterado o conceito de dissuasão, especialmente em relação ao terrorismo, fenômeno que tem um adversário com ideologias agressivas, altamente destrutivo e sem base territorial (Proença Garcia 2010).

Para Quinlan (2004), a dissuasão não exige que especifiquemos precisamente qual a forma que a nossa não-aceitação assumirá, necessitando apenas que deixemos claro que a ação censurável não será permitida e que temos o poder de impedi-lo com os meios à nossa disposição, sendo que o meio escolhido será o que acharmos necessário para o propósito.

Ousamos discordar. Dentro de uma tradução interpretativa, a dissuasão seria um compromisso condicional de retaliar, ou ainda uma retribuição específica destinada a uma outra parte diante de um comportamento indesejado. Concentra-se, exclusivamente, em sanções negativas (ou ameaças) e na prevenção de comportamentos indesejáveis. Assim, nos parece impossível aplicar a estratégia em face de organizações não estatais envolvidas em terrorismo

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

internacional, que na maioria das vezes não possuem bens vulneráveis.

Wilner (2011) sustenta que os terroristas possuem outros valores que podem ser ameaçados e, assim, quando identificadas maneiras menos tradicionais de dissuasão, distintas de estratégias baseadas em punições, estas poderiam ser aplicadas para coagir terroristas.

Ocorre que isso exige diferenciar os atores associados e as suas funções. Em uma análise das organizações terroristas, partimos daqueles que decidem a estratégia e tomam decisões no tocante à infraestrutura de apoio. Temos ainda os operadores de nível médio, no caso os soldados e o grupo que atua na rede de apoio. Ainda existem os facilitadores e financiadores. Cada um dos atores pode ter concepções diferentes do fenômeno, da organização e dos atos a serem deflagrados. Assim, teremos opiniões diferentes "sobre oferecer a própria vida por uma causa superior e poder tomar uma decisão mais ou menos racional antes de agir", o que afeta a eficácia potencial das medidas de dissuasão (Ginkel 2015).

É bem verdade que algumas interpretações acerca do terrorismo referem que o fenômeno na verdade é "manejado" por "fanáticos racionais" (Sprinzak 2000). Entretanto, diferentemente dos líderes dos grupos terroristas que "manejam" as organizações, os indivíduos que são radicalizados virtualmente e que entregam suas vidas em ataques suicidas são irracionais.

Conforme Gray (2010), uma estratégia bem-sucedida de *deterrence* necessita que o inimigo coopere e, de certa forma, opte por ser objeto dela. A configuração da dissuasão requer um conflito e um interesse comum entre as partes envolvidas, não tendo aplicabilidade em casos de puro e completo antagonismo de interesses. Seguindo os ensinamentos de Schelling, a *deterrence* envolve resultados mutuamente vantajosos para as partes envolvidas, já que grande parte dos conflitos passa por situações de barganha (Schelling 2011, 16).

Não é esse o perfil do indivíduo radicalizado virtualmente. O fanatismo irracional não permite o desenvolvimento da dissuasão, na medida em que esses indivíduos, não tendo discernimento da razão, não possuem condições de cooperar. O fanatismo desencadeia tendência de aceitação de riscos a partir de contextualizações divergentes, nas quais o "protagonista" atua sem racionalidade. Como não há interesse em negociar, esse indivíduo encontra-se em completo antagonismo de interesses em relação ao Estado. Além disso, os indivíduos autorradicalizados frequentemente têm baixo conhecimento da ideologia da organização terrorista (Napoleoni 2015, 71) e suas ações

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

costumar estar dissociadas da estrutura das organizações, as quais muitas vezes sequer têm conhecimento prévio da ação desencadeada.

Considerações finais

O terrorismo global se transformou em um dos principais catalizadores do sentimento de insegurança social. O recrudescimento do terror passa inexoravelmente pelo processo de radicalização de indivíduos, operacionalizado por organizações terroristas através das redes sociais. Tais organizações têm se valido de todas as vantagens tecnológicas do processo de globalização para fins de propagação e publicidade de ideologias extremistas.

Estratégias tradicionais de "combate militar" ao terrorismo, reiteradamente aplicadas para neutralização e prisão de agentes terroristas e de sujeitos radicalizados, não se mostram efetivas. Ao revés, fortalecem a ideologia extremista das organizações e, consequentemente, o recrutamento e a radicalização de novos agentes, especialmente no espaço virtual.

Não mais se pode buscar um enfrentamento ao terrorismo a partir de estratégias belicosas e retributivas que a história demonstra terem sido, além de inócuas, propulsoras do fenômeno. O terrorismo deve ser enfrentado como fenômeno criminal, devendo haver uma efetiva atuação integrada das instituições de segurança, dos órgãos de inteligência e do sistema de justiça.

O enfrentamento moderno ao terrorismo, em um período de globalização e de verdadeira revolução na seara da tecnologia da informação, deve se basear em lógicas preventivas e integradas, exigindo a reavaliação de cenários e de atores. Segurança, inteligência e estratégia, na atual ordem mundial, são temáticas indissociáveis, que demandam prévio e acurado estudo acadêmico, para a posterior implementação de políticas públicas eficientes.

Foi nesse contexto que esta pesquisa se propôs a investigar a aplicabilidade da *deterrence* frente à radicalização virtual de caráter terrorista. Marcante ao longo da Guerra Fria, a estratégia era lastreada nos princípios da capacidade, da credibilidade e da comunicação, e notabilizou-se por materializar uma ameaça, de forma a incutir na mente do adversário o receio de um ataque. Contemporaneamente, a *deterrrence* permanece tendo alcance estratégico contra algumas ameaças. Porém, referido alcance, a nosso ver, resta restrito à área militar, que, como abordado, não é o campo adequado para o moderno enfrentamento ao terrorismo.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Ademais, a natureza dos atores envolvidos na radicalização virtual — muitas vezes irracionais, fanáticos e dispostos ao sacrifício — inviabiliza a lógica da dissuasão, que pressupõe um cálculo racional de custos (perdas e ganhos) por parte do adversário. Além disso, a dissuasão requer a existência de um bem valorizado que possa ser ameaçado, o que não se aplica aos objetivos absolutistas e destrutivos perseguidos pelos agentes terroristas.

Estado e agentes terroristas radicalizados por meio das redes sociais possuem interesses totalmente antagônicos, não havendo o que ser barganhado entre estes, na medida em que buscam resultados distintos: paz ou terror.

Conclui-se, portanto, que, apesar de seu legado histórico, a teoria da dissuasão não se mostra aplicável como estratégia de prevenção à radicalização terrorista promovida no ambiente virtual. Novos paradigmas de enfrentamento, alinhados à realidade das ameaças assimétricas e à complexidade da radicalização virtual, devem ser desenvolvidos e incorporados às políticas de segurança internacional.

Agradecimentos

Este artigo resulta da adaptação de trabalho científico apresentado em provas públicas de Doutoramento em Direito e Segurança na Faculdade de Direito da Universidade Nova de Lisboa em outubro de 2023. O Curso teve apoio da Polícia Federal, no âmbito do Programa de Capacitação (PROCAP), após aprovação em concurso do Comitê Gestor de Capacitação.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Referências

Alarid, Maeghin. 2016. "Recruitment and Radicalization: The Role of Social Media and New Technology." In *Impunity: Countering Illicit Power in War and Transition*, editado por Michelle Hughes e Michael Miklaucic Washington. Center for Complex Operations; Peacekeeping and Stability Operations Institute.

Ares, Pedro Miguel Martins. 2015. "Prevenção da radicalização e do extremismo violento." CEDIS Working Papers - Direito, Segurança e Democracia 17. Faculdade de Direito da Universidade Nova de Lisboa. http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_prevenção-da-radicalização-e-do-extremismo-violento.pdf.

Barrett, Richard. 2014. The Islamic State. Nova York: Soufan Group.

Beck, Glenn. 2015. It is about Islam: exposing the truth about ISIS, Al Qaeda, Iran, and the Caliphate. Nova York: Threshold Editions/Mercury Radio Arts.

Beck, Ulrich. 2015. Sociedade de risco mundial: em busca da segurança perdida. Lisboa: Edições 70.

Berntsen, Gary. 2008. Human intelligence, counterterrorism, and national leadership: a practical guide. Washington: Potomac Books.

Bush, George W. 2002. "Text of Bush's Speech at West Point." New York Times, 1º de junho de 2002. https://www.nytimes.com/2002/06/01/international/text-of-bushs-speech-at-west-point.html.

Bush, George W. 2006. "President Delivers Commencement Address at the United States Military Academy at West Point." News and Policies, The White House/President George W. Bush, 27 de maio de 2006. https://georgewbush-whitehouse.archives.gov/news/releases/2006/05/20060527-1.html.

Buzan, Barry. 1997. "Rethinking security after the Cold War." Cooperation and Conflict 32 (1): 5-28.

Callegari, André Luís, Cláudio Rogério de Souza Lira, Elisangela Melo Reghelin, Manuel Cancio Meliá e Raul Marques Linhares. 2016. O crime de terrorismo: reflexões críticas e comentários à Lei de Terrorismo – de acordo com a Lei nº 13.260/2016. Porto Alegre: Livraria do Advogado Editora.

Carvalho, Hernâni. 2016. Terroristas: como aderem, como nos olham e como agem entre nós. Lisboa: Matéria Prima.

Chuy, José Fernando M. 2018. Operação hashtag: a primeira condenação de terroristas islâmicos na América Latina. Novo Século: São Paulo.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Chuy, José Fernando M. 2021. "Novo Terrorismo? Do fracasso da guerra ao terror à radicalização virtual." Revista Brasileira de Ciências Policiais 12 (5): 145-173. https://periodicos.pf.gov.br/index.php/RBCP/article/view/728/456.

Correia, João Manuel Pinto. 2018. "Deterrence no século XXI: desafios para a estratégia contemporânea." Revista Militar 2599/2600, agosto/setembro. https://www.revistamilitar.pt/artigo/1340.

Crenshaw, Martha. 2010. "O terrorismo visto como um problema de segurança internacional." In Terrorismo & relações internacionais: perspectivas e desafios para o século XXI, editado por Mônica Hertz e Arthur Bernardes do Amaral. Rio de Janeiro: PUC-Rio; Edições Loyola.

Crenshaw, Martha, e Gary Lafree. 2017. Countering Terrorism. Washington: Brookings Institution Press.

Davis, Paul K. e Brian Michael Jenkins. 2002. Deterrence and influence in counterterrorism: a component in the war on al Qaeda. Santa Monica: RAND.

Demant, Peter Robert. "Terrorismo e Globalização: extremização religiosa ou leilão midiático?" In Terrorismo & relações internacionais: perspectivas e desafios para o século XXI, editado por Mônica Hertz e Arthur Bernardes do Amaral. Rio de Janeiro: PUC-Rio; Edições Loyola.

Díaz Matey, Gustavo. 2017. "El papel de la inteligencia en la lucha contra el terrorismo salafista yihadista." Revista CIDOB d'Afers Internacionals 116: 207-228.

El-Said, Hamed. 2015. New approaches to countering terrorismo: designing and evaluating counter radicalization and de-radicalization programs. Londres: Palgrave Macmillan.

Evans, Graham, e Jeffrey Newnham. 1998. Penguin Dictionary of International Relations. Londres: Penguim Books.

EUA (Estados Unidos da América). 2002. The National Security Strategy. National Security Council, The White House/President George W. Bush, setembro de 2006. https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/.

Fonseca, Guilherme Damasceno, e Jorge Mascarenhas Lasmar. 2017. Passaporte para o terror: os voluntários do Estado Islâmico. Curitiba: Appris.

Fraga Iribarne, Manuel. 2004. "El terrorismo hoy." In Terrorismo, editado por Adriano Moreira. Coimbra: Almedina.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Garcia, Francisco Proença. 2010. Da guerra e da estratégia: a nova polemologia. Lisboa: Prefácio Editora.

Ginkel, Bibi van. 2015. "The (In-)Effectiveness of "deterrence" as an instrument against jihadist terrorist threats." Perspectives 6. The International Centre for Counter-Terrorism.

Gray, Colin. 2000. "Deterrence in the 21st century." Comparative Strategy 19 (3): 255-261. https://doi.org/10.1080/01495930008403211.

Gray, Colin. 2003. Maintaining Effective Deterrence. Carlisle: Strategic Studies Institute; US Army War College.

Gray, Colin. 2010. "Gaining compliance: the theory of deterrence and its modern application." Comparative Strategy 29 (3): 278-283. https://doi.org/10.1080/01495933.2010.492198.

Hopf, Ted. 1994. Peripheral visions: deterrence theory and American foreign policy in the Third World, 1965–1990. Ann Arbor: University of Michigan Press.

Íñigo Álvarez, Laura. 2016. "Los grupos armados ante el Derecho Internacional contemporáneo: obligaciones y responsabilidad." *Revista Electrónica de Estudios Internacionales* 31: 229-242. https://doi.org/10.17103/reei.31.11.

Kajibanga, Rosa. 2016. "Defesa nacional: novas ameaças." CEDIS Working Papers - Direito, Segurança e Democracia 33. Faculdade de Direito da Universidade Nova de Lisboa. https://cedis.novalaw.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_defesa-nacional_novas--ameaças.pdf.

Knopf, Jeffrey. 2010. "The Fourth Wave in Deterrence Research." Contemporary Security Policy 31 (1): 1-33. https://doi.org/10.1080/13523261003640819.

Koschade, Stuart. 2006. "A social network analysis of Jemaah Islamiyah: the applications to counterterrorism and intelligence." Studies in Conflict & Terrorism 29: 559-575. https://doi.org/10.1080/10576100600798418.

Laqueur, Walter. 1976. "The futility of Terrorism." Harper's Magazine 252 (1510): 99-104.

McCants, William. 2016. The ISIS Apocalypse: the history, strategy, and doomsday vision of the Islamic State. Nova York: Picador.

Napoleoni, Loretta. 2015. A Fênix Islamista: o Estado Islâmico e a reconfiguração do Oriente Médio. Rio de Janeiro: Bertrand Brasil.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Nasser, Reginaldo. 2021. A luta contra o terrorismo: os Estados Unidos e os amigos talibãs. São Paulo: Contracorrente.

OSCE (Organization for Security and Cooperation in Europe). 2014. Preventing terrorism and countering violente extremism and radicalisation that lead to Terrorism: a community-policing approach. http://www.osce.org/secretariat/111438?download=true.

Puchades Navarro, Miguel. 2011. "Análisis económico de la respuesta a la amenaza del terrorismo y su impacto sobre las libertades públicas." In Estado de derecho y derechos fundamentales en la lucha contra el terrorismo una aproximación multidisciplinar (histórica, jurídico-comparada, filosófica y económica), editado por Aniceto Masferrer. Pamplona: Thomson Reuters.

Queiroz, Cristina. 2013. Direito Internacional e Relações Internacionais. Coimbra: Coimbra Editoras.

Quinlan, Michael. 2004. "Deterrence and Deterrability." Contemporary Security Policy 25 (1): 11- 17. https://doi.org/10.1111/j.1745-9125.2010.00191.x.

Ramos, António Fonte. 2009. "A nova dimensão do terrorismo transnacional e o seu impacto no sistema político internacional – do 11 de setembro ao 11 de março." In Terrorismo transnacional: estratégias de prevenção e resposta. Lisboa: IESM; Edições Prefácio.

Richardson, Louise. 2006. What terrorists want: understanding the enemy, containing the threat. Nova York: Random House.

Schelling, Thomas. 2008. Arms and influence. New Haven: Yale University Press.

Schelling, Thomas. 2011. The Strategy of Conflict. Cambridge: Harvard University Press.

Snyder, Glenn. 1961. Deterrence and Defense: toward a theory of national security. Westport: Greenwood Press.

Sprinzak, Ehud. 2000. "Rational Fanatics." Foreign Policy, setembro/outubro de 2000, 66-73. https://foreignpolicy.com/2009/11/20/rational-fanatics/.

Stern, Jessica, e J. M. Berger. 2015. Estado Islâmico, Estado de terror. Lisboa: Vogais.

Suarez, Marcial. 2013. As Guerras de George W. Bush e o terrorismo no século XXI. Curitiba: Appris.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.262
ISSN 2595-4717

Tomé, Luís. 2015. ‘‘Estado Islâmico: percurso e alcance um ano depois da autoproclamação do ‘Califado’.’’ JANUS.NET e-journal of International Relations 6 (1).

Trager, Robert, e Dessislava Zagorchen. 2005. ‘‘Deterring terrorism: it can be done.’’ International Security 30 (3): 87-123.

Wagner, Patrick. 2004. Deterrence and terrorism: can global terrorism be deterred? Munique: Grin Verlag.

Weimann, Gabriel. 2014. ‘‘Social media’s appeal to terrorists.’’ Insite Blog on Terrorism and Extremism. http://news.siteintelgroup.com/blog/index.php/entry/295-social-media’s-appeal-to-terrorists.

Wilner, Alex. 2011. ‘‘Deterring the undeterrable: coercion, denial, and delegitimization in counterterrorism.’’ Journal of Strategic Studies 34 (1): 3-37. https://doi.org/10.1080/01402390.2011.541760.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Artigo de pesquisa

Irene Calaça[1]
ORCiD 0000-0002-8372-8464

INTELIGÊNCIA DE ESTADO E ÉTICA NO BRASIL

https://doi.org/10.58960/rbi.2025.20.264

Calaça, Irene. 2025. "Inteligência de Estado e ética no Brasil," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.264. https://doi.org/10.58960/rbi.2025.20.264.

Recebido em 13/12/2024
Aprovado em 17/11/2025
Publicado em 19/12/2025

1 Especialista em Bioética pela Universidade de Brasília (UnB). Mestre em Letras e Linguística pela Universidade Federal de Goiás (UFG). Oficial de Inteligência da Agência Brasileira de Inteligência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

INTELIGÊNCIA DE ESTADO E ÉTICA NO BRASIL

RESUMO

A Atividade de Inteligência (AI) aplica técnicas operacionais que podem suscitar questionamentos de natureza moral. Considerando o Estado Democrático de Direito, qual arcabouço ético caracterizaria a AI? Em pesquisa bibliográfica, analisamos cinco abordagens éticas, comparando-as com normativos da AI. No Brasil, exige-se moralidade administrativa dos profissionais; há controle do Estado sobre atos da AI; conflitos de direitos fundamentais são apreciados juridicamente caso a caso. Constata-se sobreposição de papeis: profissionais atuam como depositários de ações intrusivas de Estado e como indivíduos. O arcabouço ético que melhor descreve o contexto brasileiro é a Teoria da Atividade de Inteligência Justa, com causa justa, protocolos, autorização por autoridade competente, reciprocidade, intenção íntegra, proporcionalidade, discernimento, detalhamento das reais necessidades e sigilo em ações.

Palavras-chave: Atividade de Inteligência, ética.

NATIONAL INTELLIGENCE ACTIVITY AND ETHICS IN BRAZIL

ABSTRACT

Intelligence Activity (IA) applies operational techniques that may evoke moral issues. In view of the Democratic Rule of Law, which ethical framework would characterize Brazilian IA? Through bibliographic research, we analyzed five ethical approaches, comparing them with IA regulations. In Brazil, administrative morality is required from professionals; there is a State control over IA; conflicts of fundamental rights are legally assessed on a case-by-case basis. There exists an overlapping of roles: professionals act as both custodians of State actions and individuals. The ethical framework that best describes the Brazilian context is the Just Intelligence Theory, that requires just cause, protocols use, authorization by competent authority, reciprocity, honest intention, proportionality, discernment, detailing of real needs and secrecy.

Keywords: *Intelligence Activity, ethics.*

LA INTELIGENCIA DEL ESTADO BRASILEÑA Y LA ÉTICA

RESUMEN

La Actividad de Inteligencia (AI) aplica técnicas operativas que pueden plantear cuestiones de naturaleza moral. Considerando el Estado Democrático de Derecho, ¿qué marco ético caracterizaría la AI? Con investigación bibliográfica, analizamos cinco enfoques éticos, comparándolos con las regulaciones de AI. En Brasil, se exige moralidad administrativa de los profesionales; existe control estatal sobre AI; los conflictos de derechos fundamentales se evalúan jurídicamente. Hay una superposición de papeles: los profesionales actúan como titulares de las acciones del Estado y como individuos. El marco ético que mejor describe el contexto brasileño es la Teoría de la Actividad de Inteligencia Justa, que utiliza protocolos, justa causa, autorización de autoridad, intención honesta, reciprocidad, proporcionalidad, discernimiento, necesidades reales y secreto en las acciones.

Palabras clave: *Actividad de Inteligencia, ética.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Introdução

A inteligência de Estado é milenar e evoca série de "expectativas compartilhadas". Tanto os Estados (aliados ou não), como os cidadãos esperam da inteligência a aplicação de técnicas que, moralmente, não seriam aceitas entre pessoas físicas ou jurídicas, tais como vigilância.

A inteligência de Estado realiza atividade sigilosa, empregando técnicas operacionais especializadas no intuito de "contornar obstáculos a fim de alcançar objetivo determinado pelos Estados em contextos conflitivos e adversos" (Brasil 2023, 18), ou seja, visando realizar ações sigilosas que atendam interesse público dentro do espaço a ela designado pelo ordenamento jurídico do País.

Considerando vivermos em Estado Democrático de Direito, surge questionamento: Qual arcabouço ético melhor caracterizaria a inteligência do País nos dias de hoje, tendo em vista a moralidade administrativa que é cobrada de todos órgãos públicos?

Discorremos sobre a questão com base em pesquisa bibliográfica. Examinamos a ética na inteligência de Estado brasileira em quatro momentos: primeiro, problematizamos a ética da Inteligência de Estado em contexto internacional, para, a seguir, apresentarmos teorias que propõem abordagens éticas na área. O terceiro tópico delineia as peculiaridades da ética no Estado e na inteligência brasileira, a partir da Constituição Federal de 1988 (Brasil 1988), doravante denominada CF, e o quarto, apresenta nossos comentários e conclusões.

O objetivo do presente artigo é incitar juristas e profissionais de inteligência a se aprofundarem no tema da ética e a desenvolverem mais estudos sobre a área.

A ética da Inteligência de Estado em contexto internacional

Definido como "conjunto organizado das instituições políticas, jurídicas [...] sob um governo autônomo e ocupando um território próprio e independente" (Japiassú e Marcondes 2001, 90), Estado é uma entidade idealizada, que vem sendo personificada.

Ao Estado vêm sendo atribuídas características, sentimentos ou ações próprias dos seres humanos, facilitando que possam ser codificadas como regras semelhantes às do Direito. Essa personificação é ferramenta útil, pois chama

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

para o ente as implicações morais internacionais que seriam prejudicais aos cidadãos: os Estados Unidos da América (EUA) invadiram o Iraque; a Rússia atacou a Ucrânia. Não foi determinado cidadão que praticou a ação funesta, mas o Estado personificado.

> Todo Estado celebra tratados na expectativa de que serão observados[;] e os Estados que violam os tratados[,] ou negam que o fizeram, ou defendem a violação com argumentos que visam a demonstrar que essa violação era legal ou moralmente justificável (Carr 2001).

Para serem reconhecidos na comunidade internacional, os Estados obrigam-se a aceitar os cânones éticos e as regras do direito internacional. Nesse intuito, seus representantes justificam moralmente as ações políticas que tomam. Assim, encontramos alegações de que os EUA invadiram o Iraque no ano de 2003 para eliminar as armas de destruição em massa do regime de Saddam Hussein, ou que a Rússia atacou a Ucrânia no ano de 2022 revidando a agressão sofrida pelas populações de Donetsk e Lugansk. Em nível supranacional, verifica-se que as agressões mencionadas, atos que seriam imorais para o indivíduo, tornam-se aceitáveis quando praticadas em nome da pessoa coletiva, em prol de um "bem maior", que seria autopreservação do Estado (Hobbes 2003).

Por sua vez, o nível infra estatal é mantido através de convenções morais, uma espécie de contrato social aplicado a indivíduos e empresas, cuja quebra poderia originar o caos dentro do Estado e, portanto, deve ser evitado.

Assim, vemos que a União Europeia dificulta entrada de imigrantes e refugiados em suas fronteiras (Euronews 2024; Galvin 2021), no intuito de evitar aumento da criminalidade, diminuição do padrão de vida de seus nacionais, entre outras justificativas, ou seja, realiza ações que contrariam os direitos humanos, mas que não são interrompidas.

O mesmo se repete com a aplicação de técnicas de espionagem sobre países considerados "aliados". A comunidade internacional aceita o emprego dessas técnicas, que não seriam cabíveis a indivíduos e empresas, como prerrogativa da defesa do Estado como instituição[1], ao mesmo tempo em que condena espionagem industrial e atuação de hackers por interesses privados[2].

1 De acordo com Carr, o Estado possui direito ao bem comum e à autopreservação, os quais superam a obrigação moral; e práticas como espionagem são "comuns a todas as grandes potências, e um estado que não recorra a esses expedientes poderá encontrar-se em desvantagem" (Carr 2001, 207).

2 Seumas Miller lembra que, muitas vezes, a linha que diferencia o emprego de técnicas operacionais por membros de governo, cidadãos e mesmo organizações pode ser tênue. Conside-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Sobre grampeamento de telefones de autoridades de países aliados (inclusive do Brasil), efetuado pelos EUA nos anos de 2013 e 2015, eis comentário do ex-ministro francês Bernard Kouchner em entrevista:

> A indignação europeia é menos sobre a espionagem cruzar qualquer linha moral e mais sobre a extensão do domínio da inteligência dos Estados Unidos. Vamos ser honestos, nós escutamos também. Todo mundo está ouvindo todo mundo, mas não temos os mesmos meios que os Estados Unidos, o que nos deixa com inveja (Kouchner 2013).

Independentemente de ser ou não democrático, nenhum governo pode se permitir revelar informações completas e francas acerca de suas próprias forças e deficiências, nem mesmo divulgar a outros países todo conhecimento que possui sobre parceiros e concorrentes. Seria muita exposição. Quaisquer sintomas de ineficiência ou despreparo de um país se refletem em seu status político.

Nesse contexto, a atividade de inteligência exerce importante papel estratégico na obtenção e guarda de conhecimentos sobre eventos e situações que possam impactar o processo decisório de gestores, bem como na identificação e defesa de ações externas que constituam ameaças aos interesses da sociedade e do Estado – tudo de forma discreta.

Após os ataques terroristas de 11 de setembro de 2001 nos EUA, houve uma mudança radical nas ações da Atividade de Inteligência por todo mundo. A Atividade passou a ser securitizada, ou seja, direcionada para a segurança tanto interna, como externa, dos Estados.

Países tecnologicamente avançados tomaram os referidos eventos como mote para aplicar técnicas de coleta de dados e de vigilância em massa na própria população[3], e, até mesmo, para recrutar crianças em ações de inteligência (Rayment 2023), sob o rótulo de "proteção" a ameaças terroristas. Fazem-se necessários debates sobre moralidade e ética na atividade de inteligência.

---

re-se, por exemplo a empresa Huawei, seus executivos e os membros governo chinês: os atos de uns elementos encontram-se concatenados com os de outros (Miller 2021, 230).

3 Como exemplo de vigilância em massa, podemos citar aquela conduzida pela aliança de compartilhamento de informações de sinais Five Eyes Intelligence Oversight, formada por Austrália, Nova Zelândia, EUA, Canadá e Reino Unido (EUA 2024a). Por ser supranacional, a organização não atende às leis de proteção de dados dos cidadãos dos países que a integram. Assim, um país encontra-se apto a coletar dados de alvos para outro país-membro, que não fica eticamente comprometido diante da própria população (BBC News Brasil 2013; Frazão 2016; Miller 2020; Miller e Mueller 2020).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

A seguir, apresentamos a ética e examinamos abordagens éticas empregadas pela literatura internacional como justificativa (ou não) do emprego de ações invasivas de inteligência.

Teorias éticas na Inteligência de Estado

Ética é a reflexão sobre condutas da vida coletiva, uma filosofia da moral associada à reflexão sobre o "agir bem"[4]. Ela examina o emprego de valores[5] comportamentais como moral, justiça, transparência e retidão, que sinalizam uma boa conduta social, além da forma como esses se refletem na sociedade, gerando equilíbrio e respeito nas relações entre as pessoas.

A ética possui "faces" ou abordagens, que variam de acordo com a cultura, a época e o pensador que a idealizou, as quais podem ser empregadas para analisar a moralidade dos atos dos serviços de inteligência. Essas "faces" surgiram e foram moldadas em determinado período histórico, têm sua razão de ser e atendem a argumentos plausíveis, que, mantidos ao longo dos séculos, são evocados ainda hoje.

A literatura internacional (Erskine 2010; Jones 2010) propõe quatro abordagens éticas aplicadas ao contexto da atividade de inteligência, dispostas em um contínuo crescente, que se inicia com restrições ao uso da força (imposição de ações exclusivamente morais) em ações de inteligência, até a aceitação de que algumas ações mais duras são justificáveis pelo bem do Estado. Enriquecemos essa escala com um quinto elemento, do que resulta o seguinte alinhamento de abordagens: idealista, utilitarista de regras e atos (nossa inserção), Teoria da Atividade de Inteligência Justa, consequencialista e realista.

Em um extremo da escala, alocamos a **abordagem idealista** ou deontológica (do grego deon, que significa "dever"), que tem sua origem em Kant (Abbagnano 2007, 385) e concebe a moralidade como absoluto, um fim em si mesmo. Segundo o filósofo, ações imorais não podem ser usadas como medida para justificar o atingimento de objetivo, ainda que legal (Miranda

4 Filosoficamente, encontramos ambiguidade na noção de "bem". Uma das acepções seria "bem" como perfeição ideal, realidade perfeita (ética do fim em si mesmo); outra, como objeto de desejo que direciona as ações do ser humano (ética móvel). Maiores detalhes em Abbagnano (2007, 380; 385).

5 O termo "valor" tem sua origem nas ciências econômicas, onde diferencia algo (objeto ou coisa) necessário ao indivíduo. Em Filosofia, o conceito recebeu novas acepções, como "avaliação qualitativa [...] sobre a moralidade de um ato", ou "Juízo que estabelece se algo deve ser objeto de elogio, recomendação ou censura" (Japiassú e Marcondes 2001, 268).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Filho 2019). Alguns atos são intrinsicamente errados, independentemente de suas consequências. Nessa perspectiva, as avaliações éticas precisam considerar a "bondade" e a "maldade" intrínsecas dos atos para aceitá-los ou não.

O outro extremo do espectro é ocupado pela **abordagem realista** (Hobbes 2003; Maquiavel 1976). Nessa perspectiva ética, o valor moral maior seria o da razão de Estado. O interesse nacional de determinado país se tornaria, per se, um princípio moral, e a defesa do Estado, um dever do governante em relação à população que o conduziu ao poder[6]. Segundo Maquiavel (1976), governantes estariam autorizados a utilizar quaisquer meios que lhe pareçam adequados para subverter, por força ou subterfúgios, a instabilidade política, visando o bem universal, ou seja, aquilo que em nossos dias seriam a estabilidade do Estado e a segurança nacional. Sob essa perspectiva alguns países justificam o emprego de métodos como tortura para coleta de dados.

Próximo à abordagem realista, encontra-se a **abordagem consequencialista** (Erskine 2010), que, para julgar moral ou não um ato da inteligência, leva em consideração efeitos danosos de certas ações para a comunidade em geral. Trata-se de cálculo moral utilitarista[7], em que o pretexto para uso de ações criticáveis ocorre quando o benefício delas decorrente é maior que o malefício. A simples existência de benefícios não justificaria as ações. Para os consequencialistas, os meios empregados para reunião[8] de dados seriam moralmente justificados pelo impacto positivo do conhecimento obtido. O bem maior justificaria, inclusive, a adoção de meios invasivos.

A **Teoria da Atividade de Inteligência Justa** (TAIJ) também possui fundo utilitarista (Gendron 2005; Bellaby 2012; Omand e Phythian 2018). De acordo com Miller (2021, 225-228), a TAIJ foi inspirada na Teoria da Guerra

6 Conforme Hobbes (2003), em uma República os cidadãos pactuam entre si, atribuindo ao governante eleito por maioria o direito de representá-los (inclusive àqueles discordantes que perderam o pleito) e autorizando que tome decisões como se suas fossem, no intuito de viverem sob paz, segurança e proteção. Entre outras prerrogativas, cabe ao governante o direito de manter paz ou guerrear com outras nações, ou seja, de decidir "quando a guerra corresponde ao bem comum e qual quantidade de forças devem ser reunidas..." (Hobbes 2003, 154).

7 Seriam sete as variáveis a serem consideradas ao determinarmos o "cálculo de utilidade" da ação, sob a perspectiva ética: "intensidade [do bem/do prazer ocasionado]; duração; certeza ou incerteza; proximidade no tempo; fecundidade; pureza e extensão. Os prazeres que sustentam maiores valores em relação a essas variáveis teriam maior valor moral" (Araújo 2015, 17). Assim, caberia ao Estado, por exemplo, tomar decisões que promovessem o bem dos cidadãos em escala pública, e não privada. Argumentos e contra-argumentos ao utilitarismo são examinados em Araújo (2015).

8 Em Inteligência, "reunião" é coleta e busca (operacional) de dados.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Justa[9], mas dela se diferencia pela aplicação do princípio reciprocidade em situações de autodefesa do Estado, característica exclusiva da atividade de inteligência. Assim, a TAIJ é sensível aos ditames da abordagem idealista, porém admite que os países não podem sacrificar seus interesses e aceitar ameaças à sua segurança. Essa abordagem ética identifica condições que, se aplicadas a ações de inteligência, minimizariam danos aos interesses de indivíduos: necessidade, autoridade legítima, intenção correta, último recurso, reciprocidade, proporcionalidade e discriminação. A TAIJ reconhece os direitos individuais dos cidadãos, bem como a necessidade de os serviços utilizarem métodos encobertos e intrusivos, porém considera que as exceções às normas éticas devem ser justificadas e proporcionalmente limitadas.

Acrescentamos à lista de Erskine (2010) e Jones (2010) a **abordagem utilitarista de regras e atos**, trazida por Araújo (2015). Esta toma como premissa a existência de dois níveis de raciocínios morais, um intuitivo (utilitarismo de regras) e outro, crítico (utilitarismo de atos). Em situações cotidianas, ambos níveis coincidiriam, porém, diante de dilemas morais mais complexos, regras não gerariam a resposta correta, assim, apelaríamos para raciocínio moral crítico do indivíduo, empregando cálculo de utilidade sobre as consequências dos atos para as pessoas envolvidas no dilema.

As abordagens acima descritas podem ser utilizadas para pensarmos os dilemas encontrados, ora pelos profissionais de inteligência, ora pelo próprio órgão, a fim de amparar – perante a sociedade ou a própria consciência – o emprego de ações operacionais. As cinco formam molduras éticas que justificam ou racionalizam ampla gama de práticas e políticas de inteligência em diversos países.

Concluindo esse tópico, vimos que a ética investiga motivações e valores comportamentais em sociedade. Encontramos cinco abordagens éticas que podem ser aplicadas à atividade de inteligência, diferenciadas pelo menor ou maior grau de intrusão dessa sobre a sociedade, a saber: idealista, utilitarista de regras e atos, TAIJ, consequencialista e realista.

A seguir, descrevemos as peculiaridades da ética na inteligência de Estado brasileira, a partir do contexto do Estado Democrático de Direito, e, em seguida, buscamos conectá-las com as cinco abordagens éticas já examinadas. Finalizamos, então, o estudo, trazendo nossas considerações.

9 A Teoria da Guerra Justa adota tradicionalmente critérios de motivo e proporcionalidade para invocar a legitimidade do uso da força em determinado evento bélico (Bellaby 2012, 14).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

A ética na Inteligência de Estado brasileira e a democracia

O tratamento da ética no Brasil possui suas peculiaridades, contudo, é perfeitamente ajustável às teorias acima expostas, respeitados graus de profundidade estabelecidos pela legislação interna. A seguir, discorremos sobre a moldura ética empregada no País – tanto a cobrada da atividade de inteligência (exercida por órgãos públicos que representam o Estado), como a dos profissionais de inteligência (indivíduos).

No Brasil, exige-se comportamento ético de todos servidores públicos. A ''ética'' e a ''moralidade'' mencionadas na CF e em códigos de conduta de agentes públicos são oriundas de princípios jurídicos (i.e, são normativas) e adaptadas à Administração Pública. A violação desses preceitos gera consequências externas ao sujeito, tais como sanções jurídico-administrativas e penais (Pellanda 2005).

O princípio moralidade, especificado no art. 37 da CF, disciplina as condutas interpessoais, ou seja, a ética dentro da administração pública. Enquanto a moral comum distingue bem e o mal, a moral administrativa é guiada pela diferença entre boas e más práticas da administração pública (Mello 2004).

A moralidade dos atos públicos é estabelecida através do cotejamento de fins (finalidade da ação), meios utilizados e ideia de legitimidade das ações para o atendimento do interesse público ou bem comum.

> O agente público tem o dever de bem administrar os interesses a ele confiados. Quando administra mal ou utiliza seus poderes administrativos para atingir resultados 'divorciados do interesse público a que deveria atender', ele viola a moralidade administrativa (Mello 2004, 97).

O princípio moralidade busca evitar, na administração pública, o desvio de finalidade, motivos ou conteúdo: as ações devem ser motivadas por necessidade pública, respeitar direitos fundamentais e ter registros de acesso rastreáveis, ''para efeito de responsabilização em caso de eventual omissão, desvio ou abuso'' (STF 2021). Por conseguinte, a imoralidade administrativa se caracteriza pela usurpação, por parte dos agentes públicos, dos poderes de Estado e pelo não cumprimento das premissas básicas referentes à legalidade e à manutenção do bem comum (interesse público e fins institucionais).

Do princípio moralidade originam-se princípios como probidade, eficiência e impessoalidade nos atos dos servidores.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Os profissionais da área de inteligência de Estado brasileira são servidores públicos concursados, ou seja, eles possuem direitos, deveres e obrigações delimitados por lei, ao mesmo tempo em que precisam atender à necessidade de autopreservação do Estado.

> As atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado (Lei nº 9.883, de 07 de dezembro de 1999).

Permite-se à atividade de Inteligência de Estado o uso de técnicas e meios sigilosos, observados controles internos e externos, a fim de que se assegure à sociedade a consonância das ações da inteligência com os princípios constitucionais, a lisura em ações e a fidelidade às instituições e à Ética.

Surgem, então, questionamentos. Considerando a discrição que envolve a atividade, como conferir se a inteligência de Estado cumpre os parâmetros exigidos por lei?

Segundo a ADI nº 6529 (STF 2021), toda movimentação dentro da atividade de inteligência é registrada e autorizada por meio de sistema governamental de gestão de documentos e envolve elaboração de planos, planejamentos, análises de risco, prestações de conta, relatórios de inteligência e outros documentos envoltos de fé pública[10], os quais, mesmo sendo sigilosos, podem ser acessados por órgãos de controle[11], que atestam a conformidade administrativa e jurídica das ações (Brasil 2023). Por conseguinte, não obstante o grifo de sigilo que envolve os documentos, esses são legais e podem ser recuperados e auditados, o que assegura ética e transparência na atividade de inteligência.

Outra pergunta que surge: Como conciliar a inteligência com as garantias fundamentais do Art. 5º da CF, ou seja, os direitos fundamentais à vida, à liberdade, à igualdade, à segurança e à propriedade?

10 A fé pública é bem jurídico protegido em relação à autenticidade de documento público. É "a confiança que a sociedade deposita nos objetos, sinais e formas exteriores (moedas, emblemas, documentos), aos quais o Estado, mediante o direito, privado ou público, atribui um valor probatório qualquer, bem como a boa-fé e o crédito dos cidadãos nas relações da vida comercial e industrial", conforme assinala Rocco (Cardoso 2017, 3).

11 Alguns órgãos de controle democrático da atividade de Inteligência são: Congresso Nacional (Comissão Mista de Controle das Atividades de Inteligência), Tribunal de Contas da União; Controladoria-Geral da União, além da Secretaria de Controle Interno da Presidência da República (Brasil 2023, 22-23).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Encontramos na própria Constituição brasileira o direito à vida – princípio que garante ao indivíduo viver com dignidade, preservando sua intimidade, vida privada e integridades física e moral[12]; o direito à liberdade, ao sigilo e ao acesso de informações lado a lado com ressalvas ligadas ao bem do Estado, de indivíduos e das instituições democráticas[13].

Em caso de colisão de direitos fundamentais, não existiria prevalência de um sobre o outro. A solução exigiria análise ponderada, a ser realizada caso a caso pelo Poder Judiciário.

No Brasil, em certas situações, sob autorização explícita da legislação e de juízes, o interesse coletivo é colocado acima dos princípios da liberdade e do sigilo de determinado cidadão, considerando-se a segurança de outrem e a estabilidade social. É o que acontece com cidadãos que são acompanhados por incitarem atos terroristas, ou com aqueles que têm sigilo de usuário quebrado em redes sociais, por prática de injúria ou difamação, afinal, a liberdade de um indivíduo não pode ser usada para encobrir ameaças e ataques contra outras pessoas ou a democracia.

Frisamos, contudo, que essa autorização legal para acessar dados privados é delegada pelo Estado à organização e deve considerar o interesse público ou o bem comum[14], não podendo ser utilizada em benefício do servidor que pratica o ato, nem com fins corporativistas.

Da mesma forma, a organização deve respeitar o ordenamento jurídico e o próprio cidadão, que não terá seus direitos civis e constitucionais anulados aleatoriamente em prol do benefício da comunidade em geral – exatamente

12 Art. 5º "II- ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei; III- ninguém será submetido a tortura nem a tratamento desumano ou degradante". (CF 1988).

13 Direito ao sigilo "de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial..." (Idem, Art. 5º, XII); direito ao "acesso à informação e resguardado o sigilo da fonte quando necessário ao exercício profissional" (Idem, XIV). Direito de ir e vir, de não ser preso ou detido sem motivo ou sem ter infringido a lei.

14 Antônio Ferraz mostra que interesse público não se confunde com o interesse de grupos particulares, nem com a Razão de Estado encontrada em Maquiavel e Hobbes. Segundo o autor, o conceito corresponderia à expressão positiva do "bem comum", ao interesse real da população: "Interesse público é pertinente a toda a sociedade, personificada no Estado. É o interesse à preservação permanente dos valores transcendentais dessa sociedade. Não é, assim, o interesse de um, de alguns, de um grupo ou de uma parcela da comunidade; nem mesmo é o interesse só do Estado, enquanto pessoa jurídica empenhada na consecução de seus fins. É o interesse de todos, abrangente e abstrato. E por ser de todos não é de ninguém. " Antônio Ferraz (Andrade e Silva 2000, 11).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

o contrário do que advogaria a abordagem consequencialista[15].

Prosseguindo, nota-se que, por um lado, o profissional inteligência é cobrado como depositário de ações intrusivas do Estado, e, por outro, é demandado como indivíduo, devendo manter comportamento ético e boas práticas, no intuito de preservar honra e tradição dos serviços públicos e da organização[16].

Mesmo respeitando a legalidade e visando suprir uma necessidade de Estado, tais ações não se justificariam sob a ética idealista kantiana por serem intrusivas. Ademais, a situação cria sobreposição da ética do Estado sobre a do indivíduo na área da inteligência, originando dilema ético[17].

Pelo mesmo motivo, ações intrusivas do Estado não poderiam ser realizadas sob a abordagem utilitarista de regras e atos. O profissional de inteligência tem consciência da moralidade administrativa exigida dos servidores de Estado brasileiros. Qualquer iniciativa que tome para resolver dilemas oriundos da atividade (utilizando "cálculo de utilidade" pessoal) depositaria sobre seus ombros eventuais ônus legais que surgissem.

As referidas ações tampouco poderiam ser realizadas sob a ética realista, uma vez que o poder exacerbado advindo dessa não atenderia às bases constitucionais brasileiras, centradas no Estado Democrático de Direito. No Brasil, por exemplo, seria ética e juridicamente inadmissível o emprego da vigilância *Five Eyes Intelligence Oversight* (DNI 2024), realizada por outros países – também democráticos.

Isso posto, se tomarmos como parâmetro o texto constitucional brasileiro, o qual reconhece direitos fundamentais, mas não prevê direitos e garantias de caráter absoluto, bem como os códigos de ética profissionais exigidos dos servidores[18], podemos sugerir que a moldura ética que melhor descre-

15 Nos EUA, o *Foreign Intelligence Surveillance Act* (EUA 1978), por exemplo, autoriza testes de equipamentos de vigilância eletrônica, para os quais "não seria lógico obter o consentimento de pessoas que por acaso fossem envoltas pela vigilância". O Reino Unido, por sua vez, possui legislação autorizando "condutas criminais" em ações de inteligência (Reino unido 2022).

16 Consideradas as peculiaridades das áreas, dilemas semelhantes são enfrentados por profissionais de outros campos, como jornalistas investigativos (em relação a terem ou não atingido o limite da legalidade, ou mesmo da segurança para obtenção de determinado dado) e médicos (que, em situação de crise, precisam optar por atender paciente que tenha maior chance de sobrevida).

17 Dilema ético são situações "em que não há decisão obviamente certa ou errada, mas, sim, uma resposta certa sob diferentes aspectos" (Michaelis s.d).

18 Sobre princípios e valores éticos, assim como comportamentos exigidos e vetados aos

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

ve o contexto histórico encontrado na atividade de inteligência de Estado brasileira é a caracterizada pelo utilitarismo, conforme a variante da Teoria da Atividade de Inteligência Justa, detalhada por Omand e Phythian (2018, 226) e Miller (2021).

Segundo os autores, riscos éticos são minimizados quando as ações de inteligência acontecem sob causa justa, com protocolos que seguem estatutos legais transparentes ao público e com documentos governamentais que esclarecem explicitamente a intenção da "segurança nacional".

Da mesma forma, autoridade competente deve autorizar e, conforme o nível, conduzir, supervisionar e prestar contas da operação. Quanto mais intrusiva seja a atividade, mais alto deve ser o nível hierárquico do decisor a autorizá-la. Isso porque a confiança da sociedade é facilmente destruída se, após algum escândalo, não ficar claro quem autorizou a operação, ou então, se a cadeia de custódia do documento estiver ausente ou tiver sido rompida[19].

Faz-se necessária, também, intenção íntegra, que direcione a ação de inteligência para o bem maior e evite o uso da máquina pública em benefício pessoal. Há que se repudiar agendas políticas e outras sendo encobertas para realização de missão.

Importante considerar a proporcionalidade e a reciprocidade entre a necessidade, os riscos éticos da operação e o dano a ser evitado, em outras palavras, há que se sobrepesar ônus e bônus de conduzir ou não uma operação, bem como em que escala deve ser conduzida, considerando o tipo de alvo das ações de inteligência – se interno ou externo, pessoa física, organização ou Estado.

Omand e Phythian (2018), salientam a necessidade de discernimento, ou seja, a capacidade de se distinguir os verdadeiros alvos dos demais cidadãos inocentes, evitando invasões de privacidade, vigilância em massa ou "expedições exploratórias" desnecessárias. Primar sempre pelos princípios "simplicidade" e "segurança".

Há que se considerar a perspectiva razoável de sucesso da ação de inteli-

servidores públicos: CF 1988; Decreto nº 1.171 de 22 de junho de 1994; Portaria nº 66, de 17 de fevereiro de 2022.

19 "Cadeia de custódia" é o controle do registro de acessos e de procedimentos pelos quais o documento passou. Ela garante a integralidade, autenticidade e rastreabilidade dos documentos (Gava e Flores 2021).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

gência. No planejamento, faz-se necessário detalhamento das necessidades técnicas e humanas para acessar e administrar o risco de danos colaterais – inclusive daqueles que não seriam alvo de coleta. Outro ponto é a checagem da necessidade real da missão: não haveria meios menos intrusivos de investigação?

Acrescentaríamos a manutenção do sigilo profissional como corolário de todo esse processo, no intuito de minimizar riscos e salvaguardar a integridade de dados e de todos envolvidos em ações de inteligência.

Conforme Gendron (2005), na geopolítica internacional, como em um jogo, os participantes atuam em consenso, reconhecendo e respeitando as regras (da Inteligência, no caso), sendo capazes de identificar se seriam alvos de operações, a depender dos acessos que possuam ou da posição que ocupam no "tabuleiro" de eventos. Quem estiver ocupando a função "X", de interesse à Inteligência adversa, deve estar consciente de que será alvo dessa Inteligência adversa, devendo tomar as medidas necessárias à própria proteção. Aquele que não quiser ser envolvido no jogo da espionagem, que abandone a função.

Considerações Finais

Moral e ética regulam a convivência dentro dos grupos sociais e ajudam a moldar os cidadãos para que sejam mais empáticos em suas tomadas de decisão. Em mundo caracterizado pela volatilidade, a harmonia e a paz social são mantidas quando garantimos a todos cidadãos que as convenções morais são seguidas e que a máquina pública atua com ética, observa os direitos fundamentais de todos indivíduos de forma igualitária e defende o Estado Democrático de Direito.

A ética possui diversas faces, que variam de acordo com o país, a cultura e a época. Neste trabalho comentamos cinco. O epíteto de "ser ético" cumprindo a atividade de inteligência pode ser atribuído, por exemplo, àqueles que consideram praticar apenas o bem (abordagem idealista) e garantir a transparência de quaisquer dados, independentemente das consequências políticas geradas, conforme fez o soldado Bradley Manning, suposta fonte do WikiLeaks (Leigh e Harding 2011). Por outro lado, que "bem" é esse? Atingir o "bem" de uma sociedade ocidental pode afetar negativamente outra, que possua cultura e crenças diferenciadas, implicando em perdas econômicas ou mesmo mortes de inocentes por efeitos, ainda que involuntários, das decisões tomadas pelos altos escalões.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Prosseguindo, "ser ético" também pode estar ligado àqueles que cumpram quaisquer ações necessárias à proteção do Estado e dos cidadãos, a fim de evitar instabilidade política e eventuais danos à maioria da sua população – não importando os meios que utilizem. Ações de inteligência respaldadas pela "razão de Estado" continuam sendo realizadas[20], ainda que pouco divulgadas, para evitar desgastes à imagem do Estado envolvido.

A depender da perspectiva, ferramentas utilitaristas também podem auxiliar a sobrepesar ônus e bônus de tomar ou não determinada atitude, podendo ser usadas por indivíduos (utilitarismo de regras e atos) e pelo Estado – consequencialistas, que buscam atingir um bem maior para justificar adoção de meios invasivos, ou adeptos à Teoria da Atividade de Inteligência Justa, a qual impõe parâmetros às ações de inteligência.

Todas essas molduras têm sua razão de ser, seus "argumentos", e todas podem estar certas. Tomando por base normativos brasileiros, a moldura ética que mais se aproxima ao contexto contemporâneo da Inteligência no País é a Teoria da Atividade de Inteligência Justa. Os descritores éticos apresentados nessa teoria são replicados em portarias e normas correntes, permitindo conciliar, ainda que parcialmente, a moralidade administrativa e a ética.

Na atividade de inteligência, são tarefas constantes observar a consciência individual do profissional e garantir a execução de tarefas imprescindíveis às necessidades de Estado sem fugir à legalidade e à moralidade administrativa.

Além-fronteiras, cada país busca a perspectiva (ou "solução") que seja mais vantajosa aos próprios interesses e é nosso dever, como servidores públicos, encontrar o melhor caminho para o Brasil, sempre considerada a perspectiva da legalidade.

A perfeição pode ser atingida? Não sabemos. Mas buscar entender o que seria um ideal ético e nos aperfeiçoarmos na tentativa de alcança-lo é produtivo, é positivo e é realizável.

20 Vide "armas silenciosas" empregadas pela inteligência russa (EUA 2024b; 2024c) ou o plano estadunidense de conversão de agentes em Guantánamo (Monge 2013).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Referências

Abbagnano, Nicola. 2007. *Dicionário de Filosofia*. Tradução coordenada e revista por Alfredo Bosi. São Paulo: Martins Fontes.

Andrade e Silva, Daniele Souza de. 2000. "Interesse público: necessidade e possibilidade de sua definição no Direito Administrativo". Em *Direito Constitucional, Administrativo, Tributário e Filosofia do Direito*. Coleção Bureau Jurídico, v. II. Brasília: ESAF, 21-31. https://www.jfpe.jus.br/images/stories/docs_pdf/biblioteca/artigosperiodicos/DanielleSouzadeAndrade/InteressepubliconecessidadeepossibilidadeEstudantescadernoacademicon62000.pdf.

Araújo, Leandro Shigueo. 2015. *Ética utilitarista: problemas e respostas*. Dissertação de Mestrado. Uberlândia: Universidade Federal de Uberlândia.

BBC News Brasil. 2013. "Espionagem: como as agências de inteligência coletam dados?". *BBC News Brasil*, 30 de outubro de 2013. Acesso em 10 de dezembro de 2024. https://www.bbc.com/portuguese/noticias/2013/10/131030_inteligencia_coleta_dados_cc.

Bellaby, Ross. 2012. "What's de Harm? The Ethics of Intelligence Collection". *Intelligence and National Security* 1: 93-117, https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.621600.

Brasil. 1988. *Constituição da República Federativa do Brasil*. Brasília, DF: Presidência da República. Acesso em 13 de outubro de 2025. https://www.planalto.gov.br/ccivil_03/constituicao/constitiuicao.htm.

Brasil. 2023. Doutrina da Atividade de Inteligência. Agência Brasileira de Inteligência. https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

Cardoso, Beatriz. 2017. "Crimes contra a fé pública: análise geral". Jusbrasil, 26 de maio de 2023. https://www.jusbrasil.com.br/artigos/crimes-contra-a-fe-publica/417491325.

Carr, Edward Hallet. 2001. *Vinte anos de crise: 1919-1939. Uma introdução ao estudo das relações internacionais*. Brasília: Universidade de Brasília.

Erskine, Toni. 2010. "As rays of light to the human soul: moral agents and Intelligence gathering." Em *Ethics of Spying,* v. 2, editado por Jan Goldman. Lanham: Scarecrow Press.

EUA (Estados Unidos da América). 1978. Foreign Intelligence Surveillance Act (FISA). Acesso em 13 de outubro de 2025. https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

EUA (Estados Unidos da América). 2024a. Five eyes intelligence oversight and review council (FIORC). ODNI (Office of the Director of National Intelligence). Acesso em 13 de outubro de 2025. https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

EUA (Estados Unidos da América). 2024b. "Silent weapons: examining foreign anomalous health incidents targeting Americans in the Homeland". Homeland Security, 8 de maio de 2024. https://homeland.house.gov/hearing/silent-weapons-examining-foreign-anomalous-health-incidents-targeting-americans-in-the-homeland/.

EUA (Estados Unidos da América). 2024c. "Silent weapons: examining foreign anomalous health incidents targeting Americans in the Homeland. Witness testimony." Homeland Security, 8 de maio de 2024. https://homeland.house.gov/wp-content/uploads/2024/05/2024-05-08-CTI-HRG-Testimony.pdf.

Euronews. 2024. "Oito países da UE estão a iniciar conversações para rever a situação na Síria e gerir a crise migratória." *Euronews*, 18 de maio de 2024. Acesso em 13 de outubro de 2025. https://pt.euronews.com/my-europe/2024/05/18/oito-paises-europeus-apelam-a-regulacao-da-crise-migratoria-siria.

Frazão, Pedro Henrique Oliveira. 2016. *Um big brother global? Os programas de vigilância da NSA à luz da securitização dos espaços sociotecnológicos*. Dissertação de Mestrado em Relações Internacionais. João Pessoa: Universidade Estadual da Paraíba.

Galvin, Joe. 2021. "Cooperação entre UE e Líbia resulta em violações aos direitos de migrantes." *Repórter Brasil*, 23 de dezembro de 2021. Acesso em 13 de outubro de 2025. https://reporterbrasil.org.br/2021/12/cooperacao-entre-ue-e-libia-resulta-em-violacoes-aos-direitos-de-migrantes/.

Gava, Tânia Barbosa Sales, e Daniel Flores. 2021. "Auditoria e certificação ao longo da cadeia de custódia digital arquivística". *Informação & Informação* 26 (4): 424-49. https://doi.org/10.5433/1981-8920.2021v26n4p424.

Gendron, Angela. 2005. "Just War, Just Intelligence": an ethical framework for foreign espionage", *International Journal of Intelligence and Counterintelligence* 18 (3): 398-434. http://dx.doi.org/10.1080/08850600590945399.

Hobbes, Thomas. 2003. *Leviatã*. São Paulo: Martins Fontes.

Japiassú, Hilton; e Danilo Marcondes. 2001. *Dicionário básico de Filosofia.* 3ed. Rio de Janeiro: Zahar.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Jones, Jennifer M. 2010. "Is Ethical Intelligence a contradiction in terms?", Em *Etics of Spying*, v. 2, editado por Jan Goldman. Lanham: Scarecrow Press.

Kouchner, Bernard. 2013. Entrevista feita por Max Fischer. "Why America spies on its allies (and probably should)." *The Washington Post / Radio Liberty*. 29 de outubro de 2013. Acesso em 13 de outubro de 2025. https://www.washingtonpost.com/news/worldviews/wp/2013/10/29/why-america-spies-on-its-allies-and-probably-should/.

Leigh, David, e Luke Harding. 2011. *A Guerra de Julian Assange contra os Segredos de Estado*. Campinas: Verus.

Maquiavel. 1976. *O príncipe*. São Paulo: Cultrix.

Mello, Claudio Ari. 2004. "Fragmentos teóricos sobre a moralidade administrativa," *Revista de Direito Administrativo* 235: 93-116. https://doi.org/10.12660/rda.v235.2004.45127.

Michaelis. s.d. "Dilema." Em *Michaelis Dicionário Brasileiro da Língua Portuguesa*. Editora Melhoramentos. Acesso em 19 de dezembro de 2025. https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/dilema/.

Miranda Filho, Fábio N. de. 2019. "Legitimacy of Intelligence According to Political Thinkers". *Global Security and Intelligence Studies* 4 (1): 45-69. https://gsis.scholasticahq.com/api/v1/articles/27813-legitimacy-of-intelligence-according-to-political-thinkers.pdf.

Miller, Seumas. 2021. "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity." *Social Epistemology* 35 (3): 211-231. https://doi.org/10.1080/02691728.2020.1855484.

Miller, Greg. 2020. "The intelligence coup of the century". *The Washington Post*, 11 de fevereiro de 2020. Acesso em 13 de outubro de 2025. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

Miller, Greg, e Peter Mueller. 2020. "Compromised encryption machines gave CIA window into major human rights abuses in South America." *The Washington Post*, 17 de fevereiro de 2020. Acesso em 13 de outubro de 2025. https://www.washingtonpost.com/national-security/compromised-encryption-machines-gave-cia-window-into-major-human-rights-abuses-in-south-america/2020/02/15/bbfa5e56-4f63-11ea-b-721-9f4cdc90bc1c_story.html.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.264
ISSN 2595-4717

Monge, Yolanda. 2013. "A CIA usa infiltrados em Guantánamo". *El País*, 26 de novembro de 2013. Acesso em 13 de outubro de 2025. https://brasil.elpais.com/brasil/2013/11/26/internacional/1385486042_815869.html.

Omand, David, e Mark Phythian. 2018. *Principled spying: the ethics of secret intelligence*. Oxford: Oxford University Press.

Pellanda, Osiris Vargas. 2005. "Ética profissional na atividade de inteligência: uma abordagem jusfilosófica". *Revista Brasileia de Inteligência* 1 (1): 53-68. http://repositorio.enap.gov.br/handle/1/4642.

Rayment, Sean. 2023. "At least 21 children have been recruited by the intelligence services and police since 2015 to help snare drug dealers and terrorists". *Mailonline* 8 de julho de 2023. Acesso em 13 de outubro de 2025. https://www.dailymail.co.uk/news/article-12278473/At-21-children-recruited-intelligence-services-police-2015.html.

Reino Unido. 2022. Covert human intelligence sources, CHIS: revised code of practice (accessible), 13 de dezembro de 2022. Acesso em 13 de outubro de 2025. https://assets.publishing.service.gov.uk/media/63985c2fe90e077c2e1ce84c/Revised_CHIS_Code_of_Practice_December_2022_FINAL.pdf.

STF (Supremo Tribunal Federal). 2021. Ação Direta de Inconstitucionalidade nº 6529 MC-PETA. Supremo Tribunal Federal. Relator: Ministra Carmem Lúcia. Pesquisa de Jurisprudência, Acórdãos, 27 de maio. Acesso em 13 de outubro de 2025. https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Artigo de pesquisa

Rafael Ferro Angelo[1]
ORCiD 0000-0001-7560-4587

MATRIZ SOC DE DIFUSÃO: UMA FERRAMENTA PRÁTICA EM AUXÍLIO À VELOCIDADE INFORMACIONAL

https://doi.org/10.58960/rbi.2025.20.269

Angelo, Rafael. 2025. "Matriz SOC de difusão: uma ferramenta prática em auxílio à velocidade informacional." *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.269. https://doi.org/10.58960/rbi.2025.20.269.

Recebido em 25/03/2025
Aprovado em 04/07/2025
Publicado em 24/09/2025

1 Agente de Polícia Federal. Mestre em Avaliação e Monitoramento de Políticas Públicas pela ENAP. Especialista em Ciências Policiais pela Escola Superior da Polícia Federal. Pesquisador do grupo de pesquisa e desenvolvimento em Inteligência Policial, Análise Criminal e Estratégias de Prevenção à Criminalidade (ANP/PF). MBA Executivo em Coaching. Bacharel em Administração Estratégica.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

MATRIZ SOC DE DIFUSÃO: UMA FERRAMENTA PRÁTICA EM AUXÍLIO À VELOCIDADE INFORMACIONAL

Resumo

A nova dinâmica global, volátil, incerta, complexa e ambígua, expõe organizações a volumes crescentes de dados, redefinindo processos decisórios e reconfigurando poderes e atores, com destaque para as organizações criminosas. Além disso, embora a atividade de Inteligência adquira expressividade na interface interorganizacional, seu caráter sigiloso tem dificultado o compartilhamento oportuno de conhecimentos. Portanto, o objetivo geral do estudo é mapear os desafios relacionados à integração informacional, tendo como objetivo específico desenvolver uma ferramenta de apoio à decisão de compartilhamento de informações: a Matriz SOC, ponderando a Sensibilidade, a Oportunidade de compartilhamento e a Confiança no receptor. Os achados sugerem que seu uso possa facilitar a decisão de compartilhamento, acelerando, padronizando e reduzindo a ambiguidade na disseminação interinstitucional de conhecimentos.

Palavras-chave: Inteligência, difusão, velocidade informacional, matriz de decisão.

THE SOC SHARING MATRIX: A PRACTICAL TOOL FOR HELPING THE SPEED OF INFORMATION

Abstract

The new global dynamic, volatile, uncertain, complex and ambiguous, exposes organizations to increasing volumes of data, redefining decision-making processes and reconfiguring powers and actors, with emphasis on criminal organizations. Furthermore, although Intelligence Activity acquires expressiveness at the interorganizational interface, its confidential nature has hindered the timely sharing of knowledge. Therefore, the general objective of the study is to map the challenges related to informational integration, and the specific objective is to develop a tool to support the decision to share information: the SOC Matrix, considering Sensitivity, Opportunity of sharing and Trust [Confidence] in the receiver. The findings suggest that its use may facilitate the decision of sharing, thus accelerating, standardizing and reducing ambiguity in the interinstitutional dissemination of knowledge.

Keywords: Intelligence, sharing, speed of information, decision matrix.

LA MATRIZ SOC DE DIFUSIÓN: UNA HERRAMIENTA PRÁCTICA PARA AUXILIAR LA VELOCIDAD INFORMACIONAL

Resumen

La nueva dinámica global, volátil, incierta, compleja y ambigua, expone a las organizaciones a volúmenes crecientes de datos, redefiniendo la toma de decisiones y reconfigurando poderes y actores, con énfasis en las organizaciones criminales. Además, aunque la actividad de inteligencia adquiere expresividad como interfaz interorganizacional, su carácter confidencial ha dificultado el intercambio oportuno de conocimientos. El objetivo general es mapear los desafíos relacionados con la integración informacional, teniendo como objetivo específico desarrollar una herramienta para apoyar la decisión de compartir información: la Matriz SOC, considerando la Sensibilidad, la Oportunidad y la Confianza en el receptor. Los hallazgos sugieren que su uso puede facilitar la decisión de compartir, acelerando, estandarizando y reduciendo la ambigüedad en la difusión interinstitucional del conocimiento.

Palabras clave: Inteligencia, difusión, velocidad informacional, matriz de decisión.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Introdução

A nova dinâmica mundial, capitaneada pelas tecnologias disruptivas na era da informação e, mais especificamente, pela quarta revolução industrial como catalisadora da mudança atualmente em curso (Schwab 2017) expõe organizações e Estados a volumes e velocidades crescentes de dados e comunicações, redefinindo o tempo, as distância, as fronteiras e as relações entre pessoas, lugares e países (Bauman 2007).

De fato, uma abertura sem precedentes do comércio, das finanças, das viagens, das comunicações, do capital, da informação e da vigilância (Zuboff 2019) pode ser observada, projetando incerteza e imprevisibilidade nos níveis de tomada de decisão organizacionais, e originando ambientes globais voláteis, incertos, complexos e ambíguos (Mackey 1992). Mais recentemente, no contexto da pandemia de Covid-19 e da guerra na Ucrânia vemos, ainda, uma realidade frágil, ansiosa, não linear e incompressível, também denominada pelo acrônimo BANI (Brittle, Anxious, Non linear and Incomprehensible) (Cascio 2020).

Do ponto de vista criminal, o impacto de uma globalização negativa (Bauman 2007), fornece terreno prolífico à expansão de atividades ilícitas e organizações criminosas que, ao se aproveitarem das novas tecnologias, cadeias logísticas e da fragmentação de poderes estatais, logra êxito em se infiltrar em negócios legais, ilegais e níveis políticos, em flagrante desprezo a territórios e soberanias (GITOC 2021). Aos Estados, por sua vez, o respeito à soberania, territorialidade, igualdade política e não intervenção imposto por uma ordem westfaliana, outrora suficiente à governança global, se transforma em um confinamento político de ações e objetivos, ora ineficazes em escala global, salvo pela convergência de interesses expressa pela cooperação internacional (UNODC 2010; Visacro 2019).

No vácuo de controle global, novos atores sobressaem, como nos mostra a recente proliferação de organizações criminosas transnacionais (OCT). Convergentes em estratégias e fragmentárias em ações, tais estruturas demonstram notável adaptabilidade frente a contextos, oportunidades e ambientes, buscando o caminho de menor resistência estatal em seu objetivo primordial financeiro (Becker 1995). Nesse contexto, a dimensão informacional adquire ainda maior relevância, dada sua capacidade de subsidiar respostas estatais mais adequadas, eficientes e eficazes frente a ameaças complexas contemporâneas de múltiplos atores em um mundo cada vez mais interconectado, onde ameaças podem surgir de diversas frentes.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

O uso da atividade de Inteligência em todas as suas dimensões: nacional, de segurança pública e policial; e em todos os níveis organizacionais: político, estratégico, tático e operacional (Polícia Federal 2022); fornece metodologias críveis e úteis à difusão de dados, informações e conhecimentos e apresenta uma interface ao intercâmbio de conhecimentos entre organizações de estruturas e esferas distintas (Angelo 2022).

Consequentemente, o objetivo geral do estudo é mapear os desafios atuais para a Inteligência relacionados a uma maior integração informacional. Escrutinizando tal dinâmica, o objetivo específico é desenvolver uma ferramenta de apoio à decisão de compartilhamento de informações (Matriz SOC) que seja capaz de balancear a sensibilidade da informação, a oportunidade de seu compartilhamento e a confiança existente no receptor, com vista a melhorar a cooperação interorganizacional e a eficácia na luta contra a criminalidade organizada.

A metodologia utilizada é predominantemente qualitativa, e de caráter exploratório- explicativo (Gil 2017). Envolve a revisão bibliográfica de doutrinas, legislações e literatura nos temas de Inteligência, produção do conhecimento e metodologia de decisão multicritério.

Estruturalmente, o presente artigo está dividido em quatro partes, sendo a primeira destinada à atividade de Inteligência, em suas definições legais e doutrinárias. A segunda está destinada a reflexionar sobre o sigilo da atividade, em sua mistificação e adequação ao Estado Democrático de Direito; a relacionar fundamentos teóricos para a produção do conhecimento em suas inúmeras metodologias; e a refletir sobre a difusão do conhecimento. A terceira parte busca avaliar os tipos de conhecimento existentes, tácito e explícito, seus modos de conversão e a explicitar a metodologia GUT, que serve de base à adaptação da Matriz SOC. A quarta parte expõe a metodologia SOC de avaliação de difusão de conhecimentos. Por fim, conclui-se sobre algumas particularidades de uso e potenciais vantagens na utilização da matriz ora proposta.

A Atividade de Inteligência e o sigilo

Inúmeras são as definições doutrinárias e legais da atividade de Inteligência. A Política Nacional de Inteligência (PNI), Decreto Nº 8.793 da Câmara dos Deputados, de 29 de junho de 2016, documento de mais alto nível de orientação da atividade de Inteligência em nosso país, a define como o "exercício permanente de ações especializadas, voltadas para a produção e difusão de

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

conhecimentos, com vistas ao assessoramento (...) nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação".

Para o Sistema Brasileiro de Inteligência (SISBIN), refere-se à "atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório" (Brasil 1999).

Na Política Nacional de Inteligência de Segurança Pública (PNISP), encontramos sua definição como:

> o exercício permanente e sistemático de ações especializadas destinadas à identificação, à avaliação e ao acompanhamento de ameaças reais e potenciais no âmbito da segurança pública, orientadas para a produção e a salvaguarda de conhecimentos necessários ao processo decisório (...) e das ações destinadas à prevenção, à neutralização e à repressão de atos criminosos de qualquer natureza que atentem contra a ordem pública, a incolumidade das pessoas e do patrimônio (Brasil 2021).

Por sua vez, em âmbito de segurança nacional, para o Ministério da Defesa, em sua Doutrina de Operações Conjuntas, temos como propósito da atividade de Inteligência:

> assessorar o processo decisório de autoridades políticas e militares, além de apoiar o planejamento e a condução de operações militares nas situações de paz, crise ou conflito. Isto é conseguido através da difusão de conhecimentos oportunos, adequados e precisos em conformidade com os interesses políticos, estratégicos, operacionais e táticos (Defesa 2011b, 11).

Do exposto, é possível verificar que, embora cada instituição formule o conceito de Inteligência com base em particularidades e nomenclaturas inerentes a seus contextos internos e áreas de atuação, a atividade possui características essenciais, que se repetem ao longo dos textos: permanente, especializada, de assessoramento e em diversos níveis e áreas de atribuição.

Por permanente, entende-se o papel da Inteligência em prover expertise de longo prazo, enquanto instituição de Estado, em um repositório informacional estável, que ultrapassa momentos políticos e governos (Cepik 2003; Lowenthal 2009).

É especializada, pois se utiliza de metodologia e pessoal próprios, com uma doutrina mínima comum, que prevê a obtenção, produção, difusão e salvaguarda de conhecimentos, por meio de coleta, processamento e avaliação

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

de informações, que deverão ser difundidos. À Atividade de Contrainteligência recai o papel de salvaguarda dos conhecimentos produzidos, métodos, instalações e pessoal (ABIN 2023; Brasil 2021).

Com relação ao assessoramento ao processo decisório, em caráter consultivo, temos que gestores necessitam constantemente reduzir as incertezas associadas à tomada de decisão com conhecimentos situacionais, sendo esta a principal finalidade da atividade (Lowenthal 2009). Ocorre, portanto, em todos os níveis organizacionais: político-estratégico, na elaboração de políticas e planos internacionais e nacionais; tático, na elaboração de planos e ações setoriais ou operacional, envolvendo a execução de procedimentos e rotinas (Polícia Federal 2022).

Na consecução de sua finalidade, a atividade de Inteligência deve obedecer, ainda, a certas normas, princípios e pressupostos norteadores de sua conduta, a começar pela estrita obediência ao ordenamento jurídico e sistema constitucional brasileiro, uma vez que exercida no seio de um Estado Democrático de Direito.

Outros pressupostos envolvem o exercício de atividade exclusiva de Estado; de assessoramento oportuno; de busca por resultados abrangentes e de grande amplitude; que priorizem a simplicidade, objetividade e economia de meios e recursos; imparcial e segura, e sujeita a controle e supervisão por órgãos diversos; com relações de cooperação que possibilitem otimizar esforços (ABIN 2023; Cepik 2003; Lowenthal 2009; Polícia Federal 2022).

Além dos princípios e subprincípios mencionados anteriormente, merece destaque a característica responsável pelo grande secretismo e mitificação em torno da Inteligência: o sigilo. Inerente às suas atividades, como forma de obtenção de dados negados , ou na preservação de suas ações, métodos, processos, profissionais e fontes (Brasil 2016), o sigilo é visto como uma das "principais razões para haver agências de inteligência" (Lowenthal 2009, 27), permitindo desenvolver vantagens informacionais em auxílio à formulação de políticas e a tomada de decisão.

Neste ponto chama à atenção que, ao contrário do que possa inicialmente parecer, o sigilo da atividade não encontra óbice direto em garantias constitucionais de acesso à informação, como aquelas contidas na Constituição Federal de 1988 (Brasil 1988), em seu Art. 5° XIV, XXXIII, XXXIV, ou mesmo no princípio democrático de transparência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Todavia, essa adequação requer que sejam observados reservas de seus métodos e conteúdos. Sobre este aspecto, temos que:

> De modo geral, as chamadas atividades-meio do Estado (em que se incluem as atividades de provimento de informações para a tomada de decisões) seriam, nesse sentido, transparentes para os cidadãos, que olharia através delas para visualizar e controlar os atos de governantes em relação aos fins consolidados desejáveis pela comunidade política (...) Na verdade, o segredo governamental e as atividades de inteligência são compatíveis com o princípio da transparência somente quando a justificação de sua existência puder ser feita, ela própria, em público (Cepik 2003, 16-17).

Dessa forma, como justificação pública de existência e sigilo da atividade, encontramos na Lei 12.527/11, Lei de acesso à informação, em seu Artigo 24, um rol taxativo relacionando as possibilidades de classificação da informação quanto a seu grau e prazos de sigilo em função de sua imprescindibilidade à "segurança da sociedade ou do Estado" (Brasil 2011).

De forma sintética, o referido diploma relaciona informações referentes a soberania e territorialidade; relações internacionais; população; aspectos econômicos e monetários; Forças Armadas; pesquisa; desenvolvimento científico ou tecnológico; sistemas, bens, instalações e áreas de interesse estratégico; instituições e altas autoridades nacionais ou estrangeiras e seus familiares e, de maior relevância a este estudo, aquelas que possam:

> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações (Brasil 2011).

Verifica-se que o sigilo inerente à atividade de inteligência não afronta o ordenamento jurídico nacional, notadamente com relação a direitos de acesso à informação e transparência. Entretanto, como exposto, é necessário que o secretismo encontre justificação em sua utilidade e conteúdo, e não em sua forma, introduzindo um viés de aferição do quanto a disseminação de certos conhecimentos se mostrem capazes de "comprometer atividades" (Brasil 2011) da Inteligência em específico.

Fundamentos teóricos para a produção e difusão do conhecimento

Cabe à Inteligência, enquanto atividade especializada, o desenvolvimento de doutrinas e métodos de produção de conhecimento e aplicação próprios, amparados nas particularidades de sua atuação como atividade de Estado, na função de "auxiliar no entendimento da transformação qualitativa da informação em conhecimento e a presença de atores distintos, como os usuários

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

da informação" (Cepik 2003, 32).

Nesse contexto, inúmeras também são as metodologias que descrevem a produção de seu conhecimento, com nomenclaturas variando desde Metodologia de Produção do Conhecimento de Inteligência (MPC) para a ABIN (ABIN 2023) até Ciclo de Inteligência para o Ministério da Defesa (Defesa 2011a), cada qual com particularidades inerentes à esfera, contextos e âmbitos no qual ocorrem.

Para a ABIN, a MPC prevê a aplicação de seis fases não necessariamente ordenada ou com limites precisos: planejamento; reunião; avaliação; integração e interpretação; formalização e validação; difusão e resultados (ABIN 2023, 107), representada no modelo que segue (Figura 1).

Figura 1
Metodologia de Produção do Conhecimento de Inteligência (MPC)

Fonte: ABIN (2023, 108).

Na fase de planejamento serão definidos o escopo do trabalho, suas condicionantes de produção, como o usuário, sua finalidade, os limites temporais e prazo de entrega, o nível de sigilo, formatos de difusão, expectativas e propositura de equipe. Destacam-se, ainda, a definição do assunto e dos aspectos essenciais conhecidos e a conhecer

A fase de reunião envolve a coleta, reunião e preparo, segundo o planejamento, de dados, informações, conhecimentos ou outros conhecimentos de inteligência no objetivo de responder aos aspectos essenciais a conhecer

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

definidos no planejamento. Na avaliação, os insumos anteriormente coletados serão avaliados por um profissional de inteligência quanto à sua validade, pertinência, significância e credibilidade.

A próxima etapa, de integração e interpretação envolve analisar, integrar e interpretar as frações de conhecimento avaliadas de modo a construir argumentos e conclusões sobre as evidências apresentadas que possam esclarecer o assunto. O conhecimento de inteligência, então, passa à etapa de formalização e validação, onde ocorre a revisão, formatação final e sua validação analítica e técnica antes da difusão, podendo incluir revisão gramatical, lógica interna, adequação à linguagem e metadados.

Por fim, na etapa de difusão e resultados, o conhecimento de inteligência anteriormente reunido, avaliado, integrado e interpretado, formalizado e validado é difundido a seus usuários, com seus resultados sendo avaliados com vistas a melhorar os ciclos subsequentes de produção (ABIN 2023).

De modo assemelhado, a doutrina de operações conjuntas do Ministério da Defesa (Defesa 2011a) define ciclo de inteligência como um processo destinado a atender às Necessidades de Inteligência (NI), composto de quatro fases (Figura 2).

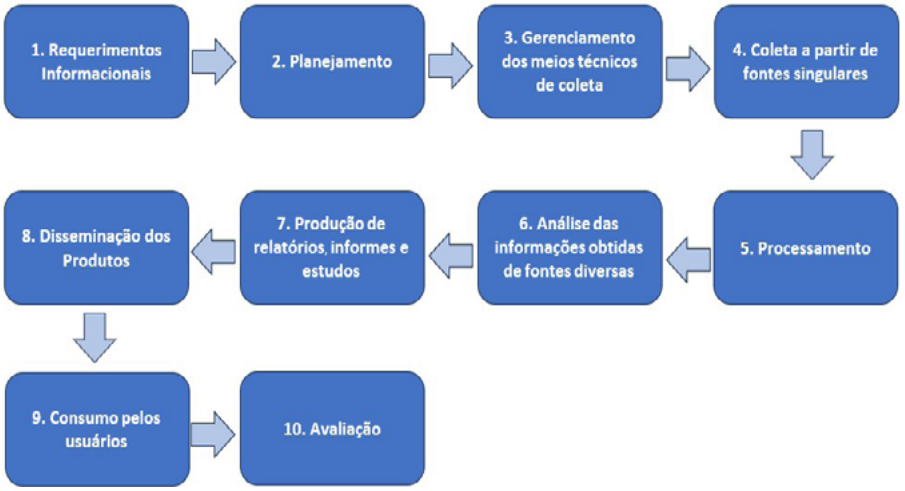
Figura 2
Ciclo de inteligência na doutrina de operações conjuntas do Ministério da Defesa

Fonte: elaborado pelo autor (2024), com base em Defesa (2011a).

Resumindo a diversidade doutrinária existente, Cepik (2003) salienta a presença recorrente de 10 etapas principais nas descrições de ciclos de Inteligência, a saber: requerimentos informacionais; planejamento; gerenciamento dos meios técnicos de coleta; coleta a partir de fontes singulares; processamento; análise das informações obtidas de fontes diversas; produção de relatórios, informes e estudos; disseminação dos produtos; consumo pelos usuários e avaliação, podendo ser representadas como na Figura 3.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Figura 3
Ciclo convencional da Inteligência



Fonte: elaborado pelo autor (2024), com base em Cepik (2023, 32).

De uma comparação das doutrinas descritas, é possível verificar semelhanças e complementariedades, embasando a elaboração neste estudo de um modelo genérico para o ciclo de Inteligência, com base na bibliografia selecionada, composto por quatro atividades de direcionamento: direção política e planejamento, coleta ou reunião, análise ou processamento e disseminação ou difusão; e uma etapa de avaliação, que retroage em melhoria contínua ao processo (Figura 4).

Figura 4
Modelo genérico para o ciclo de Inteligência

Fonte: elaborado pelo autor (2024).

Dos modelos analisados, é possível observar a presença de uma etapa específica de difusão e/ou disseminação como parte da comunicação do conhecimento produzido, permitindo ao receptor retroagir, por meio da elaboração de avaliação e feedback. Esse ciclo, caracterizado por um fluxo contínuo de informações, se mostra essencial para a melhoria da qualidade do conhecimento compartilhado.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

No entanto, a atividade de Inteligência demanda um permanente balanceamento entre a disseminação de seus resultados e sua necessidade principiológica de secretismo, impondo desafios adicionais na integração informacional entre atores de diferentes organizações. A interseção entre tais necessidades representa um dilema constante na atividade. Se, por um lado, a divulgação de informações em momento oportuno permite a adoção de medidas preventivas e/ou corretivas por parte do usuário, por outro, a exposição prematura ou inadequada pode comprometer operações, revelar fontes sensíveis ou mesmo gerar desinformação e confusão.

Dessa forma, um equilíbrio entre possíveis ganhos oriundos da disseminação de conhecimentos e a necessidade de seu sigilo e compartimentalização devem ser sempre avaliados, demandando tempo na decisão e utilização dos corretos canais de comunicação. A esse respeito, Cepik argumenta que

> problemas de agilidade são inerentes à própria natureza das atividades de serviços de inteligência, em função da contradição potencial entra a demanda por aumento das informações disponíveis sobre determinado assunto e/ou indivíduo e a simultânea necessidade de protegê-las da indiscrição alheia (Cepik 2003, 9).

Diante de tal dilema, dois cenários possíveis se apresentam. No primeiro, a necessidade de sigilo se mostra maior do que a necessidade de tornar o conhecimento oportuno. Nesse contexto, o sigilo e a compartimentalização adquirem precedência, seja por razões estratégicas ou riscos operacionais.

O segundo cenário, por outro lado, ocorre quando a necessidade de tornar o conhecimento acionável se sobrepõe ao sigilo, ou seja, quando a disseminação é justificada por ameaças iminentes, demandas institucionais ou oportunidades estratégicas que possam ser aproveitadas por diferentes atores envolvidos no processo decisório.

Embora a importância de tal interface no ambiente informacional para a produção de conhecimento útil seja amplamente reconhecida, sua aplicabilidade não tem sido imediata. Além disso, o processo está longe de ser trivial, exigindo não apenas a infraestrutura adequada para coleta, análise e disseminação de informações, mas também a coordenação entre os diferentes atores envolvidos, com significativos obstáculos técnicos e organizacionais que podem comprometer a eficiência do fluxo informacional.

Como entraves, pragmaticamente, é possível elencar algumas causas, como a divergência de objetivos entre nacionalidades, esferas, órgãos e funções distintas; a prevalência de ego institucional; brigas políticas por recursos,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

atribuições e projeção de poder; a diversidade de procedimentos técnico-doutrinários, que pode criar barreiras operacionais entre diferentes entidades; dificuldades na produção do conhecimento dentro do tempo oportuno (*timing* informacional); a tendência ao assessoramento se tornar um fim em si mesmo, e não um meio; a dificuldades em gerar sinergia entre setores e funções distintas; dentre muitos outros. Nesse escopo, um ponto crítico que merece destaque diz respeito à necessidade de criação de canais de confiança entre os diferentes agentes envolvidos no processo, vez que sua ausência pode resultar em resistência ao compartilhamento, comprometendo a qualidade da cooperação interinstitucional.

Há, assim, uma crescente demanda de organizações envolvidas no combate à criminalidade transnacional e interestadual em melhorar suas interfaces informacionais, por motivos diversos. Além disso, um aprofundamento em teorias de produção e compartilhamento de conhecimentos faz-se necessário, buscando um melhor entendimento de ambientes propícios à sinergia interinstitucional. Inicialmente, temos que sinergia pode ser entendida como:

> trabalho conjunto (...) [quando] duas ou mais causas produzem, atuando conjuntamente, um efeito maior do que a soma dos efeitos que produziriam atuando individualmente (...) Assim, a sinergia constitui o efeito multiplicador das partes de um sistema que alavancam o seu resultado global. A sinergia é um exemplo de emergente sistêmico: uma característica do sistema que não é encontrada em nenhuma de suas partes tomadas isoladamente (Chiavenato 2004, 424-425).

Portanto, é na união de instituições distintas que temos o potencial de criação de um emergente sistêmico potencialmente capaz de antagonizar redes de ilícitos organizadas. No entanto, para tal, é imperativo que se promova melhoria significativa nos canais de comunicação, de forma a tornar o conhecimento produzido acessível e utilizável de maneira eficaz, em meio à confiança mútua entre os envolvidos.

Espaços de produção de conhecimento e metodologia GUT

No âmbito desta questão, Nonaka e Takeuchi (1997) descrevem a coexistência de dois tipos de conhecimento, tácito e explícito, cuja conversão entre si ocorre de modo dinâmico, por meio de interações sociais, em quatro possibilidades: Socialização, Externalização, Combinação e Internalização, dando origem ao que denominam de modelo "SECI" (figura 5).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Figura 5
Modelo SECI

Fonte: adaptado de Nonaka & Takeuchi (1997, 69).

Do modelo, pode-se destacar a importância da condução de processos de socialização entre as organizações, o que ocorre, em meio às atividades de segurança, notadamente em treinamentos conjuntos e continuados (Angelo 2022). Outro ponto de destaque, essencial a este estudo, diz respeito à externalização de conhecimentos produzidos, sendo este um dos papéis primordiais da atividade de Inteligência em contextos interorganizacionais estatais.

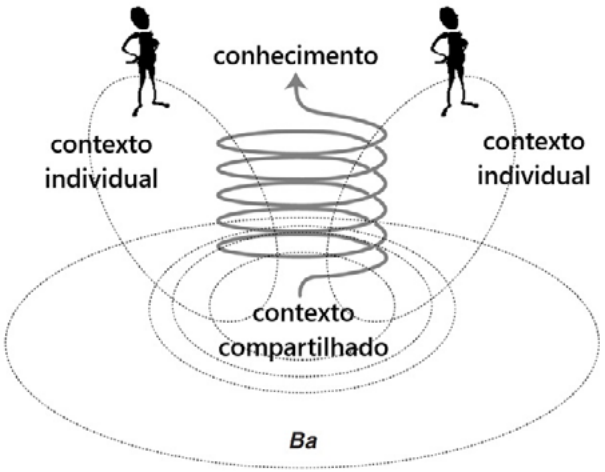
Ocorre que, diferentemente de interações humanas comuns, a criação de conhecimento entre organizações necessita de ambientes e contextos característicos para que possa ocorrer. Desta forma, Nonaka, Toyama e Konno (2000), em complemento a seu estudo inicial, defendem a criação de espaços específicos destinados à conversão e compartilhamento de conhecimento, sejam eles individuais ou coletivos, aos quais denominam de "Ba":

> plataforma para a "concentração de recursos" da organização de ativos de conhecimento e as capacidades de intelectualização entre processos de criação do conhecimento. Ba coleta o conhecimento aplicado da área e o integra. (Nonaka, Toyama e Konno 1998, 41).

O modelo pode ser mais bem compreendido por meio de uma representação visual (Figura 6).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Figura 6
"Ba" como um contexto compartilhado em movimento



Fonte: adaptado de Nonaka, Toyama e Konno (2000, 14).

Resulta que a criação e o compartilhamento do conhecimento podem ocorrer de modo satisfatório, ou não, a depender da adequação destes ambientes ("Ba") ao modo de conversão do conhecimento adotado, com impacto direto nos níveis de confiança (solicitude) obtidos naquela troca informacional em específico. Logo, é essencial que indivíduos envolvidos em relações de comunicação possuam intencionalidade compartilhada, e que haja um canal com a devida confiança estabelecida (Von Krogh, Ichijo e Nonaka 2001).

Corroborando esse pensamento, não é possível intencionalmente criar confiança mútua, mas esta pode ser estimulada por meio de estruturas e contextos adequados (Holanda, Francisco e Kovaleski 2009), quando organizações compartilham experiências e conhecimentos em torno de um conceito comum. Isso é particularmente relevante em instituições voltadas para o combate conjunto e sistêmico da criminalidade organizada (Angelo 2022). Sobremaneira:

> [o] uso do conhecimento é diferente daquele dos recursos tangíveis. Ao usar recursos tangíveis é preciso distribuir eficientemente de acordo com as funções e objetivos. Conhecimento, contudo, é intangível, sem fronteiras, e dinâmico, e se não for usado em um momento específico em um local específico, não tem valor. Portanto, o uso do conhecimento requer a concentração dos recursos do conhecimento em um determinado espaço e tempo (Nonaka e Konno 1998, 41).

O princípio da oportunidade em Inteligência é, portanto, essencial à capacidade de tornar o conhecimento produzido útil, independente do nível de as-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

sessoramento realizado. Nesse sentido, é crucial uma melhora na velocidade de compartilhamento de dados entre instituições envolvidas na repressão a crimes, no entendimento de ser esse um contexto que demanda maior permissividade informacional.

Porém, nessa demanda, é essencial que não sejam desconsiderados os princípios básicos norteadores da atividade, notadamente aqueles relacionados ao sigilo, em determinados casos. Nessa direção, como relatado anteriormente, a conformação do conteúdo do resultado da atividade à justificação pública de sigilo deverá sempre ser realizada, tomando por óbvio que conteúdos secretos e sigilosos deverão atender a seu grau formal de classificação.

Com relação aos demais conteúdos, com enfoque pragmático, é possível o desenvolvimento e aplicação de técnicas capazes de avaliar e balancear a sensibilidade do conhecimento produzido, a oportunidade de seu uso e o nível de confiança existente por meio de uma Análise Multicritério de Decisão (MCDA) adaptada dos fundamentos teóricos da metodologia GUT.

A matriz de priorização GUT pode ser descrita como uma ferramenta da área de qualidade na solução de problemas, por meio de priorização de ações, dentre os cursos de ações disponíveis à organização (Kepner e Tregoe 1981). Para tal, se utiliza dos atributos de gravidade, urgência e tendência, que dão origem a seu acrônimo, na seleção do caminho com menor impacto adverso potencial.

No contexto da atividade de Inteligência e da segurança institucional, a matriz GUT tem se tornado uma ferramenta valiosa para orientar a priorização de informações, tomada de decisão e recursos institucionais. Seu uso contribui para decisões mais fundamentadas e equilibradas, permitindo um aprimoramento estratégico ao reduzir a subjetividade de tomada de decisões, favorecendo um processo mais transparente e fundamentado.

Embora possua aplicabilidade nas ciências administrativas na priorização de ações; na etapa de planejamento das ações do ciclo PDCA (*Plan, Do, Check, Act*) a ferramenta permite uma visão ampla de possíveis alternativas em nível executório, orientando a ação e atividade finalística institucional (Andrade, Reis e Sanches 2022). Portanto, viabiliza um diagnóstico capaz de sugerir medidas referentes à difusão de conhecimentos interinstitucionais.

O acrônimo GUT se refere a seus três critérios fundamentais: Gravidade, Urgência e Tendência, utilizados na avaliação e hierarquização de questões

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

organizacionais. Gravidade (G) se refere à intensidade de risco ou danos que podem ocorrer caso um problema não seja tratado adequadamente, considerando o impacto potencial da decisão sobre os objetivos, resultados, processos e pessoas.

O critério de urgência (U) se relaciona ao tempo disponível à ação organizacional antes que os efeitos negativos do problema ou da ausência de decisão se manifestem. Avalia, portanto, a necessidade temporal de resposta, determinando se a situação requer uma intervenção imediata ou se pode ser postergada. O critério de tendência (T) se refere ao prognóstico de desenvolvimento do problema na ausência de intervenção. Considera a probabilidade de agravamento da situação no tempo, caso nenhuma ação ou decisão seja tomada no tempo presente.

A aplicação da matriz demanda a atribuição de notas para cada um dos três critérios descritos, geralmente por intermédio de uma escala de Likert em cinco graus: 1 a 5, sendo 1 a menor gravidade, urgência ou tendência e 5 a maior. As notas podem ser atribuídas por apenas uma pessoa ou por um grupo de especialistas através dos métodos Delphi ou Mini-Delphi (Andrade, Reis e Sanches 2022), sendo utilizadas rodadas sucessivas de convencimento ou a média de suas notas como nota final para os critérios.

Essa modalidade possui o adicional de remover a subjetividade e possíveis vieses individuais e pessoais da equação, ao diluí-los entre as outras notas. Após a avaliação individual de cada critério, o índice final da Matriz GUT pode ser obtido pela multiplicação das pontuações de Gravidade, Urgência e Tendência (G x U x T). Organizacionalmente, espera-se que os resultados com índices mais altos sejam tratados com maior prioridade através do direcionamento de recursos e esforços.

De todo o exposto, no objetivo específico do estudo de desenvolver uma ferramenta de apoio à decisão de compartilhamento de informações integrando metodologias específicas, os princípios da atividade de inteligência, e a confiança oriunda de contextos de compartilhamento de conhecimento com fins de atuação em redes de instituições interestaduais e internacionais distintas, o presente artigo sugere a utilização de uma matriz GUT adaptada à difusão, ora denominada de ‘‘Matriz SOC’’, com base em três critérios, definidos conforme o Quadro 1.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Quadro 1
Critérios para análise da Matriz SOC

Critério	O que deve ser considerado na análise
Sensibilidade da informação (S)	Critério que avalia o grau e necessidade de sigilo dos dados, informações e conhecimentos obtidos.
Oportunidade da difusão (O)	Critério que avalia a necessidade temporal de difusão dos dados, informações e conhecimentos obtidos, com base no uso potencial em atividades de enfrentamento à criminalidade organizada.
Confiança no receptor (C)	Critério que avalia a confiança existente no receptor da mensagem, com base na probabilidade de uso correto e compartimentalização.

Fonte: Elaborado pelo autor (2024).

A Matriz SOC

A avaliação por meio da Matriz SOC objetiva assessorar a tomada de decisão sobre o compartilhamento (ou não) de dados, informações e conhecimentos entre instituições, garantindo potencial celeridade em uma resposta sistêmica destas instituições em resposta à criminalidade organizada transnacional e entre estados da federação.

Como ferramenta de auxílio à elaboração da Matriz, optou-se por utilizar a metodologia GUT contextualizando sua aplicação à temática do estudo, pela modificação de seus critérios para Sensibilidade da informação (S), Oportunidade da difusão (O) e nível de Confiança existente no receptor (C), auxiliando o processo decisório em potencial incremento à velocidade de resposta de múltiplos atores estatais à dinamicidade criminal.

Identificada tal preferência por critérios, o ordenamento de priorização por pesos envolveu o reconhecimento de que a Sensibilidade da informação (C1) possui maior relevância na avaliação de sua difusão, seguida pela Confiança no receptor (C3) e oportunidade de difusão (C2), atendendo ao seguinte ordenamento:

$$C1 > C3 > C2$$

A atribuição de peso a cada um dos critérios foi traduzida com uso da ferramenta Rank Order Centroid (ROC) adaptada, com pesos: 1, ½ e ¼. Sobremaneira, do ordenamento e atribuição de pesos temos:

- Sensibilidade da informação (C1), com peso 1;

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

- Oportunidade de difusão (C2), com peso ¼, ou 0,25;

- Confiança no receptor (C3), com peso ½, ou 0,50.

Na aplicação da metodologia, os critérios de Sensibilidade da informação (C1), Oportunidade da difusão (C2) e Confiança no receptor (C3) devem ser avaliados individualmente por 3 (três) especialistas com base em uma metodologia Mini Delphi, simplificação da técnica estruturada preditiva Delphi utilizada para a troca de informação entre painelistas anônimos em um número de interações (Rowe e Wright 2001).

O uso de três especialistas se destina a mitigar possíveis vieses pessoais na definição da importância de cada critério, e as valorações passíveis de atribuição estão baseada em um acordo semântico elaborado em uma escala Likert em 5 graus (Quadro 2):

Quadro 2
Acordo Semântico dos critérios da Matriz SOC

	Semântica	Sensibilidade	Oportunidade	Confiança
1	Nenhum	Não é sensível	Não é oportuno	Não é confiável
2	Muito pouco	Muito pouco sensível	Muito pouco oportuno	Muito pouco confiável
3	Pouco	Pouco sensível	Pouco oportuno	Pouco confiável
4	Normal	Sensível	Oportuno	Confiável
5	Muito	Muito sensível	Muito oportuno	Muito confiável

Fonte: Elaborado pelo autor.

Observe-se que cada critério contido na tabela de acordo semântico corresponde a uma pontuação quantitativa, de 1 a 5. Desta forma, as notas finais de cada um dos critérios são a média aritmética simples (μ) resultante das três notas atribuídas pelos especialistas para cada um dos três critérios, multiplicado pelos pesos relacionados a cada critério em específico, sendo C1 = 1; C2 = 0,25 e C3 = 0,50. Seguem as fórmulas de cálculo final para cada um dos critérios.

$$S = (\text{Valor S Esp. 1} + \text{Valor S Esp. 2} + \text{Valor S Esp. 3}) / 3 \times 1$$

$$O = (\text{Valor O Esp. 1} + \text{Valor O Esp. 2} + \text{Valor O Esp. 3}) / 3 \times 0{,}25$$

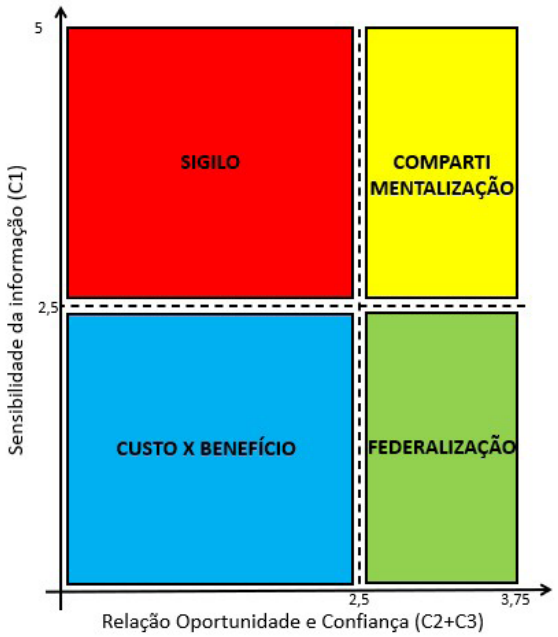
$$C = (\text{Valor C Esp. 1} + \text{Valor C Esp. 2} + \text{Valor C Esp. 3}) / 3 \times 0{,}50$$

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

As pontuações finais obtidas deverão, então, ser utilizadas para situar o resultado obtido dentro de uma plotagem bidimensional em um gráfico cartesiano composto, no eixo das abscissas (y) pela pontuação final de S. (Sensibilidade da Informação) e, no eixo das ordenadas (x): pelo somatório entre as pontuações finais de O. (Oportunidade da difusão) e C. (Confiança no receptor).

Temos, portanto, o intervalo entre 1 e 5 para o eixo "y", sendo 2,5 a sua mediana; e o intervalo entre 0,75 e 3,75 para o eixo "x", sendo mantido 2,5 como limiar de referência por opção metodológica, o que permite elaborar uma plotagem cartesiana em quatro quadrantes, cada uma atribuída a uma medida de tratamento: avaliação de custo X benefício; sigilo; compartimentalização ou federalização do conhecimento, nos moldes do modelo que segue:

Figura 7
Quadrantes da Matriz SOC



Fonte: elaborado pelo autor (2024).

- Sigilo: informação com alta sensibilidade (S ≥ 2,5) e cenário com baixa relação de oportunidade e confiança (O + C < 2,5). Baixa probabilidade de aproveitamento da informação de modo oportuno demandam recursos organizacionais em sua produção que poderiam ser mais bem utilizados em outras atividades. De mesmo modo, uma baixa confiança no receptor representa riscos associados ao compartilha-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

mento da informação que, quanto mais valiosa, menos deverá ser compartilhada. Neste cenário, a atividade de Inteligência deve prezar por manter em sigilo a informação, não realizando sua disseminação a menos que seja necessária.

- Compartimentalização: informação com alta sensibilidade (S ≥ 2,5) e cenário com alta relação de oportunidade e confiança (C2 + C3 ≥ 2,5). Neste cenário pode ser considerado haver um nível de confiança e oportunidade suficiente à difusão dos conhecimentos, porém, com amparo na alta sensibilidade da informação, sua interface deve prezar pela compartimentalização, devendo ser repassada apenas a quem tenha a necessidade de conhecê-la, através de níveis e canais corretos de comunicação.

- Federalização: informação com baixa sensibilidade (S < 2,5) e cenário com alta relação de oportunidade e confiança (C2 + C3 ≥ 2,5). O baixo nível de sensibilidade da informação associado a uma alta relação entre confiança e oportunidade faz com que mais benefícios sejam obtidos do compartilhamento e federalização do conhecimento do que de seu sigilo e compartimentalização. Esse é o cenário ideal requerido por atividades que demandam uma atuação coordenada a nível interestadual e internacional, dentro de um conceito de segurança multidimensional, pela sua capacidade em tornar o assessoramento da função informacional da inteligência plenamente acionável pelas equipes a nível operacional e local (Angelo 2022).

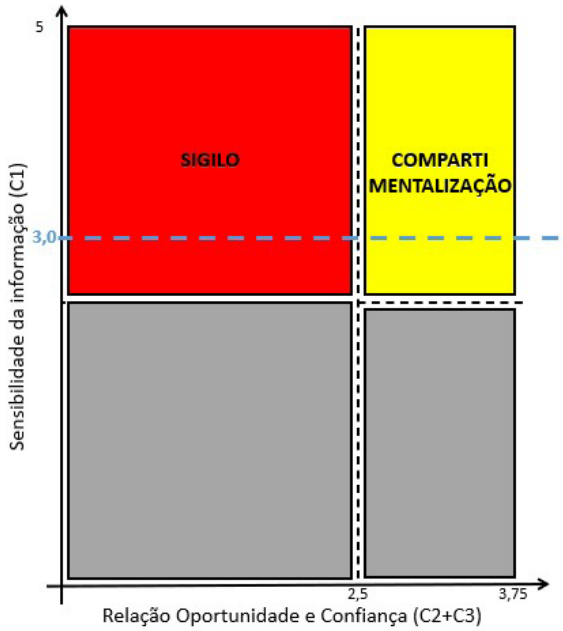
- Análise de custo X benefício: informação com baixa sensibilidade (S < 2,5) e cenário com baixa relação de oportunidade e confiança (C2 + C3 < 2,5). A baixa sensibilidade e baixa relação de confiança e oportunidade deste cenário fazem com que a difusão do conhecimento deva ser avaliada a depender de cada caso concreto individualmente, uma vez que é possível haver o vazamento do conhecimento que, por sua vez, não representa uma grande perda do ponto de vista do secretismo da atividade.

Para ilustrar a aplicabilidade da Matriz SOC, considere-se uma situação hipotética envolvendo uma operação conjunta em faixa de fronteira, com a participação de órgãos de persecução penal federais, aduaneiros e forças estaduais. Suponha que um relatório de inteligência identifique movimentações financeiras suspeitas atribuídas a uma organização criminosa transnacional, com informações variando de ‘‘pouco sensível’’ (S=3) a ‘‘muito sensível’’ (S=5).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Como esse critério possui peso 1, e adota valores sempre maiores do que 2,5 no exemplo exposto; com base na Matriz SOC, haveriam apenas duas recomendações passíveis de adoção: manutenção de sigilo, ou compartimentalização, dependendo da valoração da Oportunidade da difusão (O) e Confiança no receptor (C), como demonstra a Figura 8.

Figura 8
Plotagem de quadrantes da Matriz SOC no exemplo em que a sensibilidade varia de "pouco sensível" (S=3) a "muito sensível" (S=5).



Fonte: elaborado pelo autor.

Pressuponha-se, adicionalmente, que o grau de confiança no receptor (C) entre as instituições envolvidas na atividade ainda esteja em estágios iniciais, e seja "pouco confiável" (C = 3, com peso 0,50). Nesse sentido, a decisão recairia sobre a avaliação da Oportunidade em se difundir o conhecimento (O, com peso 0,25).

Observe-se que, no caso exemplificativo, para oportunidades consideradas de "não oportunas" (O = 1) a "pouco oportunas" (O = 3), a recomendação seria pelo sigilo; no entanto, para casos em que a opção de compartilhar se mostre "oportuna" (O = 4) ou "muito oportuna" (O = 5), o escopo se altera, recomendando-se a difusão compartimentalizada do conhecimento (compartimentalização). O Quadro 3 ilustra valores passíveis de obtenção

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

na aplicação da matriz

Quadro 3
Valores da Matriz SOC no exemplo

		Valores de O (peso 0,25)				
		1	2	3	4	5
Valores de C (peso 0,5)	1	0,75	1,00	1,25	1,50	1,75
	2	1,25	1,50	1,75	2,00	2,25
	3	1,75	2,00	2,25	2,50	2,75
	4	2,25	2,50	2,75	3,00	3,25
	5	2,75	3,00	3,25	3,50	3,75

Fonte: Elaborado pelo autor.

Do exposto temos que, mesmo diante de uma situação que exija resposta rápida, a ausência de confiança entre os atores (C) e o grau de sensibilidade da informação (S) impõem limites à sua difusão generalizada. A medida adequada, portanto, recairia na avaliação da oportunidade em compartilhar o conhecimento (O), mitigando riscos institucionais e operacionais.

A aplicação da Matriz SOC, portanto, permite melhor identificar esse ponto de equilíbrio de modo estruturado, orientando escolhas que preservem tanto a eficácia da ação quanto a integridade da informação como instrumento de apoio à decisão estratégica, sobretudo em contextos de elevada complexidade institucional.

Conclusão

Do exposto, a aplicação da matriz SOC proporciona um framework padronizado para a classificação e disseminação do conhecimento, reduzindo a ambiguidade decisória, potencialmente acelerando a velocidade informacional entre instituições, fator essencial em um ambiente de segurança que exige respostas ágeis a ameaças emergentes, como a criminalidade complexa contemporânea.

Inobstante, é crucial destacar que uma avaliação inadequada sobre o sigilo a ser atribuído ao conhecimento possui o potencial para prejudicar a confiança existente entre pessoas e instituições sendo, portanto, demandada especial atenção à correta avaliação de cenário, a depender do caso concreto. De modo similar, a classificação de uma instituição ou órgão congênere como

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

de "baixa confiança" em âmbito institucional deve ser tratada apenas internamente, sob pena de ocasionar uma crise entre as instituições.

Ademais, a integração dos critérios SOC em medidas de tratamento de sigilo, compartimentalização, custo-benefício e federalização deve ser cuidadosamente equilibrada, na promoção de uma cultura de inteligência que se mostre ao mesmo tempo segura e eficiente. A contínua revisão dos resultados da metodologia proposta é igualmente importante para a manutenção da integridade e da eficácia das avaliações realizadas.

Em síntese, a gestão adequada das informações e do conhecimento em inteligência é vital para a segurança nacional e para a confiança mútua entre instituições. Nessa seara, a utilização da Matriz SOC em auxílio à avaliação de difusão possui potencial para captar mudanças no ambiente, atraindo maior robustez e velocidade ao fluxo informacional, em contraposição a organizações criminosas. Sob outro escopo, possui a capacidade de indicar o fortalecimento do canal de confiança como demandas intrainstitucionais.

Por fim, a adoção da ferramenta possibilita às organizações estabelecerem uma linguagem comum para avaliar e classificar de riscos na comunicação, na direção de um entendimento mútuo. Por certo, uma abordagem compartilhada acelera a circulação de informações críticas, permitindo que as partes interessadas identifiquem rapidamente questões prioritárias e alinhem suas ações de forma coordenada, em uma maior capacidade coletiva de resposta aos desafios de segurança nacional e pública frente às situações adversas das novas dinâmicas criminais.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Referências

Agência Brasileira de Inteligência (ABIN). 2023. Doutrina da Atividade de Inteligência. Brasília: Abin. https://www.gov.br/Abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

Andrade, Felipe S. de, Alessandro R. dos Reis e Marcelo C. Sanches. 2022. "Análise de Risco de pessoa: a convergência das medidas de proteção com os procedimentos de segurança adequados." *Revista Susp* 1 (2). https://doi.org/10.56081/2763-9940/revsusp.v1i2.a7.

Angelo, Rafael Ferro 2022. "Segurança multidimensional nas fronteiras brasileiras: a capacidade disruptiva do programa V.I.G.I.A." *Revista Brasileira de Ciências Policiais* 13 (10): 355–94. https://doi.org/10.31412/rbcp.v13i10.968.

Barron, H., and B. E. Barret. 1996. "Decision Quality Using Ranked Attribute Weights." *Management Science* 42 (11): 1515–23.

Bauman, Zygmunt. 2007. *Tempos Líquidos*. Rio de Janeiro: Jorge Zahar.

Becker, Gary. 1995. *The Economics of Crime*. Richmond, VA: Federal Reserve Bank of Richmond.

Brasil. 1988. *Constituição da República Federativa do Brasil*. https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Brasil. 1999. *Lei Nº 9.883, de 07 de dezembro de 1999*. Diário Oficial da União, 8 de dezembro. http://www.planalto.gov.br/ccivil_03/leis/l9883.htm.

Brasil. 2011. *Lei Nº 12.527, de 18 de novembro de 2011*. Diário Oficial da União, 18 de novembro. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

Brasil. 2016. *Decreto Nº 8.793, de 28 de junho de 2016*. Diário Oficial da União, 29 de junho. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8793.

Brasil. 2021. *Decreto Nº 10.777, de 24 de agosto de 2021*. Diário Oficial da União, 25 de agosto. https://www.in.gov.br/web/dou/-/decreto-n-10.777-de-24-de-agosto-de-2021-340717199.

Cascio, Jamais. 2020. "Facing the age of chaos," *Medium*, 29 de abril. https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d.

Cepik, Marco. 2003. *Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência*. Rio de Janeiro: FGV.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Chiavenato, Idalberto. 2004. *Introdução à Teoria Geral Da Administração*. Edição Compacta. Rio de Janeiro: Elsevier Brasil.

Gil, Antonio Carlos. 2017. *Como elaborar projetos de pesquisa*. 6ª ed. São Paulo: Atlas.

Global Initiative Against Transnational Organized Crime. 2021. "The Global Illicit Economy: Trajectories of Transnational Organized Crime." Março. https://globalinitiative.net/wp-content/uploads/2021/03/The-Global--Illicit-Economy-GITOC-Low.pdf.

Holanda, Luiz M. C., Antonio C. de Francisco e João L. Kovaleski. 2009. "A percepção dos alunos do mestrado em engenharia de produção sobre a existência de ambientes de criação do conhecimento," *Ciência da Informação* 38 (2): 96–109. https://www.scielo.br/j/ci/a/GbQXXHfjW-cysgwFr7PfqKSQ/?lang=pt&format=pdf.

Kepner, Charles H., e Benjamin B. Tregoe. 1981. *O administrador racional*. São Paulo: Atlas.

Lowenthal, Mark M. 2008. *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press.

Mackey, Robert H., Sr. 1992. *Translating Vision into Reality: The Role of the Strategic Leader*. Carlisle Barracks, PA: US Army War College.

Ministério da Defesa. 2011a. *Manual de Doutrina de Operações Conjuntas 1° volume (MD30-M-01)*. https://bdex.eb.mil.br/jspui/bitstream/123456789/134/1/MD30_M01_v1.pdf.

Ministério da Defesa. 2011b. *Manual de Doutrina de Operações Conjuntas 3° volume (MD30-M-01)*. https://www.resdal.org/caeef-resdal/assets/brasil---manual-de-doutrina-de-operacoes-conjuntas---3%C2%BA--volume.pdf.

Nonaka, Ikujiro, e Noboru Konno. 1998. "The Concept of 'Ba': Building a Foundation for Knowledge Creation," *California Management Review* 40 (3): 40–54. http://contents.kocw.net/KOCW/document/2014/Chungbuk/KimSangWook/10-1.pdf.

Nonaka, Ikujiro, e Hirotaka Takeuchi. 1997. *Criação do conhecimento na empresa: como as empresas japonesas geram a dinâmica da inovação*. Rio de Janeiro: Campus.

Nonaka, Ikujiro, Ryoko Toyama, e Noboru Konno. 2000. "SECI, Ba and Leadership: A Unified Model of Dynamic Knowledge Creation," *Long Range Planning* 33 (1): 5–34. https://www.researchgate.net/publication/222666807_SECI_Ba_and_Leadership_a_Unified_Model_of_Dynamic_Knowledge_Creation.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.269
ISSN 2595-4717

Polícia Federal. 2022. *Doutrina de Inteligência Policial da Polícia Federal*. Brasília.

Rowe, Gene, e George Wright. 2001. "Expert Opinions in Forecasting: The Role of the Delphi Technique," in *Principles of Forecasting: A Handbook for Researchers and Practitioners*, organizado por J. Scott Armstrong, 125–44. New York: Springer Science & Business Media.

Schwab, Klaus. 2016. *The Fourth Industrial Revolution*. New York: Crown Currency. https://archive.org/details/the-fourth-industrial-revolution--schwab-2016/page/32/mode/2up.

UNODC (United Nations Office on Drugs and Crime). 2010. "The Globalization of the Crime: A Transnational Organized Crime Threat Assessment," https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

Visacro, Alessandro. 2019. "Fazendo as coisas certas: segurança e defesa do Estado moderno," *Cadernos de Estudos Estratégicos* 20: 49-80. https://ebrevistas.eb.mil.br/CEE/article/view/6723.

Von Krogh, Georg, Kazuo Ichijo, e Ikujiro Nonaka. 2001. *Facilitando a criação do conhecimento: reinventando a empresa como o poder da inovação contínua*. Rio de Janeiro: Campus.

Zuboff, Shoshana. 2019. "High Tech Is Watching You," *Harvard Gazette*, 4 de março. https://news.harvard.edu/gazette/story/2019/03/harvard--professor-says-surveillance-capitalism-is-undermining-democracy/.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Artigo de pesquisa

Jomar Barros de Andrade[1]
ORCiD 0009-0000-6136-1289

APLICAÇÃO DOS FUNDAMENTOS DA METODOLOGIA DA PRODUÇÃO DO CONHECIMENTO PARA A INTELIGÊNCIA CIBERNÉTICA

https://doi.org/10.58960/rbi.2025.20.273

De Andrade, Jomar Barros. 2025. "Aplicação dos Fundamentos da Metodologia da Produção do Conhecimento para a Inteligência Cibernética," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.273. https://doi.org/10.58960/rbi.2025.20.273.

Recebido em 31/03/2025
Aprovado em 10/07/2025
Publicado em 07/10/2025

1 General-de-Brigada da Reserva do Exército Brasileiro. Mestre em Ciências Militares (ECEME). Especialista em Inteligência Militar. Foi Chefe do Centro de Estudos Estratégicos do Exército (CEEEx), do Centro de Defesa Cibernética (CDCIBER) e 2º Subchefe (Informação e Comando e Controle) do Estado-Maior de Exército (EME). Desde 2020, concentra sua atuação nas áreas de Inteligência, Comando e Controle e Cibernética. Atualmente, desempenha o cargo de Gerente do Programa Estratégico Defesa Cibernética do Exército, garantindo as entregas de seus diversos projetos e contribuindo com o planejamento desse Setor Estratégico de Defesa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

APLICAÇÃO DOS FUNDAMENTOS DA METODOLOGIA DA PRODUÇÃO DO CONHECIMENTO PARA A INTELIGÊNCIA CIBERNÉTICA

Resumo

A Inteligência e a Defesa Cibernética utilizam dados oriundos do espaço cibernético para atingir seus objetivos. Apesar de a Doutrina da Atividade de Inteligência fornecer os fundamentos gerais, a produção do conhecimento a partir da fonte cibernética demanda o seu aprofundamento. A Técnica de Avaliação de Dados de Cibernética deve ser ampliada para além de seus aspectos originalmente desenvolvidos para as fontes humanas. Para tanto, a lições aprendidas pela Segurança Cibernética são úteis e valiosas. A Metodologia da Produção do Conhecimento empregada para a Inteligência Cibernética, servindo-se de técnicas, procedimentos e ferramentas específicas, é fundamental para que seja possível o desenvolvimento de aplicações de Inteligência Artificial. Por fim, a formação dos recursos humanos deve evoluir, para que mais componentes do Sistema Brasileiro de Inteligência contribuam para a produção de conhecimento cibernético.

Palavras-chave: Inteligência, defesa cibernética, Inteligência Artificial, metodologia.

APPLICATION OF THE FOUNDATIONS OF THE KNOWLEDGE PRODUCTION METHODOLOGY TO CYBER INTELLIGENCE

Abstract

Intelligence and Cyber Defense employ data originating from cyberspace to achieve their objectives. Although the Doctrine of Intelligence Activity provides general foundations, the production of knowledge from cyber sources requires further development. The Cyber Data Evaluation Technique must be expanded beyond its aspects originally developed for human sources. To this end, the lessons learned from Cybersecurity are useful and valuable. The Knowledge Production Methodology employed for Cyber Intelligence, making use of specific techniques, procedures, and tools, is essential for enabling the development of Artificial Intelligence applications. Finally, the training of human resources must evolve, so that more components of the Brazilian Intelligence System may contribute to the production of cyber knowledge.

***Keywords**: Intelligence, cyber defense, Artificial Intelligence, methodology.*

APLICACIÓN DE LOS FUNDAMENTOS DE LA METODOLOGÍA DE PRODUCCIÓN DE CONOCIMIENTO PARA LA INTELIGENCIA CIBERNÉTICA

Resumen

La Ciberinteligencia y la Ciberdefensa utilizan datos del ciberespacio para alcanzar sus objetivos. Si bien la Doctrina de la Actividad de Inteligencia proporciona las bases generales, la producción de conocimiento a partir de fuentes cibernéticas requiere mayor estudio. La Técnica de Evaluación de Datos Cibernéticos debe ampliarse más allá de sus aspectos desarrollados originalmente para fuentes humanas. Para ello, las lecciones aprendidas en Ciberseguridad son útiles y valiosas. La Metodología de Producción de Conocimiento empleada para la Ciberinteligencia, que utiliza técnicas, procedimientos y herramientas específicos, es esencial para el desarrollo de aplicaciones de Inteligencia Artificial. Finalmente, la formación de recursos humanos debe evolucionar para que más componentes del Sistema de Inteligencia Brasileño contribuyan a la producción de conocimiento cibernético.

***Palabras clave**: Inteligencia, ciberdefensa, Inteligencia Artificial, metodología.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Introdução

A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação (TIC) e das oportunidades econômicas e sociais oriundas do ambiente digital (Brasil 2020). A conectividade em tempo integral e a disponibilidade imediata de conteúdo tornaram-se aspectos fundamentais da vida de grande parcela da sociedade.

A Estratégia Nacional de Segurança Cibernética (E-Ciber), já em sua introdução, destaca que tais avanços fazem surgir, na mesma proporção, novas e crescentes ameaças que colocam em risco a administração pública e a sociedade. Além disso, a escala de produção e a disponibilização de informação representam oportunidades e desafios para a Inteligência, o que tem levado, no exterior, a estudos para a criação de estruturas dedicadas à produção do conhecimento especializadas no domínio cibernético (AFCEA 2022).

Sobre esse cenário já altamente complexo, a rápida expansão de aplicações de Inteligência Artificial (IA) tem levado as organizações, ao redor do mundo, a uma corrida para a adoção de ferramentas com essa tecnologia. Reconhecimento de imagens, tradução de idiomas e o uso de ferramentas conversacionais, dentre outras, já são realidade nas áreas de Defesa, Inteligência e Segurança Pública, em diversos países (McMahon 2024, 1).

A Inteligência de Estado e seus profissionais são desafiados por essa conjuntura. Nesse contexto, a Doutrina da Atividade de Inteligência (DAI) estabeleceu o conceito de Inteligência Cibernética como aquela voltada a temas relativos ao Espaço Cibernético (EC), cuja produção busca apoiar a atuação do Brasil frente a vulnerabilidades e ameaças, informando políticas públicas e planos estatais nesse domínio, bem como acompanhar e avaliar capacidades, intenções e atividades de atores externos naquele espaço (Brasil 2023b, 159).

Cabe destacar que o conceito de Fonte é fundamental para a atividade. A expressão Fonte Cibernética, embora não expressamente definida na DAI, passará a ser utilizada para indicar a origem, no espaço cibernético, dos dados utilizados por aquela disciplina.

Pelo seu caráter especializado, a atividade de Inteligência se apoia na Metodologia da Produção do Conhecimento (MPC) (Brasil 2023b, 107) que, com os ajustes necessários às particularidades de cada setor, está consagrada

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

por seu emprego em diversos órgãos de Inteligência brasileiros (Brasil 2023b, 106). No entanto, não há dúvidas que o seu arcabouço teórico, embora consolidado, foi desenvolvido originalmente para trabalhar com fontes humanas (Calaça 2023, 156).

Com o já citado exponencial desenvolvimento das TIC, em especial na área de Cibernética, surgiram novas oportunidades para a Inteligência. No entanto, para que os produtos elaborados a partir de dados oriundos dessas fontes tecnológicas sejam confiáveis, oportunos e possuam a qualidade necessária aos desafios, atuais e futuros, a serem enfrentados pelo Brasil, é necessário que os fundamentos da MPC se desenvolvam e sejam capazes de embasar a atuação nesses domínios.

Destaca-se que, apesar de seus diferentes conceitos e objetivos, a análise de seus respectivos fundamentos evidencia a existência de pontos em comum entre a Segurança Cibernética, a Defesa Cibernética e a Inteligência. Na primeira, o principal ator no que se refere ao Setor Cibernético é o Gabinete de Segurança Institucional da Presidência da República (GSI-PR), preponderando as atividades de proteção, enquanto na segunda, também passa a haver a possiblidade de execução de medidas de exploração e ataque, em cumprimento às demandas das autoridades competentes (Brasil 2023d, 28). A Inteligência se relaciona com ambas, tanto contribuindo para a proteção da informação, quanto se beneficiando dos dados obtidos e dos conhecimentos produzidos (Brasil 2023d, 17).

Porém, ao mesmo tempo que tal convergência indica a possibilidade de compartilhamento de procedimentos e técnicas, também as diferenças de escopo, prioridades e tempos de atuação devem ser bem compreendidas, a fim de permitir uma atuação coordenada dos respectivos órgãos especializados.

Por meio de uma metodologia da pesquisa bibliográfica, o presente artigo irá revisar a literatura existente sobre o tema, aí considerados o marco legal em vigor, os manuais de emprego das Forças Armadas, a produção científica nacional e internacional e, principalmente, a Doutrina da Atividade de Inteligência. Desse modo, o objetivo é aprofundar e expandir uma metodologia oficial.

A análise está estruturada para, ao longo do desenvolvimento, obter o alinhamento dos conceitos na bibliografia, apontando tanto os fundamentos da DAI que são diretamente aplicáveis à Cibernética, quanto aqueles que necessitam de adaptações, para os quais serão apresentadas sugestões

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

baseadas na literatura selecionada. Ao longo do trabalho, serão levantados aspectos relativos ao impacto da IA nas diversas etapas da metodologia.

Por fim, ênfase especial será dada à Técnica de Avaliação de Dados e à execução das fases do ciclo de produção do conhecimento, para o que serão realizados estudos de caso sumários, para contextualizar sua aplicação para a Inteligência Cibernética.

O Espaço Cibernético e os processos de Coleta e Busca de dados

Para a DAI, o Espaço Cibernético é entendido como o conjunto das infraestruturas informáticas e telemáticas interconectadas, que compreende hardware, software, dados, usuários e quaisquer relações lógicas entre eles (Brasil 2023b, 49). Com isso, são de interesse para a Inteligência Cibernética tanto as redes e equipamentos de comunicações quanto os sistemas de informação sobre eles estabelecidos e, não menos importantes, as pessoas que atuam e se relacionam naquele ambiente.

A Doutrina Militar de Defesa Cibernética (DMDC) apresenta definição semelhante, considerando o EC como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (Brasil 2023d, 17). Além disso, divide o espaço cibernético em três camadas: física (dispositivos e infraestrutura de TIC), lógica (aplicações, serviços, protocolos, etc) e ciberpersona (identidades virtuais dos usuários). Tais conceitos serão úteis posteriormente, ao considerarmos a atuação das diferentes disciplinas da Inteligência no EC (Brasil 2015).

Conclui-se que o Espaço Cibernético é transversal às áreas de atuação interna e externa e, embora a Inteligência Cibernética tenha foco nos temas a ele relacionados, não esgota o tema, nem exclui sua importância para as demais áreas. Para fins da MPC, o espaço cibernético em si não é a fonte dos dados, mas o ambiente onde os dados estão. Portanto, para que tais dados sejam obtidos, devem existir os fundamentos técnicos e regulatórios para que sejam realizadas ações especializadas (Brasil 2023b, 145) e ações operacionais (Brasil 2023b, 144) no ciberespaço.

De maneira geral, os conceitos de busca e coleta previstos na DAI são aplicáveis no ambiente cibernético, com as necessárias contextualizações. Coleta é ação especializada que visa à obtenção de dados e informações de livre acesso (Brasil 2023b, 149). Sob o ponto de vista da Inteligência Cibernética,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

enquadram-se na situação de livre acesso os sítios, blogs, serviços de notícias, dentre outros, mesmo aqueles para os quais seja necessário um registro ou assinatura, gratuito ou não, que permita o acesso ao conteúdo oferecido.

Em qualquer circunstância, o acesso a qualquer insumo ou produto do trabalho da Atividade de Inteligência se baseia na necessidade de conhecer (Brasil 2023b, 166). Isso posto, mesmo na coleta de dados já devem ser identificadas e adotadas as medidas de segurança que garantam o sigilo e a discrição, inerentes ao trabalho do profissional de Inteligência (Brasil 2023b, 29).

Busca, por sua vez, é a aplicação combinada de técnicas operacionais para obtenção de dados, informações e conhecimentos indisponíveis (Brasil 2023b, 148). No EC, a busca é realizada sobre redes, sistemas ou qualquer outro componente do ambiente, inclusive pessoas, cujo acesso não seja ostensivamente permitido ou exija o emprego de técnicas especializadas operacionais, para acessar e extrair os dados de interesse.

As técnicas operacionais raramente são empregadas de forma isolada (Brasil 2023b, 137). No caso específico das ações cibernéticas, as características do ambiente naturalmente levam a uma combinação de procedimentos, onde a busca de dados indisponíveis vai exigir o uso especializado de recursos técnicos, o que eventualmente pode ser feito de forma anônima a partir de um ponto de acesso, com outras similares às ações baseadas em recursos humanos, porém adaptadas às características ciberespaço.

Nesse sentido, não há como deixar de identificar a importância, para efeitos do estudo dessa temática, do emprego de modelos conceituais (ou *frameworks*) para conhecer as ameaças e para a normatização das ações proativas (aqui consideradas tanto as operações cibernéticas, quanto as de Inteligência no ciberespaço). A DAI não contempla esse tipo de *framework,* razão pela qual é oportuna a menção ao Modelo Comum de Ameaça Cibernética (*Common Cyber Threat Framework* - CCTF), elaborado pelo Escritório do Diretor Nacional de Inteligência dos Estados Unidos da América (EUA 2018).

Originalmente elaborado para permitir uma melhor compreensão da ameaça cibernética, no âmbito da comunidade de Inteligência norte-americana, nele é visível a incorporação e a simplificação dos conceitos de *Cyber Kill Chain* (Lockheed Martin s.d.), e a estrutura MITRE ATT&CK (Mitre Corporation s.d.), sintetizados em um modelo de quatro etapas: preparação, engajamento, presença e efeito/consequência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Embora a solução dessa lacuna específica esteja fora do escopo deste artigo, entende-se que a incorporação de soluções como o CCTF à DAI pode contribuir tanto para o desenvolvimento de técnicas de busca no espaço cibernético, quanto para a Contrainteligência, com a aplicação dos conceitos da segurança cibernética aplicados na proteção contra ameaças no ciberespaço. Tal situação é mais uma evidência prática da, já mencionada, convergência de fundamentos entre a Inteligência e a Defesa/Segurança Cibernética.

Cabe destacar que dados ou redes mal protegidos não podem ser considerados abertos e, ainda que sua obtenção possa ser feita com o emprego de técnicas simples, ainda assim envolvem procedimentos que só podem ser empregados por pessoal especializado, no contexto de uma Operação de Inteligência. Dessa forma, a penetração em redes externas é um tema sensível, que demanda o estabelecimento de rígidos mecanismos de controle.

A Fonte Cibernética, a Inteligência Cibernética e o Analista de Inteligência

O conceito de Fonte é basilar para a atividade de Inteligência. Definida como a origem de um dado, informação ou conhecimento (Brasil 2023b, 156), as suas características são as discriminadoras dos tipos de Inteligência atualmente contemplados pela DAI, quais sejam, de Fontes Humanas (*Human Intelligence* – HUMINT), Fontes Técnicas (*Technical Intelligence* – TECHINT) ou Fontes Abertas (*Open Source Intelligence* – OSINT). A doutrina considera que os dados oriundos do espaço cibernético estão abarcados pela Inteligência de Sinais (*Signals Intelligence* – SIGINT), que é uma subdivisão da TECHINT.

No entanto, a literatura não dá uma definição de Inteligência Cibernética em função da fonte de seus dados, como nos demais tipos. A DAI, embora adote essa expressão, a define quando trata das áreas de atuação, junto com as inteligências interna, externa e transnacional (Brasil 2023b, 53).

Para fins deste artigo, não será oferecida uma definição diferente da que já está na doutrina, mas será aproveitado o acrônico constante da Inteligência Militar Terrestre, sendo empregada o termo CYBINT (de Cyber Intelligence), para designar a Inteligência Cibernética (Brasil 2015, 3-4), disciplina cujos dados principais têm origem em fontes atuando ou localizadas nas diversas camadas do ciberespaço.

Assim sendo, aplicando-se os conceitos apresentados, até o momento, às peculiaridades do EC, podem ser consideradas como possíveis fontes ciber-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

néticas, dentre outras:

> • Operadores de sistemas próprios (cuja capacidade técnica, perícia ou talento individual sejam fatores determinantes para o resultado alcançado);
>
> • Agentes de Inteligência;
>
> • Sistemas automatizados especializados em obter e processar dados oriundos do ambiente cibernético, cujo produto possa ter sua veracidade acompanhada ao longo do tempo;
>
> • Fontes abertas diversas, gratuitas ou não, especializadas em pesquisa, acompanhamento, análise ou quaisquer outros serviços, voltados para a coleta e processamento de dados oriundos do ambiente cibernético; e
>
> • Operadores de sistemas do alvo, ou outros elementos que tenham acesso ao mesmo, a partir de seu recrutamento como colaboradores.

Nesse ponto, cabe destacar que não se deve confundir a CYBINT com a Inteligência de Ameaças, denominação amplamente consolidada da área da Segurança e Defesa Cibernéticas, que levanta e organiza informação detalhada e acionável sobre ameaças cibernéticas (IBM 2022), de diversos tipos (*malwares, phishings, zero-day exploits,* etc) (IBM 2024a) e atores, em especial as Ameaças Persistentes Avançadas (*Advanced Persistent Threats* – APT) (IBM 2024a). Embora a última produza dados e informações que são utilizados pela primeira, o escopo da CYBINT é bem mais amplo, por não estar limitado ao estudo apenas das ameaças.

Ressalta-se que, atualmente, várias disciplinas de Inteligência, além da CYBINT, atuam no espaço cibernético. A totalidade dos dados de interesse da Inteligência de Mídias Sociais (*Social Media Intelligence* – SOCMINT) (Brasil 2023b, 160) e a maioria dos utilizados pela OSINT, e até pela HUMINT, se encontram no EC.

Aproveitando o conceito de camadas do EC apresentado pela DMDC, SOCMINT e HUMINT atuam fortemente na camada de Ciberpersona, OSINT coleta dados nos sistemas operados na camada Lógica, enquanto categorias de TECHINT têm como foco os sistemas da camada Física. A CYBINT, pela variedade de seus objetivos, atua nas três camadas, de forma coordenada com as demais disciplinas e aproveitando os conhecimentos por elas produzidos.

Longe de ser contraditória, tal situação apenas reforça a característica da Inteligência de se apoiar na integração de diversas fontes para produzir conhecimento. No entanto, aponta também para a necessidade de alinhamento e padronização das técnicas especializadas, empregadas pelos diversos atores.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Os profissionais de inteligência contam com extensa bibliografia sobre a aplicação de Técnicas de Análise Estruturada (TAE) para a produção de conhecimento, sendo crescente o número de profissionais, de diversas áreas, especializados em questões do espaço cibernético. No entanto, não é comum a disponibilidade, em fontes abertas, de material acadêmico ou profissional que faça a convergência das TAE com a cibernética.

O Analista de Inteligência deve possuir, ao mesmo tempo, a competência técnica para trabalhar com os dados das diversas fontes, conforme sua especialidade, e o domínio da MPC.

Em consequência, o arcabouço intelectual de um Analista de CYBINT deve abranger uma base técnica em cibernética, que permita a compreensão do linguajar da área, mas também uma visão abrangente da conjuntura, permitindo a compreensão e a integração de fatos e eventos em todos as expressões do Poder Nacional (político, econômico, psicossocial, militar, científico e tecnológico) (Brasil 2024, 29). Além disso, deve ter conhecimento sobre assuntos de TECHINT e estar familiarizado com técnicas e procedimentos de OSINT e SOCMINT, entre outras, para que possa identificar vulnerabilidades e ameaças, apoiar o processo decisório e acompanhar atores externos no EC.

Ao mesmo tempo, para que os dados obtidos, a partir dos diversos aspectos inerentes a esse ambiente, sejam transformados em conhecimento utilizável, esse profissional deve dominar a MPC, sendo capaz de contemplar as peculiaridades inerentes ao processamento de dados oriundos dos diversos tipos de fonte. Com essas características, o profissional será capaz de ir além dos aspectos puramente técnicos da temática e produzir conhecimentos que, efetivamente, possam contribuir para reduzir a incerteza no processo decisório dos assuntos que se relacionam com a Cibernética.

Inteligência Artificial e CYBINT

O surgimento de programas de computador que simulam a conversa humana com o usuário final, utilizando técnicas de IA conversacional, como processamento de linguagem natural (PLN), conhecidos como chatbots (IBM, 2021), foi um evento disruptivo. Para a Inteligência, essas aplicações representam uma oportunidade de melhoria na rapidez e qualidade no tratamento de grande quantidade de dados, permitindo ao analista mais tempo para a sua interpretação.

A Empresa de Dados Abertos (*Open Source Enterprise* – OSE), subordinada

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

à Diretoria de Inovação Digital (FAS 2015) da Agência Central de Inteligência (Central Intelligence Agency – CIA), lançou uma ferramenta interna, no estilo do ChatGPT, para permitir melhor acesso às fontes abertas por seus analistas (McMahon 2024, 1). No entanto, junto com o entusiasmo por seu potencial, surgem também preocupações com a ética e a integridade da informação contida nos produtos gerados por IA (UNESCO, s.d.).

Em um trabalho produzido para o Centro de Excelência em Defesa Cibernética Cooperativa (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN), Biondi et al. (2021, 12-28) expõem que, embora a definição de CYBINT e seu relacionamento com as demais disciplinas seja uma tarefa em curso, já são inúmeras as oportunidades para a aplicação de técnicas de IA e aprendizado de máquina em seu proveito. Os autores destacam, dentre outras, o contraterrorismo, a identificação de relacionamentos em múltiplos domínios, a descoberta de radares, o ataque contra redes sem fio, a quebra de senhas, a superação de sistemas de proteção, dentre outros.

Apesar dessas possibilidades serem facilmente visualizadas, a efetiva implementação da IA na CYBINT passa por consideráveis desafios. Embora essa análise esteja além do escopo deste trabalho, devem ser destacados alguns aspectos fundamentais, que terão impacto na execução da MPC.

Para tanto, é especialmente interessante o trabalho de Goldfarb et al. (2021, 17) que, ao estudarem as possibilidades da IA e do aprendizado de máquina em apoio ao processo decisório (uma das missões fundamentais da Inteligência), propõem que são duas as variáveis que definem o desempenho de um sistema dessa natureza: a qualidade dos dados e a dificuldade para o julgamento. Dados são de alta qualidade quando a informação de qualidade é abundante e não contaminada por preconceitos, vieses e outras anomalias. A dificuldade para o julgamento é menor, por sua vez, quando os objetivos são claramente definidos e têm a concordância dos diversos envolvidos. Em situações em que os dados são de alta qualidade e o julgamento é claro, sistemas automatizados seriam até mais eficientes que os seres humanos. Na situação oposta, onde os dados são de baixa qualidade e o julgamento é difícil, a automatização não é possível (Quadro 1).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Quadro 1
Implicação dos Dados e do Julgamento para a automação do processo decisório

		Dados	
		Alta qualidade	**Baixa qualidade**
Julgamento	**Claro**	Processo decisório totalmente automatizado é mais eficiente	Automação completa é possível, mas arriscada
	Difícil	Predições automatizadas podem assessorar decisões humanas	Processo decisório automatizado não é possível

Fonte: Goldfarb *et al.* 2021, 18.

O raciocínio de Goldfarb et al. é especialmente apropriado para o emprego do aprendizado de máquina pela Inteligência. Embora as aplicações já estejam em curso e as possibilidades sejam amplas, a IA somente será eficiente caso seus algoritmos sejam desenvolvidos sobre processos muito bem estabelecidos e alimentados com dados de alta qualidade.

Dessa forma, a existência de uma MPC sólida para a Cibernética é fator crítico para o sucesso de iniciativas de Inteligência Artificial na CYBINT. Em síntese, são necessários Analistas de Cibernética, tanto para ensinar as máquinas a realizar a análise, quanto para rotular os dados necessários para seu treinamento.

O emprego de *chatbots* para a resposta de perguntas objetivas, apresentando os resultados em formato definido, já é uma realidade. Para tanto, tais sistemas acessam bancos de dados, selecionam o que é relevante e produzem textos, desempenhando o papel de fonte e de analista. Assim sendo, é fundamental que a credibilidade dessa fonte, a veracidade desses dados e a qualidade desse analista sejam conhecidos.

Não há resposta imediata para essa questão. No entanto, é fundamental que os produtos gerados por IA atendam aos requisitos exigidos pela MPC, para que possam basear a produção de conhecimentos, com impacto em todas as disciplinas que tocam o espaço cibernético, mas principalmente na OSINT e CYBINT.

Como fundamento para uma possível abordagem prática, são interessantes os aspectos estabelecidos na Diretiva para a Comunidade de Inteligência 203 (*Intelligence Community Directive* 203 – ICD 203), do Escritório do Diretor Nacional de Inteligência dos EUA. O trabalho foi a consequência dos estudos realizados para corrigir processos que levaram às falhas de inteligência sobre a existência de armas de destruição em massa, que acabaram fundamentando a invasão do Iraque pelos EUA, em 2003 (McMahon 2024, 2).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

A ICD 203 versa sobre os padrões de análise que devem ser seguidos por todas as disciplinas do sistema de inteligência norte-americano. O documento estabelece cinco Padrões Analíticos (*Analytic Standards* – AS): Objetividade, Independência de Considerações Políticas, Oportunidade, Base em todas as fontes disponíveis de Inteligência e Implementação evidente dos nove Padrões para a Prática de Análise (*Analytic Tradecraft Standards* – ATS) (EUA 2023, 4-6):

> 1. Descrever apropriadamente a qualidade e a credibilidade das fontes, dados e metodologias aplicadas;
>
> 2. Expressar e explicar adequadamente as incertezas associadas com os principais raciocínios analíticos;
>
> 3. Distinguir apropriadamente a diferença entre informação baseada em Inteligência e julgamentos ou deduções do analista;
>
> 4. Incorporar a análise de alternativas;
>
> 5. Demonstrar a relevância para o usuário e considerar as implicações;
>
> 6. Usar argumentação clara e lógica;
>
> 7. Explicar se houve uma mudança de posição em relação a conhecimentos anteriormente produzidos;
>
> 8. Fazer avaliações e julgamentos precisos; e
>
> 9. Incorporar informação visual, quando apropriado.

McMahon (2024, 4-6) analisa quais seriam as condições para uma adesão aos ATS 3 e 4. No que diz respeito à ATS 3 (Distinguir informação de dedução), uma ferramenta de IA generativa, ao ser consultada pelo analista, deveria ser capaz de:

> • Citar a fonte original - para que o analista pudesse verificar e replicar os achados da ferramenta;
>
> • Atestar a fidelidade ao texto original - usando aspas ou outro recurso para diferenciar citações literais de paráfrases;
>
> • Ater-se aos fatos - evitando, a não ser que solicitada, a apresentação de deduções a partir dos fatos existentes;
>
> • Apresentar contexto para as indicações - caso solicitado, apresentar indicações, porém destacando claramente o que é fato e o que é dedução;
>
> • Manter a consistência caso a situação evolua - caso o surgimento de novos dados modifique a resposta, a causa da mudança deve ser rastreável;
>
> • Apresentar o resultado em um formato pré-estabelecido - nos mesmos modelos estabelecidos para a confecção dos diversos tipos de documento de Inteligência;
>
> • Fazer sentido: o julgamento feito pela ferramenta deve ser plausível e apoiado em bases sólidas.

Ao analisar a ATS 4 (Incorporar alternativas), o autor sugere que, sendo de-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

mandada a apresentar diferentes hipóteses para determinado fenômeno, a ferramenta de IA deve ser capaz de apresentar apenas alternativas factíveis, mantendo-se fiel aos padrões anteriormente citados para a ATS 3. Nesse caso, a ferramenta deve, ainda, explicar os pontos fortes e fracos de cada alternativa (McMahon 2024, 11).

Nesse ponto, destaca-se a importância de "fazer a pergunta certa". Os sistemas de IA generativa são projetados para gerar saídas específicas com base na qualidade das perguntas ("prompts") apresentadas. A engenharia de prompts ajuda os modelos a conhecerem e a responder melhor a uma ampla gama de consultas, das mais simples às mais técnicas (IBM 2023). Para a Inteligência, analistas que formulam bons prompts obtém os melhores resultados.

A partir daí, em que pese o elevado potencial do uso de tecnologia no apoio à análise de Inteligência, o ser humano na função de analista continua a ser responsável por suas análises, e responsabilizável perante o tomador de decisão (McMahon 2024, 9).

Dessa forma, pode-se concluir que a aplicação da IA para a Inteligência é factível, permite a aplicação da TAD e tem a OSINT como campo inicial para o aprendizado de valiosas lições. No entanto, seu emprego sem bases sólidas, ao invés de reforçar, irá comprometer o trabalho da Inteligência.

Processos definidos e dados de qualidade são fundamentais para que os algoritmos sejam desenvolvidos e treinados. As técnicas e procedimentos, em especial no campo da engenharia de prompts e ciência de dados, têm potencial para aplicação nas demais disciplinas, particularmente na CYBINT. Por fim, os aspectos éticos e técnicos da aplicação da IA na Inteligência devem ser aprofundados e incorporados à regulamentação da atividade e à MPC.

Aplicação da TAD para a Fonte Cibernética

O objetivo da TAD é a determinação do grau de credibilidade do dado. A DAI apresenta os procedimentos gerais para a sua realização e, em uma das poucas fontes encontradas que aprofunda o tema, Calaça (2023, 155) apresenta um detalhamento dos questionamentos a serem feitos, a fim de proporcionar mais orientações para o analista que a realiza. Porém, a própria autora reconhece que a técnica, originalmente para fontes humanas e, posteriormente, estendida para fontes tecnológicas, depende fortemente da capacidade do analista que a executa (Calaça 2023, 156).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Cabe destacar que a realização da TAD sobre os dados obtidos, a partir de qualquer tipo de fonte, é condição necessária para os trabalhos da MPC. Se um dado não pode ser avaliado de forma estruturada, não possui credibilidade e, dessa forma, não pode ser utilizado para produzir conhecimentos de Inteligência, o que o torna, em última análise, inútil. Em síntese: sem uma TAD para a Fonte Cibernética, não há CYBINT.

Nesse ponto, há distinção importante a fazer: nas situações em que o dado desejado está indisponível, seu detentor deixa de ser uma Fonte e passa a se enquadrar no conceito de Alvo (Brasil 2023b, 146). No entanto, a sua capacidade de originar o dado desejado necessita ser avaliada, durante o processo de seleção dos objetivos da ação cibernética. Ou seja, para a CYBINT, a determinação do valor do alvo cibernético segue uma lógica semelhante ao processo de avaliação da fonte cibernética.

Dessa forma, a definição de uma TAD Cibernética é condição fundamental para o prosseguimento da elaboração doutrinária, necessária para o funcionamento do sistema de Inteligência, em geral, e à especialização de seus recursos humanos, em particular.

Dentro da TAD, o primeiro aspecto a ser tratado é o da avaliação da idoneidade da fonte. Sobre esse aspecto, os aspectos fundamentais a serem avaliados, que determinarão o grau a ser atribuído, são: autenticidade, confiança e competência (Brasil 2023b, 112). A DAI assim define os aspectos a serem avaliados:

> • Autenticidade: avaliar quem produziu, expediu, modificou ou destruiu um determinado conhecimento, informação ou dado sensível (Brasil 2023b, 148). O analista deve identificar se a fonte, de fato, produziu ou obteve o dado (Calaça 2023, 156).
>
> • Confiança: evidenciada pela precisão dos dados obtidos ou fornecidos pela fonte, ao longo do tempo (Calaça 2023, 155).
>
> • Competência: a capacidade pessoal e a localização da fonte.

Embora a busca da redução da subjetividade seja desejável, não é prático nem possível tentar esgotar todas as possibilidades para a Fonte Cibernética. Dessa forma, um primeiro passo seria a padronização de um número de alternativas para cada critério apresentado, a serem avaliados pelo Analista de CYBINT, e integrados de forma a produzir uma classificação geral que, embora ainda subjetiva, apresenta uma metodologia que pode ser ensinada nas escolas e replicada pelos órgãos integrantes do sistema de Inteligência. A seguir, será apresentada uma proposta para essa padronização inicial, semelhante ao

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

que já existe para a HUMINT.

Para a CYBINT, podem ser identificadas duas situações particulares no que diz respeito à avaliação da idoneidade: Fontes Próprias (operadores ou sistemas) e Fontes Externas (indivíduos, sistemas, fontes abertas especializadas etc). Em ambas as situações, quando a fonte for uma pessoa, sua avaliação aproveita os tradicionais conceitos da HUMINT. Nos casos em que a fonte compreender também sistemas de informação, devem ser consideradas suas características técnicas, sintetizadas em uma avaliação de sua qualidade geral para produzir o dado em questão.

Pode-se destacar, no caso da CYBINT:

> • Autenticidade: no caso de fontes próprias, quando o operador ou sistema estiver sendo empregado em situação sob controle ou supervisão do órgão de Inteligência, a autenticidade pode ser considerada como automaticamente configurada. No caso de fontes externas, caso sejam julgadas não autênticas, sua idoneidade não pode ser avaliada.
>
> • Confiança: também avaliada em função da precisão dos resultados obtidos ao longo do tempo.
>
> • Competência: em função da qualidade do sistema (capacidade/atualização dos equipamentos, ferramentas e sistemas utilizados), da capacidade individual (dada pela capacitação técnica/experiência/talento dos operadores) e da localização da fonte (acesso ao alvo).

A qualidade do sistema e a capacidade individual são combinadas no conceito geral de Capacidade da Fonte Cibernética, que pode assumir três valores (Quadro 2):

> Sim: quando sistemas de qualidade são empregados por indivíduos ou equipes capazes;
>
> Parcial: quando falta a qualidade do sistema ou a capacidade individual; e
>
> Não: quando faltam a qualidade e a capacidade.

Quadro 2
Avaliação da Capacidade da Fonte Cibernética

Capacidade	Qualidade do Sistema	Capacidade Individual
Sim	Sim	Sim
Parcial	Sim	Não
	Não	Sim
Não	Não	Não

Fonte: elaborado pelo autor.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Após definida a Capacidade da fonte, deverá ser avaliada sua Localização. É determinado se a fonte tem ou não tem acesso ao alvo, sem gradações admitidas. Dessa forma, a combinação dessas duas variáveis é o que define a situação no quesito da competência que, em conjunto com a autenticidade e confiança, permite a determinação da Idoneidade da Fonte. Aproveitando o código alfabético apresentado por Calaça (2023, 157), temos o Quadro 3.

Quadro 3
Avaliação da Idoneidade de Fontes Cibernéticas

Letra	Grau de Idoneidade	Autenticidade	Confiança	Competência	
			Precisão	Capacidade	Localização
A	Inteiramente Idônea	Sim	Sempre	Sim	Sim
B	Normalmente Idônea	Sim	Sempre	Parcial	Sim
			Maioria	Sim	Sim
C	Regularmente Idônea	Sim	Maioria	Parcial	Sim
			Metade	Sim	Sim
D	Normalmente Inidônea	Sim	Minoria	Parcial	Sim
E	Inidônea	Sim	Minoria	Parcial	Não
F	Não avaliada	Fonte sem autenticidade ou operador/sist. não empregado			

Fonte: elaborado pelo autor.

Em seguida, os fatores básicos para o julgamento do Conteúdo são: Semelhança Externa, Coerência Interna e Compatibilidade (Brasil 2023b, 112). Enquanto a Semelhança pode ser avaliada apenas com a comparação do dado com os já existentes, a Coerência (evidenciada pela ausência de contradições internas do dado) e a Compatibilidade (manifestada pela harmonização do dado com o que já se conhece a respeito do assunto) vão demandar também o emprego de Analistas com domínio funcional do ambiente cibernético.

De forma prática, o julgamento do conteúdo pode ser feito por meio de perguntas simples, feitas pelo Analista de CYBINT:

> Há semelhança com outros dados? Respostas possíveis: sim ou não.
>
> O dado tem coerência interna? Respostas possíveis: sim ou não.
>
> É compatível com o que se sabe? Respostas possíveis: sim, muito, pouco ou não.

Assim como para a idoneidade da fonte, aproveita-se o código numérico apresentado por Calaça (2023, 157) e, após a combinação das repostas, chega-se ao grau de veracidade do conteúdo (Quadro 4).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Quadro 4
Avaliação da Veracidade do Conteúdo

Número	Grau de Veracidade	Conteúdo do Dado		
		Semelhança	**Coerência**	**Compatibilidade**
1	Confirmado por outras fontes	Sim	Sim	Sim
2	Provavelmente verdadeiro	Não	Sim	Sim
3	Possivelmente verdadeiro	Não	Sim	Muito
4	Duvidoso	Não	Sim	Pouco
5	Improvável	Não	Sim	Não
6	Não atribuída	Não apresentou características que permitam avaliar os três parâmetros		

Fonte: elaborado pelo autor.

No entanto, cabe destacar que pode ser obtida uma variedade enorme de dados a partir do EC, tais como conteúdo de bancos de dados, teor das conversas, organização das redes de interesse, tráfego de dados entre os diversos nós das redes, características dos equipamentos e sistemas empregados, medidas de proteção utilizadas e assim por diante.

Tal variedade, que evolui em alta velocidade, representa um desafio para a Inteligência, pois tem como consequência a obtenção de uma enorme quantidade de dados de diversas naturezas que, para serem adequadamente tratados e produzirem conhecimento utilizável, com oportunidade, exigem o emprego de pessoal especializado e que se adote uma metodologia sólida, estabelecida em fundamentos.

Entendendo que as questões da aplicação da TAD sobre produtos de IA ainda merece maior aprofundamento, fora do escopo do presente trabalho, mas a fim de contribuir para a compreensão do que foi apresentado, uma vez que há aspectos originais na abordagem, seguem abaixo exemplos de aplicação sumária da TAD em dados típicos de CYBINT:

> Situação A - ao receber um arquivo, o Analista de Cibernética o submeteu ao seu antivírus instalado e, após receber o resultado negativo, realizou uma verificação adicional no site https://www.virustotal.com/gui/home/upload, onde foi feita uma análise gratuita de presença de malware, comparando as assinaturas encontradas no arquivo com informações do banco de dados do portal. Nesse caso a fonte é o Virustotal e o dado é o resultado da análise.
>
> Situação B - o monitoramento da Dark Web identificou uma mensagem do hacker conhecido como Hell_Knight, que anunciava ter explorado uma

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

vulnerabilidade dos sistemas de controle industrial da Usina Hidrelétrica de Itaipu e informava as condições em que seria realizado o leilão do malware utilizado. O ator é conhecido pela Inteligência, por já ter reivindicado ataques de defacement contra órgãos públicos e colocado à venda arquivos com credenciais de acesso que se revelaram antigas. A fonte é o hacker em questão e o dado é a existência de um exploit capaz de afetar um sistema crítico.

Situação C - um operador de CYBINT, acompanhando a ferramenta de Segurança Cibernética que monitora a honeynet (CERT-BR s.d.), estabelecida pelo seu órgão, identificou sutis alterações no padrão do tráfego da rede, reportando ao Analista que havia indícios da realização de um reconhecimento (primeiro passo da Cyber Kill Chain) por parte de uma ameaça. O operador é capacitado, porém inexperiente e em fase de treinamento com novas ferramentas. Por fim, a fonte é o operador e o dado é o conteúdo de seu relatório.

Os quadros abaixos apresentam, sinteticamente, os passos e o resultado da TAD realizada pelo Analista de CYBINT (Quadros 5, 6 e 7).

Quadro 5
Estudo de Caso de TAD para CYBINT - Integridade

Situação	Integridade				
	Autenticidade	Confiança	Competência		Avaliação
		Precisão	Capacidade	Localização	
A	Sim	Maioria	Sim	Sim	B
B	Sim	Minoria	Não	Não	E
C	Sim	Maioria	Parcial	Sim	C

Fonte: elaborado pelo autor.

Quadro 6
Estudo de Caso de TAD para CYBINT - Veracidade

Situação	Veracidade			
	Semelhança	Coerência	Compatibilidade	Avaliação
A	Sim	Sim	Sim	1
B	Não	Não	Não	6
C	Não	Sim	Sim	3

Fonte: elaborado pelo autor.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Quadro 7
Estudo de Caso de TAD para CYBINT - Síntese

Situação	Integridade	Veracidade	Síntese
	Avaliação	Avaliação	
A	B	1	B1
B	E	6	E6
C	C	3	C3

Fonte: elaborado pelo autor.

MPC para a Fonte Cibernética

O funcionamento do ramo Inteligência pode ser esquematizado em um ciclo composto por cinco fases, caracterizadas por ações: Objetivar, Acompanhar, Informar, Decidir e Agir. As três primeiras fases são realizadas pelos organismos de Inteligência (Brasil 2023b, 55), não havendo especificidades para a CYBINT.

Em seu Capítulo 5, a DAI aprofunda os conceitos relativos ao Elemento de Análise, abordando conceitos fundamentais que não necessitam de contextualização adicional para sua aplicação direta na Inteligência Cibernética:

> As formas racionais de conhecer: ideia, juízo e raciocínio (Brasil 2023b, 93);
>
> Os estados da mente perante a representação da verdade: ignorância, possibilidade, probabilidade e certeza (Brasil 2023b, 96);
>
> Os insumos para a análise: dado, informação e conhecimento (Brasil 2023b, 99); e
>
> Os tipos de conhecimento de Inteligência: informe, apreciação e estimativa (Brasil 2023b, 103).

Dentro do Sistema Brasileiro de Inteligência (SISBIN), organizado pelo Decreto nº 11.693, diversos elementos têm a possibilidade e a responsabilidade de atuar no espaço cibernético, devendo ser capazes de produzir conhecimentos de CYBINT, dentro de suas áreas específicas. É importante destacar que, além dos seus órgãos permanentes, prioritariamente aqueles relacionados com a segurança integrada (Inteligência, Defesa e Segurança Pública) e diplomacia, são previstos órgãos dedicados, como aqueles que possuem unidades de Inteligência, ou atividades similares, e atuem em assuntos estratégicos relacionados à Política Nacional de Inteligência (PNI) (Brasil 2023c).

Considerando que a PNI destaca, entre as principais ameaças, a ocorrência de ataques cibernéticos (Brasil 2023c, item 6-5), conclui-se que outros ór-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

gãos intensivos em tecnologia na administração pública (tais como o Serviço Federal de Processamento de Dados - SERPRO, a Secretaria de Governo Digital - SGD, entre outros) devem ser organizados para atuar como órgãos dedicados, pois têm importante contribuição a fazer para produção do conhecimento de CYBINT.

Tais conhecimentos, evidentemente, serão de interesse tanto do Ramo Inteligência quanto do Ramo Contrainteligência (Brasil 2023b, 53; 74), podendo ser produzidos com a participação de um Elemento de Operações (Brasil 2023b, 132). Para o Analista de CYBINT, esses órgãos dedicados, capazes de obter dados no espaço cibernético, são mais um meio passível de ser acionado por meio de Pedidos de Inteligência (PI) ou qualquer outro documento padronizado.

Assim como já visto para a TAD, as diversas fases da MPC são seguidas sem maiores dificuldades pelo Analista de CYBINT, com as peculiaridades abaixo.

1. Na fase de Planejamento

   Para essa etapa, é importante destacar que a Inteligência não concorre com a Segurança Cibernética. Assim sendo, o foco da CYBINT é claro: apoiar a tomada de decisão e a ação dos entes do estado face às ameaças, oportunidades e atores operando no EC.

   Dessa forma, não é um uso apropriado do tempo do Analista a produção de conhecimentos que se assemelhem a cartilhas, informativos, resenhas ou similares, frequentemente utilizados pela Segurança Cibernética para desenvolver a mentalidade de proteção nos usuários de sistemas de informação.

2. Na fase da Reunião

   A coleta de dados poderá utilizar uma gama variada de técnicas e ferramentas específicas do ambiente cibernético para obter, de forma rápida, sistematizada e objetiva, apenas os dados de interesse para o atendimento dos aspectos essenciais a conhecer.

   Grande quantidade de dados e informações úteis são oriundos de relatórios e publicações em fontes abertas, elaboradas por organizações de Segurança/Defesa Cibernética.

   O uso de ferramentas de IA generativa pode ser particularmente útil nessa fase, considerando os aspectos já apontados.

   Nas ações de busca deverão ser empregados procedimentos específicos para ambiente cibernético, aliadas ou não às técnicas operacionais já existentes. Anonimização, emprego de avatares, monitoramento de conteúdo na deepweb são, dentre outros, tópicos de convergência entre operadores de CYBINT e profissionais de Segurança Cibernética que atuam na defesa proativa dos ativos de interesse.

3. Na fase de Avaliação

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Os dados obtidos por busca ou coleta deverão ser submetidos à TAD, com as particularidades já apontadas para a Fonte Cibernética.

A adaptação das técnicas de Segurança Cibernética é útil para desenvolver procedimentos e técnicas específicas para a Fonte Cibernética. Ferramentas de análise de rede e de incidentes, por exemplo, produzem relatórios e gráficos que podem auxiliar o Analista em seus julgamentos.

4. Na fase de Integração e Interpretação

É quando o Analista de IC deve chegar às suas conclusões, que são a parte do conhecimento que tem efetiva relevância para os tomadores de decisão.

Durante a etapa de Integração, o analista formulará Juízos que poderão ensejar a produção de diversos Informes, em função dos diferentes graus de credibilidade atribuídos às frações obtidas.

Esse conhecimento deve ser visto como um "bloco" básico de informação que mereça ser registrado para uso futuro, no prosseguimento do ciclo de análise. Resultado de um processo simples, não é comum que um informe seja apresentado a uma autoridade para apoio à tomada de decisão.

A grande quantidade de dados associados ao espaço cibernético provavelmente irá demandar algum tipo de síntese ou agregação. Por exemplo: considerando que diariamente as redes dos órgãos do Estado recebem milhares de tentativas de invasão, feitas automaticamente a partir de todo o mundo, cada tentativa isolada não tem significado particular. No entanto, a totalização do número de tentativas, associada à sua autoria e local de origem, acompanhada ao longo do tempo, pode apresentar dados de interesse para a Inteligência, justificando a produção de informes.

Na etapa da Interpretação, o Analista irá elaborar Raciocínios para concluir sobre o significado dos dados obtidos e sobre os conhecimentos produzidos. Em função da situação, serão elaboradas Apreciações, expressando a opinião ou certeza do Analista sobre fatos passados, presentes ou seus desdobramentos no futuro imediato, ou Estimativas, projetando as opiniões para cenários futuros.

Como exemplos de Apreciações de CYBINT podem ser citadas análises sobre comportamentos de ameaças cibernéticas durante períodos determinados, avaliações do poder cibernético de atores estatais ou não estatais, resultados de análises de resiliência de sistemas próprios, dentre outros. Embora tais conhecimentos possam se valer de produtos de Segurança e Defesa Cibernética como insumos (tais como análises, relatórios, etc), deles se diferenciam não só por empregarem a Linguagem de Inteligência, mas por terem objetivos específicos, levantados durante a fase de planejamento da MPC.

As Estimativas de CYBINT, por sua vez, buscam identificar as principais forças presentes no cenário cibernético e antecipar seus comportamentos no futuro, na forma de cenários. Da mesma forma que nas Apreciações, existe ampla disponibilidade de trabalhos acadêmicos e profissionais sobre o futuro da Cibernética, que podem subsidiar o trabalho do Analista.

Destaca-se a importância das Estimativas de CYBINT para a atividade crucial de alerta estratégico para os mais altos níveis de decisão. As temáticas da ciberspionagem, invasão de sistemas, extração de dados, ataques a infraestruturas críticas, operações de informação e atuação do cibercrime são todas atuais, relevantes e frequentemente motivado-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

ras de crises. Todas elas são adequadas para a produção de cenários e elaboração de indicadores, a cargo da CYBINT (Gentry 2022, 739-744).

Para elaborar tais raciocínios, o Analista deverá se valer das Técnicas de Apoio à Análise constantes da doutrina (Brasil 2023b, 116), enriquecidas pelos recursos, ferramentas e processos da Segurança Cibernética, como já mencionado.

Considerando que a produção de conhecimento é mais eficiente quando feita em grupos multidisciplinares, é altamente vantajosa a organização de equipes compostas por especialistas em Inteligência, que dominem a MPC e as TAE, e técnicos em cibernética, preferencialmente incluindo aqueles com perfil ofensivo - hacking ético (IBM 2023b). O SISBIN, pela variedade de seus integrantes, está em posição única para organizar esse tipo de grupo, pois conta com todas as capacidades em seus diferentes órgãos.

5. Na fase de Formalização e Validação:

   Não há diferenças nessa fase da CYBINT em relação às demais disciplinas, devendo ser seguida a padronização adotada pelos órgãos do SISBIN para a formalização dos documentos. No entanto, é importante destacar que a Linguagem de Inteligência (Brasil 2023b, 123) é fundamental para a correta compreensão do conhecimento, por seus usuários.

   Considerando que o linguajar especializado dos profissionais de cibernética não é de amplo conhecimento, além de ser carregado de imagens e termos técnicos, o analista de CYBINT deve dar objetividade e simplicidade para o produto final, apresentando a informação de acordo com o perfil do usuário e está sendo apoiado.

6. Na fase de Difusão e Resultados, não há diferenças para a CYBINT.

Por fim, destaca-se que, tendo sido evidenciada a aderência da Inteligência Cibernética à MPC, incluídas as suas peculiaridades, é necessária a formalização e a padronização de seus fundamentos que, a partir de então, podem e devem ser objeto de especialização dos recursos humanos do SISBIN. Dessa forma, o papel dos estabelecimentos de ensino de Inteligência é fundamental, como polo irradiador desse conhecimento para todo o sistema.

Conclusão

As ideias expostas não têm o objetivo de esgotar o assunto, mas esperam contribuir para o debate, ainda incipiente, sobre a necessária convergência de esforços para a sistematização da produção do conhecimento pela Inteligência Cibernética, nova e importante disciplina da atividade.

Cabe destacar que a adequação da metodologia para as peculiaridades da Fonte Cibernética, embora não seja suficiente, é condição necessária para a Produção do Conhecimento. Além disso, é absolutamente essencial na construção do arcabouço doutrinário para a atuação dos diversos atores

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

estatais atuantes no ambiente cibernético, com evidentes reflexos para a especialização dos recursos humanos empregados.

Como foi dito, os aspectos de Inteligência são apenas uma parcela do amplo e complexo ecossistema do Espaço Cibernético. No entanto, a experiência mostra que essa parte é fundamental para que o SISBIN cumpra sua missão de contribuir para a proteção dos interesses do Brasil. A visão da Inteligência, que combina a produção do conhecimento com a proteção dos ativos de informação, é especialmente capaz de produzir uma metodologia integrada e objetiva para a CYBINT. Os fundamentos técnicos da Segurança Cibernética, por sua vez, representam uma valiosa fonte de dados e a oportunidade para aprendizado de lições.

Por fim, para que a Inteligência não desperdice a oportunidade representada pelo rápido desenvolvimento das aplicações de IA, é fundamental que a MPC seja aprofundada para contemplar as peculiaridades das fontes tecnológicas, em especial da CYBINT, definindo seus processos e desenvolvendo a capacidade de trabalhar com a enorme massa de dados, de diversas naturezas.

Dessa forma, a maturidade do SISBIN e de sua MPC, aliados à qualidade dos estabelecimentos de ensino do sistema, são importantes instrumentos para a organização e a integração dessa nova e importante área de atuação do Estado brasileiro.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Referências

Armed Forces Communications & Electronics Association International. 2022. "U.S. Cyber Command Means To Magnify Cyber Intelligence". The Cyber Edge Newsletter. Acessado em 24 de março de 2025. https://www.afcea.org/signal-media/cyber-edge/us-cyber-command-means-magnify-cyber-intelligence.

Biondi, Fabio, Giuseppe Buonocore e Richard Matthews. 2021. "Generative Adversarial Networks from a Cyber Intelligence perspective".

Brasil. 2015. EB20-MF-10.107 - Inteligência Militar Terrestre (2ª Ed). Exército Brasileiro. https://bdex.eb.mil.br/jspui/bitstream/123456789/95/1/EB20-MF-10.107.pdf.

Brasil. 2016. Decreto Nº 8.793, de 29 de junho de 2016 – Fixa a Política Nacional de Inteligência. Secretaria Geral. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

Brasil. 2020. Estratégia Nacional de Segurança Cibernética. Secretaria Geral da Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

Brasil. 2023a. Política Nacional de Cibersegurança. Casa Civil. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

Brasil. 2023b. Doutrina da Atividade de Inteligência. Agência Brasileira de Inteligência. https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

Brasil. 2023c. Decreto Nº 11.693, de 6 de setembro de 2023 - Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. Casa Civil. https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm.

Brasil. 2023d. MD31-M-07 - Doutrina Militar de Defesa Cibernética. Ministério da Defesa. https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf.

Brasil. 2024. Fundamentos do Poder Nacional. Escola Superior de Guerra. https://www.gov.br/esg/pt-br/centrais-de-conteudo/publicacoes/fundamentos-do-poder-nacional/fundamentos-do-poder-nacional-rev-2024-mac2-1.pdf.

Calaça, Irene. 2023. "Técnica de Avaliação de Dados (TAD) e Fonte em Inteligência". *Revista Brasileira de Inteligência* 18: 149-165. https://doi.org/10.58960/rbi.2023.18.232.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Rede no Brasil). s.d. "Honeypots e Honeynets: Definições e Aplicações". Acessado a 28 de junho de 2025. https://www.cert.br/docs/whitepapers/honeypots-honeynets/.

EUA (Estados Unidos da América). 2018. A Common Cyber Threat Framework: A Foundation for Communication. Escritório do Diretor Nacional de Inteligência. Acessado a 25 de setembro de 2025. https://info.publicintelligence.net/ODNI-CyberThreatFramework.pdf.

EUA. 2023. Intelligence Community Directive 203, Analytic Standards. Escritório do Diretor Nacional de Inteligência. Acessado a 28 de junho de 2025. https://www.dni.gov/files/documents/ICD/ICD-203.pdf.

FAS (Federation of American Scientists. 2015. "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)". Acessado em 27 de março de 2025. https://fas.org/publication/osc-ose/.

Gentry, John A. 2022. "Cyber Intelligence: Strategic Warning Is Possible," *International Journal of Intelligence and CounterIntelligence* 36 (3): 729–754. https://doi.org/10.1080/08850607.2022.2095544.

Goldfarb, Avi e Jon R. Lindsay. 2021. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security* 46 (3): 7–50. https://doi.org/10.1162/isec_a_00425.

IBM. 2021. "O que é um chatbot?". Acessado em 27 de março de 2025. https://www.ibm.com/br-pt/topics/chatbots.

IBM. 2022. "O que é Inteligência de Ameaças?". Acessado em 27 de março de 2025. https://www.ibm.com/br-pt/topics/threat-intelligence.

IBM. 2023. "O que é Engenharia de Prompt?". Acessado em 27 de março de 2025. https://www.ibm.com/br-pt/think/topics/prompt-engineering.

IBM. 2023b. "O que é hacking ético?". Acessado em 28 de março de 2025. https://www.ibm.com/br-pt/topics/ethical-hacking.

IBM. 2024a. "Types of cyberthreats". Acessado em 27 de março de 2025. https://www.ibm.com/think/topics/cyberthreats-types.

IBM. 2024b. "O que são ameaças persistentes avançadas?". Acessado em 31 de março de 2025. https://www.ibm.com/br-pt/topics/advanced-persistent-threats.

Lockheed Martin. s.d. "The Cyber Kill Chain". Acessado em 25 de março de 2025. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

McMahon, Gerald. 2024. "Analytic Tradecraft Standards in an Age of AI". https://www.belfercenter.org/research-analysis/analytic-tradecraft--standards-age-ai.

Mitre Corporation. s.d. Acessado a 27 de junho de 2025. https://attack.mitre.org/.

United Nations Educational, Scientific and Cultural Organization. s.d. "Ética da IA e integridade da informação". Acessado em 27 de março de 2025. https://www.unesco.org/pt/g20/digital-economy.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Artigo de pesquisa

Larissa Maria Melo Ambrozio de Assis[1]
ORCiD 0009-0000-0681-2147

PARÂMETROS LEGAIS PARA O USO ESTATAL DE FERRAMENTAS TECNOLÓGICAS POTENCIALMENTE INTRUSIVAS PARA FINS DE SEGURANÇA

https://doi.org/10.58960/rbi.2025.20.274

Assis, Larissa Maria Melo Ambrozio de. 2025. "Parâmetros legais para o uso estatal de ferramentas tecnológicas potencialmente intrusivas para fins de segurança." *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.274. https://doi.org/10.58960/rbi.2025.20.274.

Recebido em 09/04/2025
Aprovado em 22/04/2025
Publicado em 24/04/2025

1 Pesquisadora associada ao Núcleo de Pesquisa em Inteligência (NUPI) da Escola de Inteligência (ESINT). Integrante da Rede LideraGOV do Poder Executivo Federal. Graduada em Direito pelo Centro Universirario de Brasília (UniCEUB), mestre em Direito pelo UniCEUB, com intercâmbio pela Universidad Nacional del Litoral (Argentina) e doutora em Direito pela Universidade de Brasília (UnB) com intercâmbio na Law School da Cornell University (EUA).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

PARÂMETROS LEGAIS PARA O USO ESTATAL DE FERRAMENTAS TECNOLÓGICAS POTENCIALMENTE INTRUSIVAS PARA FINS DE SEGURANÇA

Resumo

Este artigo trata da problemática dos parâmetros para o uso de ferramenta tecnológica potencialmente intrusiva (FTPI) para fins de manutenção da segurança da sociedade e do Estado e da segurança pública. O estudo parte do recorte dos direitos fundamentais afetados pelo uso de FTPIs definido na audiência pública nº 39 do Supremo Tribunal Federal. O direito à segurança da sociedade e do Estado, a construção do conceito do direito à segurança e sua relação com o uso de ferramentas tecnológicas são analisados com o objetivo de distinguir a atividade de inteligência da atividade repressiva estatal. Em sequência, aborda-se sobre o controle e a *accountability* desses ramos de atuação estatal e propõe-se parâmetros para o uso de FTPIs adequados a essas finalidades.

Palavras-chave: ferramentas tecnológicas, inteligência, sistema repressivo, segurança da sociedade e do Estado, segurança pública.

LEGAL FRAMEWORK FOR STATE USE OF POTENTIALLY INTRUSIVE TECHNOLOGICAL TOOLS FOR SECURITY PURPOSES

Abstract

This article addresses the issue of establishing parameters for the use of potentially intrusive technological tools (PITTs) for the purpose of maintaining the security of society and the State and public security. The study is based on the framework of fundamental rights affected by the use of PITTs, as defined during the 39th Public Hearing of the Brazilian Supreme Federal Court. It analyzes the right to security, the development of the concept of the right to security, and its relationship with the use of technological tools, with the aim of distinguishing intelligence from State repressive activities. Subsequently, the article discusses the control and accountability mechanisms applicable to these areas of State action and proposes parameters for the use of PITTs.

Keywords*: technological tools, intelligence, repressive system, social and state security, public safety.*

PARÁMETROS LEGALES PARA EL USO ESTATAL DE HERRAMIENTAS TECNOLÓGICAS POTENCIALMENTE INTRUSIVAS CON FINES DE SEGURIDAD

Resumen

Este artículo aborda la problemática de los parámetros para el uso de herramientas tecnológicas potencialmente intrusivas (HTPIs) por parte del Estado, con la finalidad de preservar la seguridad de la sociedad e del Estado y la seguridad pública. El estudio analiza los derechos fundamentales afectados por el uso de las HTPIs, conforme la audiencia pública nº 39 del STF. Se examina el derecho a la seguridad, la construcción de su concepto y su relación con el uso de herramientas tecnológicas, con el objetivo de distinguir la actividad de inteligencia de la actividad represiva estatal. Posteriormente, se abordan los mecanismos de control y accountability aplicables a estos ámbitos de actuación estatal, y se proponen parámetros para el uso de las HTPIs.

Palabras clave*: herramientas tecnológicas, inteligencia, sistema represivo, seguridad de la sociedad y del Estado, seguridad pública.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Introdução

Na atual Era Digital, direitos fundamentais dos cidadãos são constantemente colocados em risco no domínio cibernético tanto pela atuação de atores privados quanto públicos. Neste artigo discutiremos sobre a atuação do Estado, mais especificamente sobre os parâmetros para o uso de ferramenta tecnológica potencialmente intrusiva (FTPI) para fins de manutenção da segurança da sociedade e do Estado e da segurança pública, consideradas as finalidades estatais de atuação preventiva e repressiva.

O uso de ferramentas tecnológicas é crescente desde a revolução industrial, com especial escalada a partir da *Advanced Research Projects Agency Network* (ARPANET), na década de 1960, base para o desenvolvimento da internet nos anos 70 e 80 e, posteriormente, o seu uso civil. Porém, desde a criação e proliferação de tecnologias há a discussão sobre a vigilância global dos usuários (McLuhan e Powers 1992).

O caso Edward Snowden, em 2013, reforçou o debate sobre a vigilância estatal massiva da população a partir do uso de FTPIs.[1] O contínuo avanço tecnológico desde então torna imprescindível aprofundar o debate sobre quem vigia a atuação estatal e sobre a necessidade de transparência[2], controle e *accountability*[3] para o uso desses recursos (Cole 2014).

Esse debate ganhou densidade e dimensão no Brasil a partir da ADPF nº 1.143 (Brasil 2024b), que busca questionar as balizas para o uso de *spywares,* de

1 Vale ressaltar que essas ações foram realizadas com base no *USA PATRIOT Act*, que ampliou os poderes de vigilância externa e investigação das autoridades norte-americanas, permitindo o monitoramento de comunicações e outras atividades com o objetivo de combater o terrorismo.

2 A transparência não foi arrolada aqui porque dentro do emprego de ferramentas tecnológicas intrusivas, seja para fins de prevenção ou repressão, o sigilo é a regra, até mesmo para garantir o menor dano aos direitos à privacidade, intimidade, dos dados e da vida privada afetados pela ação estatal. Acredita-se que o parâmetro da transparência importa para a compreensão da limitação de liberdades individuais quando da análise dos estudos técnicos preliminares realizados para aquisição dessas ferramentas e do cumprimento da legislação que assegura a proteção de dados pessoais, dentre outras garantias fundamentais, e as implicações para a soberania digital do país. Apesar da relevância dessa análise, o enfoque desse estudo é centrado na perspectiva da autorização para o uso dessas ferramentas, de acordo com a motivação estatal de atuação preventiva ou repressiva. Sobre o debate de cibersegurança e soberania digital, uma referência relevante é a obra de Luca Belli e outros (2023).

3 Uso o termo *accountability* ao invés de responsabilidade pela intenção de considerar o dever de prestação de contas, de transparência, de controle e de fiscalização, enquanto um conjunto de práticas que envolvem a responsabilização de gestores e instituições por suas ações (IFAC 2001). Para o debate sobre a tradução do termo para português, confira Pinho e Sacramento (2009).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Imsi Catchers, e de dispositivos que rastreiam a localização de um alvo específico através da rede celular.[4] A ação, assim, reabriu o debate brasileiro, por meio da audiência pública, para o uso de FTPIs, sobretudo o seu uso sem critérios legais específicos que permitam o controle e a *accountability*.

Essa discussão não é exclusiva ao Brasil. O relatório da ONU sobre privacidade na era digital indica justamente esse problema e concluiu por três tendências notáveis relacionadas ao papel dos Estados na salvaguarda e promoção do direito à privacidade: a atenção ao abuso generalizado de ferramentas intrusivas de hackeamento; ao seu papel fundamental de criptografia robusta para garantir o exercício do direito à privacidade e de outros direitos; e ao monitoramento generalizado dos espaços públicos (ONU 2022).

As FTPIs, quando utilizadas pelo Estado, devem atender a finalidades específicas porque podem afetar direitos fundamentais[5]. Nesse ponto, o direito à segurança, enquanto direito fundamental previsto no *caput* do art. 5º da Constituição Federal (CF), é destacado como principal fator de motivação para o uso dessas ferramentas. Contudo, os fundamentos da Constituição, a efetivação dos objetivos do País e a proteção dos princípios das relações internacionais, previstos nos arts. 1º a 4º da CF[6], igualmente podem motivar o uso das FTPIs.

Para tanto, trataremos do tema em quatro partes. Primeiro traremos alguns esclarecimentos sobre as FTPIs destacadas na ADPF nº 1.143 e no debate da audiência pública nº 39 do Supremo Tribunal Federal (STF), particularmente sobre como elas podem afetar um determinado rol de direitos fundamentais. Em segundo, abordaremos o dever estatal de prover o direito à segurança da sociedade e do Estado, onde buscaremos compreender a construção do conceito do direito à segurança e sua relação com o uso de ferramentas tecnológicas. Em terceiro, trataremos de compreender as distinções entre a inteligência e o aparato punitivo estatal em suas finalidades de atuação

4 Em sua peça inicial, o Ministério Público Federal (MPF) não se manifesta contrário ao uso dessas ferramentas, mas reclama a omissão de parâmetros para o uso e considera a necessidade de controle judicial prévio. Na audiência pública, por exemplo, o MPF defendeu o uso de *spywares* contra estrangeiros pela inteligência (Brasil 2024).

5 Consideramos aqui o conceito de direitos fundamentais de Robert Alexy (1993), pelo qual esses direitos são normas de ordem constitucional que se distinguem por seu caráter de princípio, ou seja, um mandamento de otimização.

6 Vale ressaltar, ainda, que a motivação para relativizar tais direitos, seja pela finalidade estatal de prevenção ou repressão, não se limita aos dispositivos aqui elencados. O Estado pode, por exemplo, motivar sua atuação na proteção da ordem econômica, o que envolve também previsões do art. 170 a 181 da CF.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

para concretização do direito à segurança, com o objetivo de compreender as necessidades específicas de controle e a *accountability* desses ramos de atuação estatal. Tais bases nos serviram para propormos, ao final, alguns parâmetros mínimos de uso de FTPIs pelo Estado.

Como ferramentas potencialmente intrusivas podem afetar direitos fundamentais?

Ferramentas tecnológicas de comunicação facilitam a difusão e o acesso à informação, por meio de redes e de dispositivos eletrônicos[7]. No contexto da ADPF nº 1.143 (Brasil 2024b), há uma preocupação com a capacidade intrusiva dessas ferramentas, ou seja, de acesso aos dispositivos eletrônicos pessoais de determinado indivíduo, contra sua vontade[8], o que gera impacto para uma série de direitos fundamentais.

De acordo com a petição inicial da ADPF nº 1.143, o caráter intrusivo dessas ferramentas é definido por sua capacidade de proporcionar o monitoramento de aparelhos digitais de comunicação pessoal de forma remota. É importante compreendermos que se trata de algo diferente da ferramenta tecnológica ser invasiva, o que significa que ela subverte a forma de funcionamento do sistema para acessar o dispositivo por manipular a informação e comprometer a integridade do dispositivo eletrônico (Schneier 2018).

Para melhor compreensão de como FTPIs interferem nos direitos fundamentais, voltaremos nossa análise para o debate da audiência pública da ADPF nº 1.143, que destacou três FTPIs: *spywares*; *International Mobile Subscriber Number (Imsi) Catchers* e ferramentas de geolocalização[9].

7 Dispositivos eletrônicos funcionam a partir de uma arquitetura de infraestrutura de hardware, software e de telecomunicações, que são a base para manter sistemas de informação acessíveis aos usuários com características de flexibilidade, escalabilidade, confiabilidade, disponibilidade e desempenho (Tanenbaum e Bos 2016).

8 Em relação ao acesso de dispositivos eletrônicos é essencial considerar a ação do próprio usuário do dispositivo eletrônico rastreado. O usuário pode ter consentido com o acesso da FTPI de maneira intencional ou por omissão. É preciso conferir, também, se o usuário registrou o não consentimento de forma expressa e seu dispositivo, ainda assim, foi acessado contra sua vontade.

9 Ferramentas de geolocalização consistem em tecnologias que permitem identificar a posição geográfica de dispositivos eletrônicos, utilizando coordenadas geográficas (latitude e longitude) obtidas através de sinais de satélite, redes de internet ou radiofrequência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Spywares

Mais que ferramentas intrusivas, *spywares*[10] são invasivos por serem capazes de monitorar e registrar uma variedade de atividades do usuário, como hábitos de navegação, teclas pressionadas, credenciais de sistemas, informações pessoais e outras atividades online.

Um exemplo de *software* empregado como *spyware* é o *Pegasus*, com capacidade altamente invasiva, permitindo acesso ilimitado a um dispositivo por padrão, deixando poucos ou nenhum vestígio, e tornando difícil para os usuários saberem quais dados foram capturados. O *Pegasus*, em específico, permite o monitoramento das teclas, de todas as comunicações de um telefone (textos, e-mails, pesquisas na web), assim como de chamadas telefônicas, de localização e de acesso ao microfone e à câmera do dispositivo eletrônico[11].

Outro *spyware* de impacto expressivo é o *TriangleDB*, que possui a capacidade, também, de manipular arquivos e processos em curso pelo dispositivo eletrônico infectado, extrair dados de certificado, identidades digitais e outras credenciais, além de transmitir a localização precisa do equipamento[12].

Spywares, portanto, são instrumentos invasivos que podem viabilizar a violação dos direitos fundamentais à intimidade, à vida privada, à inviolabilidade do sigilo das comunicações pessoais e de dados, nos termos do art. 5º, incisos X, XII e LXXIX da CF.

Quando pensamos a finalidade punitiva estatal, a capacidade de manipulação de arquivos e processos nos dispositivos eletrônicos permite o uso indevido para criar provas de condutas delitivas falsas contra indivíduos, razão pela qual se soma, potencialmente, à violação de direitos fundamentais ao devi-

10 Segundo o Glossário de Segurança da Informação publicado pelo Governo Federal, *spywares* "são um tipo de malware. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware" (Brasil 2021b). Vale considerarmos também o conceito apresentado pelo *National Institute of Standards and Technology* (NIST), segundo o qual *spyware* é "*[s]oftware that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code*" (NIST s.d.).

11 A ferramenta é desenvolvida pelo NSO Group, que afirma só fornecê-la para governos autorizados a auxiliá-los no combate ao terrorismo e ao crime, além de exigir dos clientes que utilizem os seus produtos apenas para investigações criminais e de segurança nacional (Kirchgaessner *et al.* 2021).

12 Para saber mais sobre o TriangleDB confira as publicações da Kaspersky (2023).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

do processo legal para ser privado da liberdade, ao contraditório e à ampla defesa, assim como do direito à inadmissibilidade do uso de provas ilícitas, da presunção de inocência e de não ser submetido à identificação criminal, salvo nos casos previstos em Lei, conforme dispõe o art. 5º, incisos LIV, LV, LVI, LVII e LVIII da CF.

Imsi Catchers

Imsi Catchers são utilizados para localizar dispositivos eletrônicos móveis (celulares), sem capacidade para captar o conteúdo da comunicação desses dispositivos. Basicamente, esses recursos concedem, dentre outros, o acesso a metadados[13] que fornecem a localização aproximada do dispositivo, o que permite monitoramento da localização de um indivíduo que porta o aparelho celular (Broek, Roel e Ruiter 2015).

Essas tecnologias possuem diversas variantes, que podem ser empregadas de forma "passiva", que se limita a capturar o identificador do celular, ou "ativa", quando a ferramenta testa se o dispositivo está ativo. Todavia, essas FTPIs só acessam metadados, sem capacidade intrusiva de acessar o teor da comunicação. Assim, mesmo que a ferramenta consiga dizer que o dispositivo se comunica com outro, não consegue acessar o conteúdo dessa comunicação.

Os *Imsi Catchers* possuem aplicações legítimas pela inteligência, como a detecção de redes móveis clandestinas, ou até mesmo como um instrumento de contrainteligência ao identificar que alguma rede de telefonia celular esteja sendo monitorada em alguma localidade específica (Sampaio 2023).

Essas FTPIs, portanto, não possuem potencial de violar o sigilo das comunicações pessoais e de dados. O uso repetitivo de *Imsi Catchers* pode fornecer conhecimento de hábitos de localização, por exemplo, o que podemos considerar, eventualmente, como uma relativização de direitos à intimidade, à vida privada, à privacidade.

Quanto à finalidade punitiva estatal, essas ferramentas não realizam qualquer ação invasiva, com acesso intrusivo somente aos metadados. Dessa forma, elas não detêm capacidade lesiva de, teoricamente, serem utilizadas para promover uma instrução probatória eivada de vícios por violação de direitos

13 Os metadados possuem diversos conceitos, mas podemos considerá-los como dados que descrevem outros dados (Arakaki e Arakaki 2020). No caso dos metadados registrados da comunicação de dispositivos eletrônicos, esses metadados são como um envelope do processo comunicacional que registra dados como a identificação do usuário, a localização, o tipo de mensagem, a rede utilizada, o horário, a duração.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

fundamentais ao devido processo legal para ser privado da liberdade, ao contraditório e à ampla defesa, assim como do direito à inadmissibilidade do uso de provas ilícitas, da presunção de inocência e de não ser submetido à identificação criminal, salvo nos casos previstos em Lei.

Geolocalização

A geolocalização, por sua vez, não se confunde com comunicações privadas e pode ser usada para monitoramento de pessoas, tanto pelo uso do Serviço Móvel Pessoal (SMP), pelo *Global Positioning System* (GPS) ou por meio de "aplicativos".

A SMP é um serviço de telecomunicações de superfície, que permite a comunicação entre aparelhos móveis e aparelhos de diferentes estações, a partir de ondas de rádio que viabilizam a transmissão de dados e voz, inclusive com acesso à internet de banda larga para navegação via web, enviar e receber e-mails e usar aplicações que dependem do acesso à internet.

Para realizar essa transmissão entre os dispositivos são utilizadas Estações de Rádio Base (ERBs) e, a partir da triangulação dos dados de diferentes ERBs, é possível identificar a localização aproximada de um dispositivo[14].

O GPS pode ser entendido como um sistema de triangulação que usa sinais de rádio enviados por satélites artificiais. Receptores de GPS interpretam esses sinais e convertem as informações em coordenadas geográficas. Por meio dessa tecnologia, é possível precisar a localização de dispositivos, mesmo com serviços de *bluetooth*, *wi-fi* e telefonia desativados.

Por último, os aplicativos, popularmente conhecidos como Apps, são *softwares*, instalados em dispositivos eletrônicos, que oferecem soluções às necessidades dos usuários. Essas aplicações, vale destacar, permitem o compartilhamento da localização em tempo real, exigindo que o usuário disponibilize sua localização. Uma das razões para expansão do mercado de dados foi a perspectiva econômica do desenvolvimento de aplicações e serviços de tecnologia da informação, que viabilizaram a venda e "aluguel" de dados pessoais, no intento de reduzir custos para a transação dos empreendimentos tecnológicos (Varian 1996). Diversos Apps permitem o compar-

14 A Agência Nacional de Telecomunicações (Anatel) é a responsável por regular e controlar o acesso a dados da rede SMP. Sobre a regulamentação do SMP é importante conferir, ao menos, a Lei nº 9.472 – Lei Geral de Telecomunicações - LGT, de 16 de julho de 1997, a Resolução Anatel nº 477, de 7 de agosto de 2007, a Resolução Anatel nº 550, de 22 de novembro de 2010 e a Resolução Anatel nº 738, de 21 de dezembro de 2020.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

tilhamento da localização em tempo real, com a autorização concedida pelo usuário, o que é realizado utilizando tanto a geolocalização por GPS, como por SMP que permite a conexão com a internet.

Essas FTPIs de geolocalização não acessam dados ou comunicações, logo, não possuem essa capacidade lesiva. O uso delas permite georreferenciar pessoas a partir de seus dispositivos eletrônicos, o que pode relativizar direitos fundamentais à intimidade, à vida privada e à privacidade. Pelo entendimento dos Tribunais Superiores (Brasil 2020a; 2020c; Smanio 2021), entretanto, é constitucional e legal geolocalizar indivíduos por meio de FTPIs, face às necessidades estatais de assegurar outros direitos fundamentais, como a segurança[15]. A jurisprudência indica a necessidade de se observar critérios como o motivo e a motivação que explicite a proporcionalidade do uso de determinada FTPI que permita a geolocalização de um dispositivo.

Quando consideramos a finalidade punitiva estatal, o uso indevido desses recursos pode levar à violação do direito ao devido processo legal para ser privado da liberdade, ao contraditório e à ampla defesa, assim como do direito à inadmissibilidade do uso de provas ilícitas, da presunção de inocência e de não ser submetido à identificação criminal, salvo nos casos previstos em Lei.

Os direitos fundamentais em questão não são compreendidos como absolutos, visto que a esfera de proteção de um determinado direito leva à redução de outro direito igualmente protegido em nível constitucional (Andrade 1987). Assim, é necessário considerarmos a ponderação desses direitos, no caso concreto, para relativizar sua proteção de forma proporcional, dentro da concepção de colisão entre direitos fundamentais.

Quando pensamos o rol de direitos destacados em colisão, é necessário considerar a densidade desses direitos, visto que não são compreensíveis como dispositivos estáticos, mas como normas em sentido amplo de ordem principiológica por permitirem múltiplas facetas de interpretação de acordo com o caso concreto. Segundo Robert Alexy (1993, 105):

> [l]as contradicciones de normas en sentido amplio que tienen lugar dentro del ordenamiento jurídico son siempre colisiones de principios y las colisiones de principios se dan siempre dentro del ordenamiento jurídico. Esto pone claramente de manifiesto que el concepto de colisión de

15 É preciso considerarmos, inclusive, que o setor privado promoveu a geolocalização de pessoas por Apps durante a pandemia da COVID-19 e deixou a tecnologia à disposição dos órgãos e entidades públicas para fins de combate à disseminação do Coronavirus. A *startup* In Loco chegou a disponibilizar os dados estatísticos de geolocalização ao Estado de forma gratuita para essa finalidade de controle sanitário (ABES 2020).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

> principios presupone la validez de los principios que entran en colisión. Por ello, la referencia a la posibilidad de catalogar a los principios como inválidos no afecta el teorema de la colisión sino que simplemente revela uno de sus presupuestos.

Assim, não é possível a resolução da colisão de princípios constitucionais pela simples supressão de um em favor de outro, por não se tratar de dizer que um é válido e outro não. É preciso considerar o peso ou a importância relativa de cada princípio, com o objetivo de definir no caso concreto qual será limitado em face do outro.

A compreensão da colisão de direitos fundamentais exige uma visão estrutural, com o estudo dos conceitos desses direitos, sua influência no sistema jurídico e sua fundamentação. Isso requer tanto a compreensão da jurisprudência sobre tais direitos, como a reflexão sobre qual a decisão mais correta de limitação dos direitos fundamentais dentro do caso concreto, para formular parâmetros interpretativos-concretizadores específicos para a realidade de uma determinada coletividade (Alexy 1993).

O direito fundamental à segurança e sua relação com o uso de ferramentas tecnológicas

O direito à segurança e o dever estatal de assegurá-la são complexos e envolvem tanto as esferas de prevenção quanto as de repressão. De modo geral, vale considerar a segurança como um estado de normalidade, onde os demais direitos e deveres são usufruídos e cumpridos[16]. Desde o século XVIII, ao menos, a segurança é considerada como dever fundamental do Estado, enquanto principal ator e agente securitizador, previsto no art. 2º da Declaração de Direitos do Homem e do Cidadão de 1789[17].

Assegurar esse direito possui uma relação histórica com o uso de recursos tecnológicos. Para garantir o sigilo das comunicações, por exemplo, desde o século XVI, há o registro de diversas tecnologias como mensagens cifradas,

16 O exercício do poder punitivo estatal em prol de garantir o Estado de Direito não é o enfoque central do nosso debate. A compreensão da formação dessa faceta estatal, de prover o espaço do exercício de direitos e deveres, possui relação intrínseca com a compreensão do exercício do poder político, a formação do conceito de homem cidadão e de justiça. A construção do que se compreende como exercício do poder punitivo perpassa a literatura de Aristóteles, Platão, Jean Bodin, Thomas Hobbes, Nicolas Montesquieu, John Locke, Jean-Marie Constant, Jean-Jacques Rousseau, John Rawls, dentre outros.

17 Declaração dos Direitos do Homem e do Cidadão, 1789, art. 2º: "O objetivo de toda associação política é a conservação dos direitos naturais e imprescritíveis do homem. Esses direitos são a liberdade, a propriedade, a segurança e a resistência à opressão".

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

mensagens codificadas, criptografia e, já no século XIX, o telégrafo, entre outros[18].

É no curso da Segunda Guerra Mundial que se registra crescimento dos estudos de inteligência e da perspectiva da finalidade de prevenção. O discurso da segurança era proposto para proteger a sociedade de atentados contra o bem-estar social dos seus nacionais e de interferência nas suas decisões e interesses legítimos. As estruturas de inteligência dos Estados eram incipientes, mas até o final da Guerra Fria foram desenvolvidas metodologias e formas racionais de construir o conhecimento necessário para resguardar o que se compreendia por segurança (Buzan 1983; Herman 1996).

No período da Guerra Fria, a corrida armamentista impulsionou o desenvolvimento de tecnologias voltadas para a segurança, bem como a criação efetiva de agências de inteligência[19], no contexto de reconstrução e realinhamento necessários para o desenvolvimento e a segurança dos nacionais e para orientar as políticas públicas.

É nesse contexto, já nas décadas de 70 e 80, que a pauta da segurança começa a considerar questões sociais, econômicas e humanitária na compreensão do fenômeno da insegurança, em especial da criminalidade enquanto uma problemática interna de segurança, independente da pauta de segurança nas relações exteriores[20].

No pós-Guerra Fria, os processos de redemocratização, a globalização, a

18 Desde o início, a atividade de inteligência promoveu de forma preventiva a proteção do conhecimento a partir da codificação de mensagens (Thompson e Padover 1965). O desenvolvimento da criptografia para proteger a informação é um dos marcos dessa finalidade, que inclusive é um dos destaques da ONU, ao apontar o uso de criptografia robusta como um dever do Estado (ONU 2022). Atualmente, no Brasil, compete ao órgão central do sistema de inteligência, por meio do Centro de Pesquisa para o Desenvolvimento da Segurança das Comunicações (CEPESC), promover e desenvolver esses algoritmos, que são empregados, inclusive, nas urnas eletrônicas desde 1996 (ABIN s.d.).

19 Os serviços de inteligência foram organizados e estruturados em diversos países — como Alemanha, França, Estados Unidos das Américas, Reino Unido, União Soviética, Itália, dentre outros — até a Segunda Guerra Mundial (Bobbio, Matteucci e Pasquino 2016, 1147-1148).

20 Vale ressaltar que até a década de 1980 predominava a visão tradicional, dentro de um paradigma realista de segurança centrado no Estado forte, encarregado de manter a sua própria segurança territorial e de sua população por meio de visões distintas de segurança e defesa. A Escola de Copenhague somou a perspectiva de que estudos de segurança devem abranger, além das ameaças militares, aquelas provenientes das áreas política, econômica, ambiental e social. A premissa da Escola de Copenhague é que as pautas de defesa e segurança são construídas a partir de um contexto político e social da interpretação intersubjetiva (Buzan 1983; Floyd 2007).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

abertura econômica, a redução das regulações do mercado financeiro e a abertura de fronteiras representaram mudanças expressivas que intensificaram a transformação na gestão de diversas temáticas, entre elas, a segurança. A Agenda para a Paz da ONU, de 1992, concretiza essa virada do tratamento da pauta de segurança ao reconhecer que o seu conceito relaciona-se com a instabilidade nos campos econômico, social, humanitário e ecológico (ONU 1992).

Nesse período se registra uma distinção concreta e estruturada entre as finalidades de prevenção e repressão da atuação estatal, em especial a partir dos processos de redemocratização, com o intento de aumentar as liberdades constitucionalmente asseguradas e delimitar o poder punitivo estatal (Buzan 1983; Herman 1996).

O conceito de segurança, dentro dessa perspectiva, também passou por uma expansão e novas ameaças e perspectivas relativas a atores não-estatais foram incluídas, em temas correlatos como a economia, as fronteiras, os recursos naturais, demográficos, energéticos, cibernética, entre outros. Essa mudança, por exemplo, é registrada na estrutura atual de inteligência brasileira, conforme é detalhado nos "Desafios de Inteligência - Edição 2025" (Brasil 2025).

Com a densidade dessas mudanças e a complexidade do tratamento de múltiplas facetas do direito à segurança, o uso de ferramentas tecnológicas, intrusivas ou não, passa a ser uma necessidade para a resposta estatal de concretização desse direito. O impacto das mudanças trazidas pela tecnologia à sociedade demanda uma mudança de como compreendemos o alcance dos direitos fundamentais.

Diferenças entre garantir a segurança da sociedade e do Estado e a segurança pública

Justamente pela complexidade associada ao conceito de direito à segurança, o emprego de ferramentas tecnológicas para sua concretização necessita ser considerado de forma distinta, de acordo com a finalidade preventiva ou repressiva estatal. Como destacamos inicialmente, a finalidade, enquanto propósito da norma, é essencial para definirmos como interpretá-la e aplicá-la (Maximiliano 2003; Ferraz Júnior 1980).

Nesse ponto, a finalidade estatal nos apresenta motivo e motivações distintas para justificar o emprego de FTPIs, razão pela qual nos é importante com-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

preender a diferença entre segurança da sociedade e do Estado e segurança pública e a relação dessas com as finalidades de prevenção e repressão. Isso porque elas exprimem o motivo da atuação estatal, o que reduz o espectro de motivação para o emprego de FTPIs.

Inteligência e a finalidade preventiva da segurança da sociedade e do Estado

A Segurança da sociedade e do Estado é direcionada a garantir a estabilidade e a soberania do Estado, protegendo-o de ameaças externas e internas, de forma a promover a segurança e o bem-estar dos cidadãos (Kent 1949; Platt 1974). Isso requer ações, inclusive sigilosas, direcionadas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o processo decisório nacional, assim como para permitir o adequado planejamento e proteção de conhecimentos sensíveis para as decisões e interesses nacionais legítimos.

Apesar de o texto constitucional não prever de forma explícita a inteligência, ao estabelecer o dever estatal de garantir a segurança e de resguardar a soberania nacional, dentre diversos outros deveres atribuídos ao Estado, há a consolidação implícita da atuação de um sistema de inteligência[21].

Essa expressão do direito à segurança – Segurança da sociedade e do Estado – encontra guarida constitucional no *caput* do art. 5º da CF, e regulação infraconstitucional, em especial, na Lei nº 9.883, de 7 de dezembro de 1999, que institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência como seu órgão central, com atribuições de promover a segurança da sociedade e do Estado e de fornecer os subsídios para o assessoramento estratégico do Presidente da República, o que inclui ações e operações de caráter sigiloso.

As ações estatais de inteligência brasileiras são direcionadas a prevenir o dano e promover oportunidades, ou seja, sempre na perspectiva preventiva e sob o enfoque estratégico para o adequado assessoramento ao processo decisório, que assegure os interesses nacionais legítimos e viabilize a pro-

21 De acordo com a teoria dos poderes implícitos, quando a Constituição concede uma função a determinado órgão ou instituição, também lhe confere, implicitamente, os meios necessários para a consecução das funções que lhe foram atribuídas. Dessa forma, implicitamente, é válido considerar que o texto constitucional abarca a atuação do sistema de inteligência, por estabelecer deveres aos órgãos e instituições que dependem da atuação de um sistema de inteligência. Sobre o reconhecimento da teoria dos poderes implícitos e a imprescindibilidade do serviço de inteligência, confira a jurisprudência do STF (Brasil 2007; 2021a; 2022).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

teção dos conhecimentos sensíveis.

Atualmente, no Brasil, o mapa de ameaças e oportunidades da atividade de inteligência é orientado em uma perspectiva do conceito de segurança pós-Guerra Fria, pela Política Nacional de Inteligência, dentre diversos outros marcos normativos[22], que estabelece:

> **Atividade de Inteligência:** exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado. A atividade de Inteligência divide-se, fundamentalmente, em dois grandes ramos:
>
> **I – Inteligência:** atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado;
>
> **II – Contrainteligência:** atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (Brasil 2016b).

A Estratégia Nacional de Inteligência complementa essa visão por indicar a seguinte finalidade da atividade de Inteligência:

> [...] acompanhar o ambiente interno e externo, buscando identificar oportunidades e possíveis ameaças e riscos aos interesses do Estado e à sociedade brasileira. As ações destinadas à produção de conhecimentos devem permitir que o Estado, de forma antecipada, direcione os recursos necessários para prevenir e neutralizar adversidades futuras e para identificar oportunidades para sua atuação (Brasil 2017a).

O sistema de inteligência existe, assim, para obter dados, processá-los e transformá-los em conhecimento. Para isso é necessário gerir diversos dados de fontes abertas, de bases governamentais de acesso restrito e também dados não acessíveis por outros meios.

22 Vide a Lei nº 11.776, de 17 de setembro de 2008, que dispõe sobre a estruturação do Plano de Carreiras e Cargos da Agência Brasileira de Inteligência - ABIN; o Decreto nº 11.693, de 6 de setembro de 2023, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência; Resolução nº 2, de 2013-CN, que dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI); o Decreto nº 8.793, de 29 de junho de 2016, que fixa a Política Nacional de Inteligência; o Decreto S/N, de 15 de dezembro de 2017, que aprova a Estratégia Nacional de Inteligência; e a Portaria GAB/DG/ABIN/CC/PR no 1.205, de 27 de novembro de 2023, que aprova a Doutrina da Atividade de Inteligência. Esses normativos e outros que ainda seguem necessários de regulamentação são essenciais pela atividade de inteligência fugir à regra da transparência de suas ações, pela necessidade de sigilo, eles possuem regras mais estritas de controle e de *accountability*.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

O compartilhamento de dados dentro do sistema foi debatido pelo STF na ADI nº 6.529 (Brasil 2021a), onde se estabeleceram diretrizes complementares para o fornecimento de dados à ABIN. Sobre os dados não acessíveis por outros meios, o uso de ferramentas tecnológicas, inclusive as intrusivas, é essencial para alcançar desses dados, com o intento de promover a segurança da sociedade e do Estado. Isso porque o cenário internacional demanda ações de inteligência e de contrainteligência para proteger os interesses nacionais legítimos e seus cidadãos no ciberespaço[23], sobretudo quando consideramos o ambiente cibernético como palco de conflito entre serviços de inteligência (Broeders 2024; Nussbaum 2017; Oosthoek e Doerr 2021; Ambros 2024).

O serviço de Inteligência estatal brasileiro serve, assim, para prover informações e conhecimentos essenciais[24] para a tomada de decisão em várias dimensões institucionais, em níveis estratégico, tático e operacional, com impactos positivos nas três esferas de poder, assim como para proteger as atividades do Estado contra tentativas de interferência estrangeira[25] que

23 O STF tem debatido a importância da segurança cibernética para a proteção de direitos fundamentais no julgamento da ADI nº 5527, Min. Relatora Rosa Webber e da ADPF nº 403, Min. Rel. As ações debatem a suspensão do funcionamento, por ordem judicial, de aplicações que fornecem proteção às comunicações (Whatsapp). Em seu voto, o Min. Rel Edson Fachin destacou sete premissas: "Primeira: o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais. Segunda: os direitos que as pessoas têm offline devem também devem ser protegidos online. Direitos digitais são direitos fundamentais. Terceira: a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Quarta: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública. Quinta: A liberdade de expressão tem primazia prima facie e constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito. Sexta: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública. Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas."

24 Vale compreendermos que quando falamos em informações e conhecimentos essenciais, não está inclusiva a divulgação de todo e qualquer dado. O profissional de inteligência processa os dados e possui dever de manter sigilo sobre dados a que obteve acesso, os quais não devem ser divulgados para fins de cumprimento da legislação vigente. Dessa forma, quando hipoteticamente um profissional da inteligência acessa dados que afetam a intimidade, a vida privada ou a privacidade de indivíduos, há o dever de não divulgação dessas esferas na medida em que não é relevante para formação do conhecimento necessário para o cumprimento de suas finalidades preventivas e de assessoramento estratégico. Há diversas decisões do STF (Brasil 2016a; 2024a) que tratam sobre o compartilhamento de dados e o dever de manutenção de sigilo dos servidores públicos que os acessam.

25 Sobre essas formas de ameaças estrangeiras, destacamos algumas estabelecidas na PNI,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

comportam prejuízos ao país e ao bem-estar dos cidadãos.

Dentro da perspectiva de controle e *accountability*, a inteligência conta, atualmente, com o controle externo finalístico realizado *a posteriori,* conforme previsto no art. 6º da Lei nº 9.883, de 1999, pela Comissão Mista de Controle das Atividades de Inteligência (CCAI), do Congresso Nacional[26].

Ressalta-se que, até o momento, a inteligência não possui previsão legal de controle prévio judicial. Essa ausência normativa coaduna com a finalidade da atuação estatal de assegurar o direito à segurança da sociedade e do Estado, justamente por não afetar garantias penais e processuais penais e o direito à liberdade, conforme destacamos em seção anterior[27].

O emprego das FTPIs por esse controle requer que pensemos critérios que permitam ao controle ter a rastreabilidade e auditabilidade adequada para eventual responsabilização por violações de agentes públicos e do sistema de inteligência por suas ações.

Poder punitivo e a finalidade repressiva da segurança pública

Por sua vez, a segurança pública é uma reação formal ao crime, que abarca um conjunto de ações e políticas que o Estado realiza, a partir do seu poder coercitivo, para garantir a ordem pública e a proteção dos cidadãos. Isso envolve a atuação de órgãos e instituições que possuem atribuições de implementar a política criminal no intento de reduzir os índices de criminalidade e ampliar aos cidadãos o espaço efetivo de normalidade para o exercício de direitos e cumprimento de obrigações (Zaffaroni 2007; Zaffaroni *et al.* 2013).

A segurança pública é prevista no art. 144 da CF, que a determina como "*dever do Estado, direito e responsabilidade de todos [...]".* O caput do dis-

tais como espionagem, sabotagem, interferência externa, ações contrárias à Soberania Nacional e ataques cibernéticos.

26 Esse modelo é adotado por outros países, como Estados Unidos da América e Reino Unido. O Brasil, entretanto, ainda carece de maturidade no exercício desse controle pelo Poder Legislativo. Para conferir um estudo comparado de formas de controle da atividade de inteligência, confira Sampaio (2023; 2024e).

27 Vale considerarmos que a decisão do STF na ADI nº 6.529 (Brasil 2021a) ressalta que os órgãos e entidades do Sistema Brasileiro de Inteligência não podem compartilhar diretamente dados obtidos por meio de autorização judicial, justamente por estarem sob segredo de justiça. O debate, entretanto, não adentrou o mérito sobre como e com base em quais critérios a inteligência deve acessar dados que afetem o mapa de direitos fundamentais que possuem reserva de jurisdição para fins de persecução criminal.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

positivo ainda indica que ela *"[...] é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio*", a partir de um rol de órgãos e entidades. Podemos considerar que essa definição não explicita toda a complexidade da segurança pública, o que envolve, ainda, a atuação, além das forças policiais judiciárias, penais e militares previstas no rol do artigo, o Ministério Público, a Defensoria Pública, o sistema prisional e o Poder Judiciário.

As ações de segurança pública, por conseguinte, são direcionadas a reparar e reduzir os danos causados à ordem pública, dentro da perspectiva de controlar o crescimento da criminalidade e promover o ambiente de normalidade para o exercício do contrato social – exercício de direitos e cumprimento de obrigações pelos cidadãos. Tais ações, assim, possuem uma faceta precipuamente repressiva[28].

A estrutura punitiva estatal utiliza-se, principalmente, da polícia judiciária para construção da instrução probatória. Essa atividade é submetida ao controle externo do Ministério Público[29] e ao controle judicial[30], de acordo com a previsão legal de necessidade de autorização prévia para o emprego de determinadas técnicas e meios para obtenção de provas. É preciso considerarmos, nesse sentido, que os critérios para uso de FTPIs segue uma lógica inversa, devido ao controle externo para seu emprego envolver, muitas vezes, a autorização judicial prévia, o que não dispensa a necessidade de critérios de

28 Órgãos e entidades que possuem atuação de repressão estatal, por vezes, detêm competências que somam atuação preventiva. Ocasionalmente, essas ações são baseadas em informações de inteligência, mas isso não consiste, necessariamente, em atuação de inteligência em si. Por exemplo, as polícias militares possuem programas de policiamento ostensivo com o intento de permitir tanto uma atuação imediata de repressão em caso de necessidade, quanto de inibir práticas delitivas pela presença do aparato estatal. A definição dos locais de atuação, assim, pode decorrer de informações obtidas pelo sistema de inteligência, porém o policiamento ostensivo em si não representa uma ação de inteligência.

29 Lei Complementar nº 75, de 1993, art. 9º: "O Ministério Público da União exercerá o controle externo da atividade policial por meio de medidas judiciais e extrajudiciais podendo: I - ter livre ingresso em estabelecimentos policiais ou prisionais; II - ter acesso a quaisquer documentos relativos à atividade-fim policial; III - representar à autoridade competente pela adoção de providências para sanar a omissão indevida, ou para prevenir ou corrigir ilegalidade ou abuso de poder; IV - requisitar à autoridade competente para instauração de inquérito policial sobre a omissão ou fato ilícito ocorrido no exercício da atividade policial; V - promover a ação penal por abuso de poder."

30 O controle judicial decorre da previsão constitucional de reserva de jurisdição prevista nos incisos XI e XII do art. 5º da Constituição Federal: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" e "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

auditabilidade e rastreabilidade para eventual responsabilização por violações de agentes públicos e das estruturas estatais envolvidas por suas ações.

Problemáticas de controle e accountability relacionadas à apropriação do termo inteligência pelo aparato punitivo estatal

Como destacamos acima, a produção de conhecimento de inteligência assumiu funções delimitadas à finalidade preventiva, a partir da formação de uma metodologia de produção baseada no conceito amplo de segurança consagrado pela Agenda da Paz de 1992 (ONU 1992), que somou uma nova visão de como prover apoio às relações externas e de subsidiar o Estado em cenários de guerra e de paz (Buzan 1983; Herman 1996).

Já no final da Guerra Fria, a inteligência havia formado uma base doutrinária clássica, que consolidava essa mudança. Sherman Kent (1949, 3), nesse sentido, definiu inteligência como "conhecimento" indispensável para manutenção do bem-estar e da segurança, na perspectiva do Estado.

Essa mudança de paradigma na inteligência e a consolidação de sua metodologia e técnicas próprias para análise e produção de conhecimento levou, desde o começo desse debate, autores como Washington Platt (1974) a destacarem que inteligência servia a múltiplos setores enquanto uma ferramenta de análise e de produção de conhecimento.

Isso, porém, não torna essas áreas como próprias da inteligência. Diversos órgãos e instituições usam do nome inteligência em uma tentativa de empregar metodologias e técnicas que foram buscadas na inteligência, porém, isso não faz com que a atividade que já desempenhavam e exercem tenha se tornado atividade de inteligência no sentido estrito da atividade estatal de produzir conhecimento para a finalidade que destacamos: garantir a segurança em um sentido amplo, o que inclui o elemento do "bem-estar" destacado por Sherman Kent (1949).

Essa apropriação do termo inteligência por outras atividades estatais e até mesmo no setor privado é presente na atividade policial, o que em parte relaciona-se com a própria construção do que se compreende por direito à segurança. A relação intrínseca entre as finalidades de prevenção e repressão ao início da formação dos sistemas de inteligência leva, por vezes, a dificuldades de definição dos limites de atuação entre o aparato estatal de repressão e de inteligência (Andrade 2012).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Em emprego distinto desses parâmetros, o uso do termo inteligência pela estrutura policial, abarcando definições para "inteligência policial[31]", propicia uma série de confusões entre estruturas de aparato preventivo e repressivo. A Resolução nº 1 de 15 de julho de 2009, que regulamenta o Subsistema de Inteligência de Segurança Pública - SISP[32], por exemplo, define a inteligência policial como

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

A expressão "inteligência policial", por essa definição, atende à finalidade repressiva estatal, pela coleta, obtenção, processamento, análise e disseminação de informações e produtos gerados a partir do emprego de técnicas e meios de inteligência, por integrantes do sistema de persecução criminal, para fins de produção de provas de prática de contravenção ou crime.

A construção de provas para persecução criminal pela estrutura de inteligência é uma prática dissonante à proposta pós-redemocratização de delimitar o poder punitivo estatal para ampliar o exercício de liberdades individuais. Isso porque os espaços de controle e *accountability* das estruturas policiais de persecução criminal e de inteligência são estanques e diferentes, tal como abordado anteriormente, de acordo com essas finalidades estatais e do mapa de direitos fundamentais que atingem.

A confusão conceitual gera espaços em que a própria jurisprudência dos Tribunais Superiores permitiu, por vezes, que a atividade policial chamada de "inteligência policial" deixasse de ser submetida ao controle externo do Ministério Público.

Em 2020, por exemplo, o STF manteve decisão do Superior Tribunal de Justiça (STJ), no qual se definiu que a atividade de "inteligência policial" não se

31 Vale destacar recente proposta distinta de definição de inteligência policial que reduz a confusão entre atuação de investigação criminal e de inteligência, porém, ainda com a mistura do termo "policial", do Projeto de Lei nº 4.120/2024 da Câmara dos Deputados: "Atividade desenvolvida por policial que visa a produção de conhecimento ao processo de tomada de decisão policial, que envolve os processos de coleta, obtenção, análise e disseminação de informações e produtos gerados a partir do emprego de técnicas e meios de inteligência".

32 Vide Decreto nº 3.695, de 21 de dezembro de 2000, que cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

submetia ao controle externo, porque não estaria no escopo da atividade-fim policial descrita no art. 144 da CF[33] (Brasil 2020b; 2018). Verifica-se, assim, uma confusão do que se considera como "inteligência policial" e "inteligência de Estado"[34].

É preciso pensar critérios de controle, de rastreabilidade e auditabilidade adequados para os campos da inteligência e do aparato punitivo estatal, justamente para evitar que ações de instrução probatória para fins criminais sejam realizadas inadequadamente por meio da inteligência, seja com ou sem o uso de FTPIs, em decorrência de os agentes públicos não compreenderem as diferenças de finalidade, motivo e motivação de atuação estatal para promover a segurança da sociedade e do Estado – pela inteligência – e para segurança pública – por meio dos órgãos e entidades que integram o aparato punitivo estatal.

Considerações finais

A regulamentação brasileira sobre o uso de meios e técnicas que possam restringir direitos fundamentais, sejam elas com uso de recursos tecnológicos ou não, é mais restritiva e direcionada ao sistema repressivo, com o objetivo de efetivar garantias penais e processuais penais[35].

A inteligência possui uma lacuna de compreensão de como operacionalizar sua atividade, em especial sobre o seu espectro distinto de impacto aos direitos fundamentais, por não afetar a liberdade individual e as garantias penais e processuais penais. O arcabouço normativo já existente reclama a observação dos limites de direitos fundamentais, todavia, carece de critérios específicos para o acompanhamento do controle externo sobre o uso de meios e técnicas que afetam direitos individuais, dentre elas as que empregam o uso de FTPIs.

Consideraremos aqui, ao menos, seis critérios para definição do uso de FTPI:

33 A fundamentação indica que o art. 129, inciso VII da Constituição restringe os poderes de controle externo do Ministério Público ao disposto no art. 9º da Lei Complementar nº 75, de 1993.

34 Vale ressaltar que STF e o STJ já decidiram anteriormente pela separação estrita dessas atividades, com a declaração de nulidade de provas produzidas a partir do aparato do sistema de inteligência. Nesse sentido, em 2019, o STF julgou HC (Brasil 2017b) impetrado contra RHC do STJ (Brasil 2017c).

35 A aplicação de técnicas e meios que visem à instrução probatória do processo penal, seja no código de processo penal ou em legislação específica, possui diversas limitações legais direcionadas para assegurar as garantias penais e processuais penais.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

motivo, motivação, finalidade, eficácia, eficiência e *accountability*.

1. O motivo decorre da própria compreensão de que o uso dessas ferramentas tecnológicas intrusivas pelo Estado decorre necessariamente em um ato administrativo, que requer motivo, ou seja, situação fática para o seu emprego adequado (C. Mello 1991; 2023).

2. A motivação relaciona-se com o motivo, por explicitar as razões pelas quais o fato demanda o uso de tais ferramentas. Todo ato da Administração Pública deve ser motivado, isso porque a ordem constitucional é de ampliar o exercício de direitos e liberdades, o que requer que o Estado deva agir por estrita permissão legal de restringir esse rol de direitos e liberdades individuais[36].

   A definição de concretização do direito à segurança muda de acordo com o contexto, logo, o ato de motivar é relevante para a compreensão do rol de direitos afetados e para a concretização do direito à segurança no caso concreto, seja pelo sistema de inteligência ou pelo aparato repressivo estatal.

   A delimitação do rol de direitos afetados é essencial para proporcionalidade do emprego da ferramenta no caso concreto. A motivação, assim, precisa evidenciar a necessidade do uso do recurso tecnológico, ao destacar que não é possível obter os dados, informações e conhecimentos necessários para concretizar o direito à segurança dentro da perspectiva preventiva da inteligência, ou de construção das provas necessárias para instrução probatória a partir dos indícios concretos demonstrados, para a finalidade repressiva do exercício punitivo do poder estatal.

3. Outro ponto relevante, para a proporcionalidade da medida, é considerar a eficácia da FTPI para alcançar o objetivo da ação. Isso porque a capacidade desse recurso de alcançar seu objetivo é o que justifica o seu emprego no grau específico em que afeta os direitos e liberdades individuais. Essa capacidade é relevante para definir, por exemplo, a necessidade de o controle ser exercido de forma prévia ou *a posteriori*, no intento de modular o uso da ferramenta e reduzir os danos.

36 Essa necessidade de o Estado motivar seus atos e de agir de forma restrita aos limites permitidos no ordenamento jurídico deriva do princípio da legalidade. Nesse sentido, Censo Antônio Bandeira de Mello (2023, 1-2) explica que "[...] o princípio da legalidade implica subordinação completa do administrador à lei. Todos os agentes públicos, desde o que lhe ocupe a cúspide até o mais modesto deles, devem ser instrumentos de fiel e dócil realização das finalidades normativas. Daí a impossibilidade seja de agirem sem lei que lhes sirva de supedâneo, seja de buscarem fins estranhos aos supostos na lei que invoquem para servir-lhes de calço. [...] O Texto Constitucional brasileiro, ao estabelecer, no art. 5.°, II, que 'ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei', e no art. 84, IV, que compete ao Presidente da República '(...) expedir decretos e regulamentos para sua fiel execução', deixa explícito e com explicitude inobjetável que o princípio da legalidade administrativa é, entre nós, adotado em sua plena extensão, pois, de um lado, proíbe restrições à liberdade individual que não estejam apoiadas em lei e, de outro lado, só admite edição de atos administrativos para cumprimento de lei, já que até mesmo os decretos e regulamentos presidenciais, que são os atos administrativos mais conspícuos, são propostos como simples instrumentos de execução de lei. 4. De outra parte, a exigência de que o ato sirva à fieldade o objetivo legal, sobre ser noção corrente, representa, como é óbvio, a simples afirmação de que a lei deve ser cumprida tal qual é; vale dizer, com obsequioso respeito à sua razão de existir, não se compreendendo que possa ser manipulada como simples pretexto para alcançar fins estranhos aos que visa prover, ainda quando não se trate de fins subalternos."

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

4. A proporcionalidade da medida também possui relação com a eficiência, princípio inserido no art. 37, *caput* da CF. Enquanto expressão da concepção da "boa administração" do direito italiano, a eficiência procura os meios mais adequados para os resultados almejados pelo Estado, o que envolve necessariamente pensar os princípios da legalidade, da economicidade e da celeridade da medida empregada (O. Mello 2010; C. Mello 2015).

   A proporcionalidade do uso da FTPI, portanto, deve considerar a legalidade, a economicidade e a celeridade que ela projeta aos objetivos estatais. O sistema de inteligência, por exemplo, necessita considerar a celeridade em termos de cumprimento da sua finalidade, visto que a informação que deixa de ser ofertada em tempo oportuno não serve mais para o alcance dos resultados pretendidos.

5. A finalidade pode ser preventiva ou repressiva, o que vimos ter, ao menos no contexto atual de concretização do direito à segurança, uma relação intrínseca com a ação ser realizada pela inteligência ou pelos órgãos e instituições que integram o sistema repressivo estatal. Quando a finalidade do uso de tais ferramentas é realizada pelo aparato punitivo, a liberdade individual é afetada; logo, é preciso considerarmos critérios mais estritos de motivação para o ato, por afetar mais direitos fundamentais e ser necessário seguir o rol de garantias penais e processuais penais constitucionais. Por outro lado, quando o uso é realizado pelo sistema de inteligência, o rol de direitos atingidos é restrito aos direitos à intimidade, à vida privada, à inviolabilidade do sigilo das comunicações pessoais e de dados. Nesse ponto, não há o debate sobre o emprego de garantias penais e processuais penais, por não ser destinado à construção de provas que possam afetar a liberdade individual.

6. A *accountability*, por sua vez, soma ainda a perspectiva de capacidade de o Estado promover a prestação de contas, conceder transparência, controlar e responsabilizar ações que fujam ao escopo do motivo, da motivação e da finalidade delineadas. Isso requer estabelecer requisitos que permitam a rastreabilidade e auditabilidade do emprego de ferramentas tecnológicas intrusivas.

Concluímos, destarte, que o uso de tecnologias, sejam elas FTPIs ou não, potencializam a capacidade do Estado de restringir direitos e liberdades individuais. A concretização do direito à segurança, seja em sua faceta de segurança da sociedade e do Estado ou de segurança pública possui especificidades próprias que devem ser observadas para não legitimarmos práticas dissonantes ao regime democrático pelo uso indevido do aparato de inteligência para fins de subsidiar o aparato punitivo estatal. Ademais, para enfrentarmos a problemática de parâmetros para uso de FTPIs na concretização do direito à segurança da sociedade e do Estado e à segurança pública, é preciso considerarmos, ao menos, o motivo, a motivação, a eficácia, a eficiência, a finalidade e a *accountability* para permitir a adequada ponderação, no caso concreto, para a relativização dos demais direitos fundamentais potencialmente afetados.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Referências

ABIN (Agência Brasileira de Inteligência). s.d. *Tecnologia.* Acessado em 15 de outubro de 2024. https://www.gov.br/abin/pt-br/assuntos/tecnologia.

Alexy, Robert. 1993. *Teoria de los derechos fundamentales*. Madri (Espanha): Centro de Estudios Constitucionales.

Ambros, Christiano Cruz. 2024. "Guerra cognitiva e operações cibernéticas de influência: vieses cognitivos como tática de combate." *Revista Brasileira de Inteligência* 19: e2024.19.252. https://doi.org/10.58960/rbi.2024.19.252.

Andrade, Filipe Scarpelli. 2012. "Inteligência Policial: efeitos das distorções no entendimento e na aplicação." *Revista Brasileira de Ciências Policiais* 3 (2): 37-54.

Andrade, José Carlos Vieira de. 1987. *Os direitos fundamentais na Constituição portuguesa de 1976.* Coimbra (Portugal): Almedina.

Arakaki, Ana Carolina Simionato, e Felipe Augusto Arakaki. 2020. "Dados e metadados: conceitos e relações." *Ciência da Informação* 49 (3): 34-45.

ABES (Associação Brasileira de Empresas de Software). 2020. "In Loco adapta sua tecnologia de geolocalização para ajudar no combate à Covid-19." 12 de abril de 2020. https://abes.com.br/in-loco-adapta-sua-tecnologia-de-geolocalizacao-para-ajudar-no-combate-a-covid-19/.

Belli, Luca, Bruna Franqueira, Erica Bakonyi, Larissa Che, Natalia, Chang, Sofia Couto, Nina da Hora, e Walter B. Gaspar. 2023. *Cibersegurança: uma visão sistêmica ruma a uma proposta de marco regulatório para o Brasil digitalmente soberano.* Rio de Janeiro: FGV Direito Rio.

Bobbio, Norberto, Nicola Matteucci, e Gianfranco Pasquino. 2016. *Dicionário de Política.* Vol. 2. 2 vols. Brasília: Editora Universidade de Brasília.

Brasil. 2007. "Medida Cautelar em Mandado de Segurança (MC-MS) Nº 26.547, Min. Rel. Celso de Mello." Supremo Tribunal Federal, 9 de maio de 2007.
Brasil. 2016a. "Ação Direta de Inconstitucionalidade (ADI) nº 2390. Min. Rel. Dias Toffoli" Supremo Tribunal Federal, 21 de outubro de 2016.
Brasil. 2016b. *Política Nacional de Inteligência*. Gabinete de Segurança Institucional da Presidência da República. https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/politica-nacional-de-inteligencia.

Brasil. 2017a. *Estratégia Nacional de Inteligência*. Gabinete de Segurança Institucional da Presidência da República. https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/ENINT.pdf.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Brasil. 2017b. "Habeas Corpus (HC) Nº 147.837, Min. Rel. Gilmar Mendes." Supremo Tribunal Federal, 19 de setembro de 2017.

Brasil. 2017c. "Recurso Ordinário em Habeas Corpus (RHC) nº 57.023, Min. Rel. Min. Sebastião Reis Júnior." Superior Tribunal de Justiça, 16 de agosto de 2017.Brasil. 2018. "Recurso Especial (RESP) nº 1.439.165, Min. Rel. Min. Gurgel de Faria." Superior Tribunal de Justiça, 25 de outubro de 2018.

Brasil. 2020a. "Recurso em Mandado de Segurança (RMS) nº 62143, Min. Rel. Rogério Schietti Cruz." Superior Tribunal de Justiça, 8 de setembro de 2020.

Brasil. 2020b. "Recurso Extraordinário (RE) nº 1.271.855, Min. Rel. Roberto Barroso." Supremo Tribunal Federal, 1º de julho de 2020.

Brasil. 2020c. "Referendo na Medida Cautelar em Ação Direta de Inconstitucionalidade (Ref-MC-ADI) nº 6387, Min. Rel. Rosa Weber." Supremo Tribunal Federal, 12 de novembro de 2020.

Brasil. 2020d. "Habeas Corpus (HC) nº 168052, Min. Rel. Gilmar Mendes." *Habeas Corpus.* Supremo Tribunal Federal, 2 de dezembro de 2020.

Brasil. 2021a. "Ação Direta de Inconstitucionalidade (ADI) nº 6529, Min. Rel. Cármen Lúcia." Supremo Tribunal Federal, 22 de outubro de 2021.

Brasil. 2021b. "Portaria GSI/PR nº 93, de 18 de outubro de 2021." Gabinete de Segurança Institucional. Acessado em 10 de outubro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1.

Brasil. 2022. "Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 772, Min. Rel. Edson Fachin." Supremo Tribunal Federal, 9 de junho de 2022.

Brasil. 2023. "O Ministério Público no controle externo da atividade policial: prerrogativas e limites segundo o STJ." Notícias, Superior Tribunal de Justiça, 26 de fevereiro de 2023. Acesso em 21 de outubro de 2024. https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/26022023-O-Ministerio-Publico-no-controle-externo-da-atividade-policial-prerrogativas-e-limites-segundo-o-STJ.aspx.

Brasil. 2024a. "Ação Direta de Inconstitucionalidade (ADI) nº 7276, Min. Rel. Cármen Lúcia." Supremo Tribunal Federal, 19 de setembro de 2024.

Brasil. 2024b. "Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 1143, Min. Rel. Cristiano Zanin." Supremo Tribunal Federal.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Brasil. 2024c. "Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403, Min. Rel. Edson Fachin." Supremo Tribunal Federal, 11 de dezembro de 2024.

Brasil. 2024d. "Audiência pública n° 39 do Supremo Tribunal Federal: Regulação do uso de ferramentas de monitoramento secreto de aparelhos de comunicação pessoal." 4 de junho de 2024.

Brasil. 2024e. "Inteligência na democracia: desafios e perspectivas para a Agência Brasileira de Inteligência"". — Brasília: Abin, 2024. Acessado em 28 de dezembro de 2024. http://repositorio.enap.gov.br/handle/1/8217.

Brasil. 2025. *Desafios de Inteligência — Edição 2025*. Brasília: ABIN, 2024. Acessado em 5 de janeiro de 2025. http://repositorio.enap.gov.br/handle/1/8216.

Broeders, Dennis. 2024. "Cyber intelligence and international security. Breaking the legal and diplomatic silence?" *Intelligence and National Security* 39 (7): 1213–1229. https://doi.org/10.1080/02684527.2024.2398077.

Broek, Fabian van den, Roel Verdult e Joeiri de Ruiter. 2015. "Defeating IMSI Catchers." CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Nova Iorque (EUA): Association for Computing Machinery. 340-351. https://doi.org/10.1145/2810103.2813615.

Buzan, Barry. 1983. *People, States, and Fear: The National Security Problem in International Relations.* Brighton (Reino Unido): Wheatsheaf Book LTD.

Cellebrite. s.d. *Ufed.* Acesado em 1 de novembro de 2024. https://cellebrite.com/pt/cellebrite-ufed-pt/.

Cole, David. 2014. "Introduction: Watching the Watchers." em *Surveillance Nation: Critical Reflections on Privacy and its Threats. Articles from The Nation 1931-the Present*, por Richard Kreitner. Nova Iorque (EUA): The Nation.

Ferraz Júnior, Tércio Sampaio. 1980. *A Ciência do Direito.* São Paulo: Atlas.

Floyd, Rita. 2007. "Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move." *Human Security Journal* 5 (37): 38-49.

Herman, Michael. 1996. *Intelligence power in peace and war.* Nova Iorque (EUA): Cambridge University Press.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

IFAC (International Federation of Accountants). 2001. *Governance in the Public Sector: a governing body perspective.* Nova Iorque (EUA): IFAC.

Kaspersky Team. 2023. "TriangleDB: the spyware implant of Operation Triangulation." 21 de junho. Acessado em 2 de outubro de 2024. https://www.kaspersky.com/blog/triangledb-mobile-apt/48471/.

Kent, Sherman. 1949. *Strategic Intelligence for American World Policy,* Princeton (EUA): Princeton University Press.

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani e Michael Safi. 2021. "Revealed: leak uncovers global abuse of cyber-surveillance weapon." *The Guardian*, 18 de julho de 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

Martins, Fernando Ramalho. 2006. "Controle: perspectivas de análise na teoria das organizações." *Cadernos EBAPE.BR* 4 (1). https://doi.org/10.1590/S1679-39512006000100008.

Maximiliano, Carlos. 2003. *Hermenêutica e aplicação do direito.* Rio de Janeiro: Forense.

McDowell, Mindi e Matt Lytle. 2019. "Recognizing and Avoiding Spyware." *CISA News*, 19 de novembro de 2009. https://www.cisa.gov/news-events/news/recognizing-and-avoiding-spyware.

McLuhan, Marshall, e Bruce R. Powers. 1992. *The Global Village: Transformations in World Life and Media in the 21st Century.* Oxford (Reino Unido): Oxford University Press.

Mello, Celso Antônio Bandeira de. 1991. *Elementos de Direito Administrativo.* São Paulo: Editora Revista dos Tribunais.

Mello, Celso Antônio Bandeira de. 2015. *Curso de Direito Administrativo.* São Paulo: Editora Malheiros.

Mello, Celso Antônio Bandeira de. 2023. "Legalidade, motivo e motivação do ato administrativo." *Revista de Direito Administrativo, Infraestrutura, Regulação e Compliance* 26: 429-442. https://doi.org/10.48143/RDAI.26.mello.

Mello, Oswaldo Aranha Bandeira de. 2010. *Princípios Gerais do Direito Administrativo.* Vol. 1. 3ª Edição. São Paulo: Malheiros Editores.

NIST (National Institute of Standards and Technology). s.d. "Spyware." *Computer Security Resource Center.* https://csrc.nist.gov/glossary/term/spyware#:~:text=Definitions%3A,a%20type%20of%20malicious%20code.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Nussbaum, Brian H. 2017. "Communicating Cyber Intelligence to Non-Technical Customers." *International Journal of Intelligence and CounterIntelligence* 30 (4): 743-764. https://doi.org/10.1080/08850607.2017.1297120.

Oosthoek, Kris, e Christian Doerr. 2021. "Cyber Threat Intelligence: A Product Without a Process?" *International Journal of Intelligence and CounterIntelligence* 34 (2): 300-315. https://doi.org/10.1080/08850607.2020.1780062.

ONU (Organização das Nações Unidas). 2022. *O Direito à Privacidade na Era Digital: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos.* Trad. Instituto de Referência em Internet e Sociedade (IRIS). Acessado em 5 de 2023. https://irisbh.com.br/wp-content/uploads/2022/12/O-direito-a-privacidade-na-era-digital-Relatorio-do-G.

ONU (Organização das Nações Unidas). 1992. *An agenda for peace: preventive diplomacy, peacemaking and peace-keeping: report of the Secretary-General pursuant to the statement adopted by the Summit Meeting of the Security Council on 31 January 1992 / Boutros Boutros-Ghali*. Acesso em 5 de outubro de 2021. https://digitallibrary.un.org/record/145749?ln=en&v=pdf.

Pinho, José Antonio Gomes de e Ana Rita Silva Sacramento. 2009. "Accountability: já podemos traduzi-la para o português?" *Revista Administração Pública* 43 (6): 1343-1368.

Platt, Washington. 1974. *Produção de Informações Estratégicas.* Rio de Janeiro: Biblioteca do Exército; Livraria Agir Editora.

Sampaio, Ricardo Ramos. 2023. *A possibilidade da realização de vigilância por meio de geolocalização em tempo real pela Agência Brasileira de Inteligência.* Dissertação de Mestrado Profissional. Brasília: Departamento de Engenharia Elétrica, Universidade de Brasília. Disponível em: http://repositorio.unb.br/handle/10482/47955.

Schneier, Bruce. 2018. *Click here to kill everybody: Security and Survival in a Hyper-connected World*. Nova Iorque (EUA) e Londres (Inglaterra): W.W. Norton & Company.

Smanio, Gianluca Martins. 2021. "A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ." *Revista Brasileira de Ciências Policiais* 12 (5): 49-76. Disponível em: http://dspace.mj.gov.br/handle/1/7921.

Tanenbaum, Andrew S. e Hebert Bos. 2016. *Sistemas operacionais modernos.* 4ª Edição. São Paulo: Pearson Education do Brasil.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Thompson, James Westfall e Saul Padover. 1965. *Secret Diplomacy: espionage and Cryptography [1500-1815]*. 2ª Edição. Nova Iorque (EUA): Frederick Ungar Publishing CO.

Varian, Hal R. 1996. "Economic Aspects of Personal Privacy." em *Internet Policy and Economics: Challenges and Perspectives*, por William H. Lehr e Lorenzo Maria Pupillo. Massachusetts (EUA): Springer.

Walker, Jermaine. 2012. "Global Positioning System History." National Aeronautics and Space Administration (NASA). Acessado em 1º de outubro de 2024. https://www.nasa.gov/general/global-positioning-system-history/#:~:text=GPS%20has%20its%20origins%20in,US%20submarines%20carrying%20nuclear%20missiles.

Zaffaroni, Eugenio Raúl, Nilo Batista, Alejandro Alagia e Alejandro Slokar. 2013. *Direito Penal Brasileiro: Teoria Geral do Direito Penal.* 2 vols. Rio de Janeiro: Revan.

Zaffaroni, Eugenio Raúl. 2007. *O Inimigo no Direito Penal*. Rio de Janeiro: Revan.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Artigo de pesquisa

Guilherme Dieguez Candido[1]
ORCiD 0009-0008-8770-7610

Mateus Flach Romani[2]
ORCiD 0009-0006-6481-8495

João Souza Neto[3]
ORCiD 0000-0002-4853-8788

A EXPLORAÇÃO DE FATORES HUMANOS E TECNOLÓGICOS EM CAMPANHAS DE DESINFORMAÇÃO PATROCINADAS POR ESTADOS-NAÇÕES

https://doi.org/10.58960/rbi.2025.20.287

Candido, Guilherme Dieguez, Mateus Flach Romani e João Souza Neto. 2025. "A exploração de fatores humanos e tecnológicos em campanhas de desinformação patrocinadas por Estados-nações," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.287. https://doi.org/10.58960/rbi.2025.20.287.

Recebido em 11/08/2025
Aprovado em 20/10/2025
Publicado em 22/10/2025

1 Bacharel em Engenharia Civil pela Universidade Estadual de Maringá (UEM). Especialista em Ethical Hacking (VINCIT). Discente do programa de mestrado profissional em Segurança Cibernética (PPEE-UnB).

2 Bacharel em Engenharia de Produção pela Universidade de Brasília. Discente do programa de mestrado profissional em Segurança Cibernética (PPEE - UnB). Atua como pesquisador na área de Internet das Coisas - IoT.

3 Doutor em Engenharia Elétrica (UnB), Mestre em Engenharia Eletrônica pelo Instituto Internacional Philips na Holanda. É Pesquisador Associado no programa de Mestrado em Cibersegurança da Universidade de Brasília

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

A EXPLORAÇÃO DE FATORES HUMANOS E TECNOLÓGICOS EM CAMPANHAS DE DESINFORMAÇÃO PATROCINADAS POR ESTADOS-NAÇÕES

RESUMO

O objetivo deste artigo é conduzir uma revisão sistemática da literatura para investigar como atores estrangeiros empregam a desinformação como instrumento de interferência externa. A análise revela que ameaças exploram vulnerabilidades e limitações cognitivas humanas, manipulando vieses emocionais durante períodos de crise para distorcer a percepção da realidade. As mídias sociais e a Inteligência Artificial ocupam posição central nessas operações, viabilizando a amplificação através de bots sofisticados e deep fakes cada vez mais realistas. Uma resposta efetiva demanda a integração de medidas regulatórias, tecnológicas e sociais, incluindo fortalecimento de marcos legais, alfabetização midiática, monitoramento proativo e parcerias entre governo e sociedade civil. O estudo conclui que fortalecer a governança da informação constitui questão estratégica de soberania nacional e preservação democrática.

Palavras-chave: Desinformação, interferência externa, segurança cibernética, mídias sociais, inteligência artificial.

THE EXPLOITATION OF HUMAN AND TECHNOLOGICAL FACTORS IN STATE-SPONSORED DISINFORMATION CAMPAIGNS FOR FOREIGN INTERFERENCE PURPOSES

ABSTRACT

The aim of this article is to conduct a systematic literature review to investigate how foreign actors employ disinformation as an instrument of external interference. The analysis reveals that threats exploit human vulnerabilities and cognitive limitations, manipulating emotional biases during periods of crisis to distort the perception of reality. Social media and Artificial Intelligence occupy a central position in these operations, enabling amplification through sophisticated bots and increasingly realistic deepfakes. An effective response demands the integration of regulatory, technological, and social measures, including strengthening legal frameworks, media literacy, proactive monitoring, and partnerships between government and civil society. The study concludes that strengthening information governance constitutes a strategic issue of national sovereignty and democratic preservation.

Keywords: *Disinformation, foreign interference, cybersecurity, social media, artificial intelligence.*

LA EXPLOTACIÓN DE FACTORES HUMANOS Y TECNOLÓGICOS EN CAMPAÑAS DE DESINFORMACIÓN PATROCINADAS POR ESTADOS-NACIÓN

RESUMEN

El objetivo de este artículo es realizar una revisión sistemática de la literatura para investigar cómo los actores extranjeros emplean la desinformación como instrumento de interferencia externa. El análisis revela que amenazas explotan vulnerabilidades y limitaciones cognitivas humanas, manipulando sesgos emocionales durante períodos de crisis para distorsionar la percepción de la realidad. Las redes sociales y la Inteligencia Artificial ocupan una posición central en estas operaciones, posibilitando la amplificación através de bots sofisticados y deepfakes cada vez más realistas. Una respuesta efectiva demanda la integración de medidas regulatorias, tecnológicas y sociales, incluyendo marcos legales fortalecidos, alfabetización mediática y alianzas entre gobierno y sociedad civil. El estudio concluye que fortalecer la gobernanza de la información constituye una cuestión estratégica de soberanía nacional.

Palabras clave: Desinformación, interferencia externa, seguridad cibernética, redes sociales, inteligencia artificial.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Introdução

À medida que as revoluções da informação transformam a sociedade global, elas naturalmente abrem novos espaços para contestação e conflito (Whyte 2020a). Como afirma a Política Nacional de Inteligência do Brasil - PNI, de 2016:

> A conjuntura mundial tem alterado a percepção e a conduta dos Estados nacionais, das organizações e dos indivíduos, realçando os chamados temas globais e transnacionais. [...] As relações internacionais não se resumem ao exame de temas de convergência e a ações cooperativas [...]. O ambiente internacional caracteriza-se, ao contrário, pela contínua competição entre Estados. Cada um busca melhorar seu respectivo posicionamento estratégico (BRASIL 2016).

A era digital mudou permanentemente a forma como os Estados conduzem a guerra política, exigindo um reequilíbrio das prioridades de segurança nas democracias. A utilização do ciberespaço por atores estatais e não-estatais para subverter eleições democráticas, incentivar a proliferação da violência e desafiar a soberania e os valores dos Estados têm gerado um efeito altamente desestabilizador (Paterson e Hanley 2020). Dependendo do contexto e dos alvos, as consequências podem assumir diversas formas, incluindo o fomento à radicalização e ao recrutamento por grupos extremistas violentos. A intensificação do discurso de ódio em contextos de fragilidade polariza comunidades sociais e políticas (Duarte 2024).

Nas últimas décadas, a proliferação de *fake news* e campanhas de desinformação destinadas a manipular a opinião pública tem sido particularmente intensa durante períodos eleitorais e momentos de conflito militar (López-Cantos 2024). Estados podem aumentar as tensões geopolíticas criando notícias falsas, disseminando boatos ou forjando apoio a agendas próprias (Lapke e Browning 2024). Adversários estrangeiros usam desinformação para promover discursos alinhados aos seus interesses, o que geralmente envolve a disseminação de narrativas falsas que favorecem a nação estrangeira enquanto minam a coesão social e os objetivos políticos da nação-alvo (Vasist e Krishnan 2024). Nações se engajam em conflitos informacionais usando dados frequentemente falsos para obter vantagem sobre adversários. Muitas delas conduzem campanhas encobertas de desinformação no exterior, o que configura interferência externa (Işık *et al*. 2022).

Dentro desse contexto, torna-se cada dia mais evidente a importância do debate sobre campanhas de desinformação patrocinadas ou perpetradas por Estados-nações, incluindo suas especificidades técnicas, especialmente

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

àqueles que lidam com o processo decisório nacional ou seu assessoramento. Compreender como fontes externas de ameaça têm agido no ambiente cibernético para explorar fatores humanos e tecnológicos a fim de interferir na opinião pública nacional é essencial para que o Estado possa traçar estratégias eficazes de prevenção, detecção, obstrução e neutralização destas ações adversas.

Assim, a presente pesquisa teve como principal objetivo mapear, organizar e descrever o conhecimento existente sobre campanhas de desinformação digital patrocinadas por Estados-nações, a fim de auxiliar em práticas de segurança, políticas públicas e melhorias tecnológicas, processuais ou de intervenção que visem seu enfrentamento. Ademais, tem caráter utilitário, direcionado a melhorias tecnológicas, processos ou intervenções em contextos reais.

A abordagem é qualitativa, uma vez que se baseia na interpretação e análise de textos acadêmicos para compreender as táticas, os fatores humanos explorados e o papel das tecnologias em campanhas de desinformação. Possui ainda caráter exploratório e descritivo, pois busca mapear, sistematizar e descrever o conhecimento existente sobre o assunto. O procedimento técnico adotado foi a revisão bibliográfica sistemática, com busca estruturada e critérios de inclusão e exclusão definidos para garantir rigor e reprodutibilidade, que buscou responder às seguintes questões:

1. Como atores estrangeiros exploram fatores humanos para aumentar a eficácia de operações de desinformação digital?
2. Qual o papel das mídias sociais e da Inteligência Artificial nas operações de desinformação para fins de interferência externa?
3. Como táticas centradas no ser humano podem ser modeladas para dar suporte à detecção de ameaças em campanhas de desinformação digital?

Para garantir uma revisão abrangente e reprodutível, adotou-se uma abordagem de busca sistemática baseada em diretrizes estabelecidas para síntese de literatura. A busca foi realizada na base *Scopus*. As consultas de busca foram construídas utilizando combinações de palavras-chave relevantes e operadores booleanos. Exemplos de termos de busca primários incluem: "*disinformation*", "*state sponsored*", "*foreign influence*" e "*foreign interference*". A busca inicial foi limitada a publicações realizadas entre 2020 e 2025; a áreas das Ciências Sociais, Ciência da Computação, Engenharia e Psicologia; e a artigos de periódicos e de conferências, revisados por pares e publicados em língua inglesa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Todos os registros recuperados foram importados para uma ferramenta de gerenciamento de referências e passaram por deduplicação. Títulos e resumos foram analisados de forma independente por dois revisores, com eventuais divergências resolvidas por consenso. Os textos completos dos artigos restantes foram então avaliados com base em critérios de inclusão pré-definidos.

Os critérios de inclusão foram: (1) Estudos que abordem campanhas de desinformação patrocinadas por Estados ou atores estrangeiros; (2) Estudos que investiguem operações de influência ou interferência externa; (3) Trabalhos que analisem o uso de fatores humanos em campanhas de desinformação; e (4) Estudos que discutam o papel das mídias sociais, inteligência artificial ou outras tecnologias digitais em operações de desinformação.

Por sua vez, os critérios de exclusão foram: (1) Estudos que tratavam de estudos de caso ou de países específicos; e (2) Artigos que possuíam acesso restrito. Ao final, foram analisados 29 artigos que atenderam aos critérios de pesquisa. Para avaliar sistematicamente a literatura, dados estruturados foram extraídos de cada artigo selecionado e sintetizados com base nas perguntas de pesquisa.

A exploração de fatores humanos na eficácia de operações de desinformação digital

O termo ciberespaço é geralmente utilizado em referência às interações realizadas por meio da rede mundial de computadores (Paterson e Hanley 2020). Os conflitos informacionais têm sido, até agora, geralmente compreendidos em termos da superfície de ataque dos sistemas de informação e comunicação habilitados em rede (Whyte 2020b). Contudo:

> Os prejuízos das ações no espaço cibernético não advêm apenas do comprometimento de recursos da tecnologia da informação e comunicações. Decorrem, também, da manipulação de opiniões, mediante ações de propaganda e desinformação (BRASIL 2016).

A desinformação e o controle da informação são aspectos fundamentais a serem examinados ao se atribuir o uso intencional de um ataque cibernético com o objetivo de influenciar a opinião pública doméstica sobre um líder ou política de Estado, ou de moldar a percepção internacional sobre determinada questão (Lapke e Browning 2024). O conceito de desinformação é contextualmente relacionado ao de pós-verdade. ‘‘Pós-verdade’’ é um termo que se refere a circunstâncias em que fatos objetivos são menos influentes na formação da opinião pública do que apelos à emoção e crenças pessoais. É conceitualmen-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

te amplo o suficiente para englobar muitas expressões, incluindo *fake news*, informação errônea (*misinformation*) e desinformação (*disinformation*). Um elemento-chave que pode diferenciar estes termos é a intenção (Wu 2023). Informação errônea refere-se a informações incorretas divulgadas de forma não intencional, enquanto a desinformação é composta por informações falsas criadas intencionalmente com o propósito de enganar outras pessoas (Smith 2021). Entretanto, estes conceitos estão profundamente entrelaçados, já que pode ser difícil identificar a natureza da intenção da fonte (García Santamaría *et al*. 2024). Segundo a Doutrina da Atividade de Inteligência:

> A desinformação é o conjunto de ações que dissemina deliberadamente informações falsas, com o intuito de enganar ou confundir público-alvo específico para causar dano, induzir ao erro ou manipular situação ou evento em prol dos interesses do patrocinador. [...] Para ser mais eficaz, a desinformação deve conter elementos de veracidade ou plausibilidade em seu conteúdo (ABIN 2023, 73).

Há uma infinidade de formas pelas quais a desinformação é utilizada nas relações internacionais. Atores estrangeiros utilizam estrategicamente a manipulação emocional, os vieses cognitivos e culturais, as redes de confiança e as limitações do julgamento humano e das máquinas para aumentar a eficácia de seus esforços (Saeidnia *et al*. 2025). Quando orquestrada por Estados ou organizações, especialmente contra outros países, a desinformação se enquadra na guerra informacional (Kumar *et al*. 2025), transformando-se, assim, em uma ferramenta utilizada na disputa de poder em escala global (la Cour 2020).

A desinformação estrangeira opera em uma escala diferente das iniciativas domésticas, representando uma questão entre Estados, com potencial para escalar em disputas diplomáticas ou até mesmo em conflitos armados. Estados que conduzem campanhas de desinformação transfronteiriças geralmente dispõem de orçamentos muito maiores do que os veículos de mídia de países pequenos ou médios, o que evidencia o caráter assimétrico deste tipo de conflito. As campanhas podem fazer parte de estratégias voltadas à desestabilização de outras nações e à criação de condições para uma escalada posterior (Wagnsson *et al*. 2025).

O uso da desinformação para desgastar instituições democráticas tem sido um método amplamente adotado por Estados, pois apresenta custos de implementação relativamente baixos e gera resultados quase imediatos e de difícil reversão. Ataques de desinformação são voltados a corroer a confiança dos cidadãos na autoridade legítima ou no próprio sistema democrático (Ivan *et al*. 2021). Do ponto de vista financeiro, as ameaças cibernéticas baseadas

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

em desinformação representam uma opção atraente para os interesses estratégicos estatais, já que direcionar centenas de *bots* online custa apenas uma fração do que seria gasto com outras opções de defesa ou espionagem (Lapke e Browning 2024).

Uma das características dos conflitos humanos é o desejo de influenciar o processo decisório do adversário e forçá-lo a tomar decisões previamente determinadas pelo lado que exerce a interferência. Isso pode ser alcançado por meio do envio de informações especialmente selecionadas (Ivan *et al*. 2021).

Ataques cibernéticos de desinformação podem infligir danos psicológicos profundos às comunidades, explorando vulnerabilidades humanas (Katagiri 2023). Campanhas exploram emoções e vieses cognitivos - usam artifícios emocionais e retóricos para levar as pessoas a compartilharem e acreditarem em conteúdo falso, muitas vezes convencendo indivíduos a agir contra seus próprios interesses ao semear confusão e desconfiança (Işık *et al*. 2021 2022). Para a ABIN, em sua Doutrina da Atividade de Inteligência (2023), ‘‘adicionalmente às incertezas derivadas dos limites cognitivos, a própria forma como a realidade se apresenta ao ser humano pode ser ofuscada pela desinformação’’. Especialmente quando empregada por atores estrangeiros hostis, a desinformação é criada e disseminada intencionalmente com o propósito de enganar e manipular a opinião pública (Cartwright *et al*. 2022).

Em seu trabalho, Smith (2021) afirma que atores cibernéticos maliciosos estão manipulando o público em períodos de tensões globais, quando os indivíduos estão mais suscetíveis à desinformação. Em 2020, a Organização Mundial da Saúde (OMS) anunciou que o Corona vírus estava acompanhado por uma ‘‘infodemia’’ - uma superabundância de informações (algumas precisas e outras não) o que dificultava que as pessoas encontrassem fontes confiáveis e orientações seguras. A infodemia é um fenômeno que tem alimentado a propagação de ameaças cibernéticas por atores que se aproveitam justamente da confusão provocada por determinados eventos para disseminar informações falsas ao público em geral. Isso resulta na erosão da segurança, da dignidade humana e da equidade no ciberespaço. Eventos trágicos em escala global evocam respostas emocionais e atores maliciosos se aproveitam dessa característica humana.

No mesmo sentido, Duarte (2024) nota que campanhas de desinformação vinculadas a crises emergenciais oferecem condições propícias para operações de interferência contra comunidades, pois é justamente quando elas estão mais vulneráveis. Atualmente, esse tipo de ação é facilitado pelo amplo acesso

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

à Internet e pela proliferação dos meios de comunicação, que se tornaram o meio mais eficaz para transmitir ideologias e ideias. São atividades orientadas por narrativas, utilizando palavras, imagens e ações sincronizadas. Essas campanhas dependem mais do canal que difunde a informação do que da natureza da própria informação. García Santamaría *et al*. (2024) corroboram ressaltando que informações falsas ou enganosas podem ser consideradas críveis se forem percebidas como autênticas e replicadas por redes confiáveis.

Wu (2023) adiciona que a "diplomacia pública da pós-verdade" é uma nova forma de diplomacia pública, que emprega conteúdo gerado por meio de redes sociais, supervisionada por países para interferir nas condições cognitivas e afetivas de públicos em países-alvo. Tem sido praticada principalmente por meio de canais de comunicação na Internet e em dispositivos móveis, transcendendo as fronteiras nacionais.

Smith (2021) destaca que meios de comunicação versáteis dificultam os procedimentos de verificação de fatos (*fact checking*), que não conseguem acompanhar a velocidade com que as informações circulam na Internet. Isso oferece aos cibercriminosos uma flexibilidade ainda maior para espalhar informações falsas que apelam às emoções humanas, por meio de mensagens que transmitem senso de urgência ou imitam figuras de autoridade.

La Cour (2020) constata que aplicar uma abordagem emocional à desinformação é particularmente frutífero, pois a desinformação frequentemente aparece em combinação com discursos de ódio e apelos a emoções como raiva, ressentimento e medo. Watney (2023) acrescenta que mensagens enganosas utilizam imagens ou vídeos fora de contexto, reaproveitados unicamente para alarmar e aprofundar o senso de pânico e ansiedade.

Para Whyte (2020a), operações cibernéticas frequentemente resultam em efeitos sociopsicológicos no nível da população nacional. Tanto os incidentes cibernéticos quanto a imagem de vulnerabilidade generalizada que eles promovem contribuem para um mal-estar informacional popular, em que a confiança pública na origem e na qualidade das informações transmitidas por comentaristas, especialistas e até mesmo por outros cidadãos diminui.

Operações cibernéticas disruptivas são frequentemente um elemento crucial para impedir que vozes democráticas proeminentes assumam um papel direto no combate à desinformação. Para o público em geral, o simples conhecimento de uma interferência externa, ainda que inespecífica, pode reduzir a confiança em atores-chave e instituições relevantes. Ataques cibernéticos

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

são frequentemente direcionados a alvos políticos ou instituições públicas de valor simbólico. Cidadãos que presenciam ataques a alvos de importância nacional costumam interpretar que as ameaças estrangeiras estão sendo dirigidas contra a infraestrutura convencional, em vez da, geralmente mais difícil de conceber, funcionalidade democrática.

Ivan *et al*. (2021) contribuem dizendo que as campanhas de desinformação têm sido usadas no campo social para explorar as oportunidades proporcionadas pelas tecnologias digitais com o objetivo de alcançar fins manipulativos em torno de temas controversos. Estas campanhas estão sendo amplamente utilizadas - às vezes em combinação com outros ataques cibernéticos - por uma variedade de atores domésticos e estrangeiros para semear desconfiança e criar polarização social. Ataques de desinformação têm como objetivo a erosão da confiança dos cidadãos na autoridade legítima ou no próprio sistema democrático, minando os valores culturais compartilhados.

Por fim, Wagnsson *et al*. (2025) afirmam que a necessidade das pessoas se tornarem mais críticas em relação às informações que encontram online baseia-se no que pode ser chamado de teoria da ‘‘verdade padrão’’ (*truth-default theory*), que sugere que os seres humanos são naturalmente inclinados a acreditar nos outros e a presumir que a comunicação é honesta, a menos que existam sinais claros de engano.

O papel das mídias sociais e da Inteligência Artificial nas operações de desinformação para fins de interferência externa

A Estratégia Nacional de Inteligência do Brasil - ENINT, de 2017, define interferência externa como sendo:

> A atuação deliberada de governos, grupos de interesse, pessoas físicas ou jurídicas que possam influenciar os rumos políticos do País com o objetivo de favorecer interesses estrangeiros em detrimento dos nacionais (BRASIL 2017, 17).

Em síntese, a influência e a interferência estrangeiras envolvem esforços encobertos de uma nação para moldar ou desestabilizar os assuntos de outra (Kumar *et al*. 2025). Ao analisar o que muitos têm chamado, nos últimos anos, de ‘‘hackeamento de eleições’’, ‘‘interferência eleitoral’’ e ‘‘ingerência estrangeira’’, estudiosos frequentemente recorrem ao uso de rótulos como ‘‘guerra híbrida’’. De forma ampla, esses termos descrevem o uso de diversos elementos do arsenal estatal de interferência externa a serviço de objetivos estratégicos (Whyte 2020a).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Por sua vez, a Doutrina da Atividade de Inteligência da Agência Brasileira de Inteligência - ABIN, de 2023, conceitua e explica a interferência externa da seguinte forma:

> É uma forma encoberta de projetar poder, tratando-se de um instrumento para influenciar o outro a modificar seu comportamento conforme os interesses do patrocinador da ação. Seu caráter velado serve para moldar os acontecimentos em prol do patrocinador, que precisa se manter oculto como pressuposto para alcançar os resultados desejados (ABIN, 2023).

As ações de interferência externa possuem objetivos estratégicos definidos, que geralmente se concentram no campo político-social ou econômico. No primeiro, entre os diversos objetivos possíveis, a ação pode procurar influenciar diretamente o processo decisório; buscar distrair ou manipular um público específico; minar o capital político e social do adversário; apoiar grupos internos para mudanças de políticas públicas; ou, no extremo, mudar o regime político de outro Estado. No campo econômico, alguns dos objetivos frequentes são prejudicar concorrentes; cercear desenvolvimento tecnológico, econômico ou comercial; estimular boicotes; e desestabilizar mercados (ABIN 2023, 72-73).

Como ressaltado pela PNI (2016), ações que atentem contra a autodeterminação, a não-ingerência nos assuntos internos e o respeito incondicional à Constituição e às leis são classificadas como ações contra a soberania nacional. Desta forma:

> É prejudicial à sociedade brasileira que ocorra interferência externa no processo decisório ou que autoridades brasileiras sejam levadas a atuar contra os interesses nacionais e em favor de objetivos externos antagônicos. A interferência externa é uma ameaça frontal ao princípio constitucional da soberania (BRASIL 2016).

Para a ABIN (2023), "o potencial nocivo de notícias enganosas acompanha o crescimento exponencial da massificação informacional e da sofisticação tecnológica dos recursos digitais, cada vez mais baratos e acessíveis". Para Ambros (2024):

> "Novas tecnologias, [...], como as redes sociais, a Inteligência Artificial e maiores capacidades de coleta e processamento de dados, aumentaram significativamente a sofisticação e a velocidade na exploração do domínio informacional, ao mesmo tempo que diminuíram seus custos" (Ambros 2024, 4).

A disseminação de desinformação como ameaça cibernética é frequentemente realizada por meio da exploração de plataformas de mídia social. Com essas plataformas tendo experimentado um crescimento acentuado tanto no

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

número de usuários quanto no engajamento diário ao longo da última década, utilizar as redes sociais para popularizar uma narrativa ou impulsionar o engajamento em torno de um tema de interesse estatal tornou-se relativamente fácil (Lapke e Browning 2024). Operações frequentemente combinam desinformação com outros ataques cibernéticos, vazamentos de dados e produção de conteúdo inautêntico nas redes sociais. A maioria das contribuições acadêmicas sobre as tendências da pós-verdade enfatiza o papel da Internet e da invenção de novas tecnologias de informação e comunicação como facilitadoras (la Cour 2020).

Os desenvolvimentos tecnológicos transformaram a ecologia midiática, levando a uma crise dos meios de comunicação tradicionais e dando origem a uma grande indústria de desinformação e ciência de baixa qualidade (la Cour 2020). Nas redes sociais, atores exploram e manipulam situações espalhando desinformação e incitando violência para promover suas próprias agendas (Watney 2023), transmitindo mensagens dissuasivas e enganosas que fomentam a confusão pública e a desconfiança em relação a instituições e à ciência (García Santamaría *et al*. 2024). Campanhas de desordem informacional conduzidas online por meio das redes sociais podem impactar de forma imediata dinâmicas políticas, geopolíticas e de segurança. A instrumentalização das mídias sociais é uma prática de fácil acesso para quase todos os atores (Duarte 2024).

Duarte (2024) destaca que a informação falsa se multiplica de forma rápida e barata por meio das plataformas de mídia social. O objetivo principal é moldar a percepção, criando divisões e interferindo em diferentes processos decisórios, com o propósito concreto de alterar dinâmicas sociais e políticas. Logo, para os perpetradores desse tipo de ação, é crucial inundar blogs e redes sociais com *fake news* e narrativas alternativas sobre eventos noticiosos, a fim de dificultar a capacidade da população de distinguir fato de ficção. Assim, a disseminação de narrativas falsas e/ou incitadoras, aliada à sua propagação sistemática por meio das plataformas de mídia social, pode culminar na interrupção, corrupção ou usurpação do processo decisório.

Como ressaltam DiResta *et al*. (2021), as mídias sociais são projetadas para permitir que qualquer pessoa com uma mensagem consiga direcioná-la de forma precisa ao público ideal. Essa capacidade está tão disponível para profissionais de marketing e ativistas políticos legítimos quanto para aqueles que realizam operações de interferência patrocinadas por Estados. Quando as campanhas de desinformação utilizam canais de mídia social, conseguem alcançar populações específicas com muito mais facilidade do que o fariam

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

em canais convencionais de transmissão. Desta forma, agentes de desinformação habilidosos podem personalizar narrativas para públicos específicos. Além disso, os recursos de compartilhamento garantem que publicações atraentes tenham potencial para se disseminar por meio de transmissões *peer-to-peer*, alcançando um público amplo e aumentando a confiança no conteúdo, já que ele é compartilhado por alguém conhecido do destinatário.

Conforme acrescenta Duarte (2024), o enredo se complica ainda mais quando se considera a propagação de "*deep fakes*" nas plataformas de mídia social. *Deep fakes* são simulações digitais de imagem e voz produzidas por meio de *deep learning* no campo da Inteligência Artificial. Esse recurso tecnológico é caracterizado por um alto poder de simulação e realismo. Por isso, é frequentemente utilizado com intenções maliciosas, tanto em crimes cibernéticos comuns quanto em campanhas de desinformação de cunho político e militar. São conteúdos de imagem, áudio ou vídeo editados de forma tão sofisticada que retratam de forma realística personalidades dizendo ou fazendo coisas que, na verdade, nunca disseram ou fizeram. Um deep fake disseminado no momento certo pode ser usado de forma eficaz para enganar eleitores e criar ou agravar tensões políticas, interferindo fortemente ou até mesmo alterando o resultado de eleições democráticas (Paterson e Hanley 2020).

Segundo Paterson e Hanley (2020), os avanços em Inteligência Artificial e aprendizado de máquina também permitem que contas automatizadas em redes sociais se tornem cada vez mais sofisticadas na imitação do comportamento humano. O uso das mídias sociais como parte de operações mais amplas de guerra informacional representa um grande desafio e que os progressos tecnológicos tendem a ampliá-lo ainda mais, trazendo abordagens e ferramentas variadas - como os *deep fakes* - que podem auxiliar na condução de campanhas de guerra política. Os Estados precisam ir além dos métodos tradicionais de coleta de inteligência para garantir que mensagens maliciosas não estejam influenciando negativamente seus cidadãos.

Historicamente, operações de desinformação conduzidas por governos eram realizadas por forças militares ou serviços de inteligência. Mais recentemente, campanhas descobertas em plataformas de mídia social incluem um número significativo de operações terceirizadas que são executadas por contratados ou por exércitos de cidadãos sem vínculo formal com o governo e forças armadas (DiResta *et al*. 2021). Usuários não apenas contribuem para o conteúdo de pós-verdade - seja por causa de seus próprios interesses e perspectivas pessoais ou em nome de outros agentes patrocinadores -, mas também atuam como amplificadores, dispostos e eficazes em gerar impacto direto em públi-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

cos de determinadas localidades ou dentro de redes específicas (Wu 2023).

DiResta et al. (2021) ressaltam ainda que os Estados que decidem conduzir operações de interferência encobertas precisam fazer uma escolha fundamental: planejar e implementar a operação internamente, terceirizar o trabalho para mercenários digitais ou adotar uma combinação dessas estratégias. Mercenários digitais oferecem vantagens significativas. Dão ao Estado acesso a profissionais altamente qualificados que podem gerar economia de recursos, tornar as campanhas mais furtivas e proporcionar negação plausível em caso de exposição. Ao terceirizar, o Estado pode aproveitar mais facilmente novas tecnologias e as práticas mais atuais de marketing digital em redes sociais, aumentando o alcance da campanha de desinformação. Isso inclui estratégias multiplataforma que exploram os recursos específicos de cada mídia social para maximizar a interferência almejada.

Megiddo (2020) relata que pesquisadores também identificaram milícias digitais voluntárias, amadoras ou profissionais, que podem ser remuneradas ou não. Utilizar milícias digitais ou *bots* é útil para ocultar a origem governamental da enxurrada de conteúdo e fazer com que ela pareça mais autêntica e distribuída, ao diversificar o perfil das contas que participam da disseminação da desinformação. Essa prática é conhecida como "*astroturfing*". Além do *astroturfing*, uma tática de abafamento é o "sequestro de *hashtag*", em que uma *hashtag* associada a determinado movimento político é apropriada por seus opositores, que passam a postar em grande escala mensagens contrárias à mensagem original, mas utilizando a mesma *hashtag*. Tanto o abafamento quanto a desinformação podem ser realizados de forma eficaz por meio do uso de *microtargeting*. Muitos sites hoje geram perfis extremamente detalhados dos usuários, o que facilita a veiculação de publicações para grupos-alvo muito específicos, como já mencionado anteriormente.

Para Whyte (2020b), a estratégia de interferência externa depende das ações de vozes significativas já estabelecidas dentro de comunidades de interesse. Às vezes, isso ocorre por meio de indivíduos recrutados. Entretanto, em outros casos, *trolls* utilizam plataformas de mídia social para tentar fazer com que seu conteúdo seja notado, personalizando seu comportamento para atrair alvos específicos. Em essência, trata-se de um *spear phishing* nas redes sociais, cujo objetivo é ser notado e amplificado por outros usuários com presença já consolidada.

Megiddo (2020) concorda dizendo que a amplificação de mensagens é realizada por meio de redes de contas humanas, reais ou falsas, com o apoio de

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

bots ou ferramentas que facilitam significativamente a capacidade de curtir, comentar e compartilhar a partir de várias contas ao mesmo tempo. *Bots*, em particular, têm sido usados para atacar ou silenciar críticos, aumentar o número de seguidores e amplificar as mensagens de candidatos políticos, além de disseminar propaganda e desinformação para manipular a opinião pública.

Atores estrangeiros frequentemente implementam redes de *bots* como tática contra países-alvo - por exemplo, para interferir em eleições, minar a confiança pública ou polarizar debates. Um desafio central para essas operações é justamente evitar a detecção pelas plataformas e pelos usuários do país-alvo. É o que dizem Kumar *et al*. (2025), explicando que campanhas eficazes de desinformação costumam depender de numerosos agentes de perfil discreto em vez de um único mega-influenciador. Numa campanha de interferência externa, o objetivo é espalhar uma narrativa de forma sutil, evitando que qualquer conta falsa se torne tão proeminente a ponto de levantar suspeitas.

Bots costumam se comportar como usuários reais. Como contas influentes de verdade postam com frequência, um bot também postará regularmente - mas apenas até o ponto em que isso não chame atenção. Quem segue ou vê essas postagens pode ser influenciado pelo conteúdo, acreditando que seja uma opinião humana genuína. A vida útil de um bot pode ser longa, mas ele nunca se torna um mega-influenciador. Isso implica que ele pode influenciar muitas pessoas ao longo do tempo, mas permanecendo sempre abaixo do limiar da notoriedade. Usuários humanos e algoritmos têm menos chance de identificar um bot que não está entre as contas mais populares, permitindo que ele continue operando e influenciando opiniões ou espalhando desinformação de forma discreta (Kumar *et al*. 2025).

Modelagem de táticas centradas no ser humano para detecção de ameaças em campanhas de desinformação digital

Conter a disseminação da desinformação e garantir uma infraestrutura cibernética segura deve ser uma prioridade nas agendas estatais (Smith 2021). É o que alerta a PNI (2016) ao mencionar que:

> Há países que buscam abertamente desenvolver capacidade de atuação na denominada guerra cibernética, ainda que os ataques dessa natureza possam ser conduzidos não apenas por órgãos governamentais, mas também por grupos e organizações criminosas; por simpatizantes de causas específicas; ou mesmo por nacionais que apoiem ações antagônicas aos interesses de seus países (BRASIL 2016).

Combater a desinformação envolve uma combinação de estratégias: fortale-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

cer marcos legais contra interferência estrangeira, melhorar a alfabetização midiática e a conscientização pública, implementar ferramentas tecnológicas e promover a transparência nas fontes de informação (Işık *et al.* 2022). Se as operações de guerra informacional têm como objetivo alterar os contornos do ambiente informacional para convencer os cidadãos de que determinado discurso não é confiável ou é obra de "forças obscuras" na sociedade, então uma tarefa crítica para aqueles que buscam modelar a ameaça de forma mais eficaz é mapear o cultivo de narrativas e de temas que atingem tais objetivos (Whyte 2020b).

A redução da superfície de ataque das democracias deve, inevitavelmente, surgir em grande parte de parcerias entre a sociedade civil e o governo. Uma estratégia de dissuasão deve ser aplicada para moldar o comportamento de adversários estrangeiros de forma que seus esforços tenham pouca probabilidade de sucesso (Whyte 2020c). Educar os usuários para reconhecer sinais de desinformação ou de *bots* pode engajar o público na denúncia de contas suspeitas. A vigilância comunitária é uma camada de mitigação que complementa a detecção automatizada (Kumar *et al*. 2025).

Wagnsson *et al*. (2025) comentam que governos e outras organizações têm lançado diversas contramedidas para enfrentar o problema da desinformação disseminada por adversários estrangeiros. Uma forma de mitigar alguns dos efeitos negativos associados à desinformação é informar os cidadãos de que estão "sob ataque". Uma ameaça percebida à comunidade tende a estreitar a identificação com o grupo. Especificamente, a presença de uma ameaça externa à nação deve aumentar a saliência da identidade nacional dos cidadãos, ou seja, fazê-los identificar-se mais fortemente com seu pertencimento nacional. Esse senso fortalecido de coesão nacional deve aumentar as intenções pró-sociais e a confiança dentro do grupo, podendo inibir conflitos entre subgrupos com divisões políticas. A ideia de ativar a identidade nacional, portanto, não é fomentar o nacionalismo, mas sim reforçar o senso de coesão social, incentivando as pessoas a deixarem de lado suas diferenças e a confiarem umas nas outras diante de um desafio comum.

Para Smith (2021), a maneira mais eficaz de conter o avanço da infodemia é adotar uma abordagem centrada no ser humano e orientada por evidências, que busque responsabilizar os atores envolvidos. Esse caminho deve envolver ativamente as vítimas de ataques cibernéticos e o Estado. Também é necessário um esforço para organizar melhor o fluxo de informações e assegurar a existência de órgãos de verificação de fatos em número suficiente para combater a disseminação da desinformação no ciberespaço. Outra consideração

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

importante é a necessidade de garantir que as vítimas de ataques cibernéticos sejam ouvidas, a fim de compreender melhor a natureza desses ataques e seus impactos. As discussões devem ser orientadas para o custo humano da infodemia, resultado da exposição a informações falsas e do aumento da vulnerabilidade às ameaças cibernéticas.

Vasist e Krishnan (2024) afirmam que quando o público e as instituições governamentais se tornam mais conscientes sobre desinformação, torna-se mais difícil para falsidades maliciosas criarem raízes. Campanhas de conscientização, educação para alfabetização midiática e monitoramento proativo por agências de inteligência são ferramentas sugeridas nesse contexto. Uma maior preparação das agências permite identificar operações de desinformação mais rapidamente para neutralizá-las ou desmenti-las antes que se espalhem amplamente. Mecanismos de defesa robustos - desde o compartilhamento de inteligência sobre ameaças de desinformação até a proteção de canais de informação - continuam sendo vitais. Na prática, isso pode significar investir em cibersegurança, monitorar veículos de propaganda patrocinados por outros Estados e tornar públicas as tentativas de interferência externa.

Para Ivan et al. (2021), as sociedades democráticas precisam investir na construção de resiliência e resistência contra essa nova forma complexa de conflito, como por exemplo: (1) criar um sistema deliberativo que informe e mobilize os cidadãos, facilitando a transformação por meio da conscientização, do desenvolvimento de competências e do estímulo ao pensamento reflexivo e crítico; (2) aumentar a capacidade de cooperar no desenvolvimento de uma abordagem adaptativa e coletiva para a detecção de propaganda e desinformação; e (3) promover fluxos de cooperação entre atores governamentais, empresas digitais e de tecnologia, veículos de mídia e organizações da sociedade civil.

Wu (2023) destaca que muitos países já lançaram programas apoiados por inteligência artificial que podem automaticamente filtrar e identificar desinformação ou informação errônea na Internet. Alternativamente, novas leis e regulamentações sobre o funcionamento da mídia - em especial no que diz respeito a seus algoritmos e à proteção da privacidade - deveriam ser criadas para mitigar os impactos negativos gerados pela pós-verdade. A verificação sistemática e constante de fatos, bem como a detecção da "diplomacia pública da pós-verdade" por entidades independentes, sem fins lucrativos e apartidárias, deve ser uma necessidade para proteger o público em geral de ser enganado ou iludido. Treinamentos de alfabetização midiática que aprimorem e sensibilizem os participantes das redes sociais também podem ser úteis.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Por fim, Whyte (2020a) acrescenta que, para que a democracia funcione de maneira eficaz, a informação deve ser disponibilizada ao público de forma que seja possível julgar sua credibilidade, origem e qualidade. No nível mais básico, para que o discurso seja democrático, devem existir métodos que tornem razoavelmente fácil saber de onde a informação provém. Isso significa que interlocutores sociais e políticos não devem ser capazes de ocultar totalmente sua identidade em relação ao discurso público.

Além disso, as fontes factuais da informação devem ser observáveis por meio de uma desconstrução razoável da retórica, opinião e cobertura jornalística analisadas. Mesmo quando há informações limitadas sobre determinado assunto, a cobertura repetitiva por fontes independentes e a contextualização tanto em análises midiáticas quanto em ambientes sociais ajudam a identificar e definir elementos significativos do foco do debate. A inibição de um ecossistema razoavelmente complexo que possibilite a investigação e a interpretação leva à dominação de poucas perspectivas, sem que haja capacidade social para explorar as nuances da questão.

A exploração de fatores humanos e tecnológicos em campanhas de desinformação

A utilização de desinformação nos conflitos internacionais não é uma novidade. Contudo, a franca transição das comunicações para a rede mundial de computadores e o surgimento de tecnologias disruptivas têm direcionado esse tipo de ação para novos domínios, aumentando eficiência e furtividade ao mesmo tempo que reduz custos, trazendo, assim, possibilidades de interferência externa em níveis antes inatingíveis sem o emprego de forças cinéticas.

Os resultados encontrados mostram que Estados-nações estão explorando vieses cognitivos e emoções para aumentar a eficácia das ações de desinformação digital. Isso ocorre particularmente durante períodos de crise e tensões globais, quando as populações ficam vulneráveis e consequentemente mais suscetíveis à desinformação. Os efeitos acabam por transcender a individualidade, produzindo consequências em escala populacional.

Flagra-se particularmente preocupante a capacidade destas campanhas em desgastar a confiança dos cidadãos em informações oficiais oriundas de instituições acadêmicas e estatais, aumentando a proliferação de ciência de baixa qualidade e de narrativas falaciosas, semeando desconfiança e gerando polarização. A possibilidade de atores maliciosos ofuscarem a própria forma como a realidade se apresenta aos indivíduos demonstra a sofisticação das

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

estratégias empregadas para interferir em processos decisórios adversários.

Como introduzido, verifica-se que tecnologias como mídias sociais e Inteligência Artificial têm sido protagonistas nas operações contemporâneas de desinformação voltadas à interferência externa, tornando-se vetores preferenciais para a manipulação da opinião pública. A difusão de conteúdos falsos ou distorcidos ocorre em escala e velocidade inéditas, sustentada por algoritmos de recomendação e engajamento e práticas de compartilhamento entre pares que conferem aparência de legitimidade e autenticidade à informação manipulada.

Saturar as redes com narrativas alternativas, teorias conspiratórias e discursos polarizadores visa não apenas confundir, mas moldar percepções e criar divisões internas. Soma-se a isso o advento dos *deep fakes* e outras formas de geração de conteúdo sintético que permitem criar publicações visuais e sonoras de alta credibilidade; além dos *bots* que ampliam a capacidade de disseminação e interação, impulsionando mensagens, silenciando opositores e forjando consensos.

Destaca-se também que parece haver uma propensão à orquestração na execução destas operações: de um lado, agentes estatais que planejam e supervisionam a campanha; de outro, "milícias digitais" (voluntárias, amadoras ou profissionais) e cidadãos comuns que, vitimados pela desinformação ou movidos por afinidade ideológica, atuam como amplificadores espontâneos. A combinação entre automação, terceirização e mobilização social descentralizada confere às operações cibernéticas de interferência externa um alto grau de resiliência e dificuldade de atribuição, tornando mais complexa a atuação da nação-alvo em ações de contrainteligência.

No que diz respeito ao enfrentamento dessa ameaça, tendo em vista o avanço rápido e constante das tecnologias supracitadas, uma modelagem de táticas centradas no ser humano para a detecção de campanhas de desinformação parece ser o caminho mais promissor a longo prazo. Conscientizar e capacitar a população para essa tarefa demanda a integração de medidas jurídicas, tecnológicas e sociais. Isso implica, por parte do Estado, fortalecer marcos legais contra a desinformação e instituir parcerias entre governo e sociedade civil, incluindo o incentivo ao desenvolvimento de agências independentes de checagem de fatos. Requer, ainda, políticas públicas que abordem alfabetização digital e midiática e mecanismos de denúncia comunitária. A população mais vulnerável deve ser o público-alvo dessas ações, especialmente jovens, idosos e cidadãos com baixa escolaridade que acabam se informando sobre

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

temas relevantes apenas por vídeos, imagens e áudios veiculados por aplicativos de mensageria e mídias sociais.

Entretanto, o Estado não pode aguardar até que a população esteja consciente e capacitada. Tampouco pode transferir aos cidadãos a responsabilidade total da neutralização dessas ameaças. É necessário proteger-se em camadas. Nesse sentido, parece salutar a delegação desta incumbência aos serviços de inteligência, uma vez que possuem o mandato legal e a expertise de contrainteligência necessários para lidar com ameaças externas em ambiente físico e virtual.

Oferecer ao público um serviço oficial de checagem de fatos por parte de agências de inteligência - considerando-se um regime democrático, evidentemente - poderia conferir mais agilidade, profissionalismo e precisão no combate à desinformação digital para fins de interferência externa. Esses órgãos - que já acompanham temas e narrativas promovidos por adversários estrangeiros a fim de identificar padrões, objetivos e indicadores de ameaça - poderiam produzir e difundir alertas públicos através de um portal online, identificando e refutando informações falaciosas que representassem risco à soberania nacional e ao estado democrático de direito. Além disso, poderiam desenvolver e disponibilizar soluções para a identificação de *deep fakes* de vídeo, áudio e de imagens sintéticas ou adulteradas, auxiliando a população na detecção de conteúdo forjado.

Em conclusão, acrescenta-se que fortalecer a governança da informação representa o fortalecimento dos próprios alicerces do Estado diante das crescentes tentativas de interferência externa. A proteção da integridade informacional se mostra, assim, não apenas uma necessidade técnica, mas uma questão estratégica de soberania nacional e preservação democrática.

Conclusão

Ao conduzir uma revisão sistemática da literatura para compreender como Estados-nações empregam a desinformação como instrumento de interferência externa, este trabalho demonstra que este tipo de ação constitui uma das mais preocupantes ameaças contemporâneas à soberania e à estabilidade democrática. Campanhas maliciosas exploram vulnerabilidades cognitivas e emocionais, utilizando *bots*, mídias sociais e Inteligência Artificial para ampliar o alcance e a credibilidade de narrativas enganosas. Como resultado, tem-se na nação-alvo um ambiente informacional em que discernir entre o que é ou não verdadeiro se torna uma tarefa complexa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Frente a esse cenário, a pesquisa reafirma que o enfrentamento à desinformação exige uma resposta que combine instrumentos jurídicos, tecnológicos e educacionais. Não se trata apenas de combater a desinformação após sua difusão, mas de fortalecer a resiliência da sociedade de maneira preventiva. Isso inclui desde a formulação de marcos regulatórios que responsabilizem perpetradores e patrocinadores até políticas públicas de alfabetização digital voltadas à população mais vulnerável.

Ao mesmo tempo, destaca-se a necessidade de envolver a inteligência de Estado nesse esforço. As agências de inteligência, pela natureza de sua missão e por sua capacidade técnica, podem colaborar na detecção antecipada, obstrução e neutralização de campanhas adversas. A criação de canais oficiais de checagem de fatos por estes órgãos, aliada à disponibilização de soluções de identificação de *deep fakes* e outros conteúdos forjados, representa uma forma de auxiliar diretamente a população nacional. Sugestões de pesquisas futuras caminham no sentido de desenvolver metodologias que viabilizem esse tipo de atendimento à sociedade.

Conclui-se, portanto, que o fortalecimento da governança da informação deve ser compreendido como um imperativo de soberania e de segurança nacional. Preservar a integridade do ecossistema informacional é, assim, preservar a própria democracia, não apenas contra a desinformação em si, mas contra a corrosão silenciosa da confiança que sustenta o pacto social e a legitimidade das instituições.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Referências

ABIN (Agência Brasileira de Inteligência). 2023. Doutrina da Atividade de Inteligência. Brasília: ABIN. Governo do Brasil. https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

Ambros, Christiano Cruz. 2024. "Guerra cognitiva e operações cibernéticas de influência: vieses cognitivos como tática de combate." Revista Brasileira de Inteligência, no. 19: e2024.19.252. https://doi.org/10.58960/rbi.2024.19.252.

Brasil. 2017. Estratégia Nacional de Inteligência. Decreto de 15 de dezembro de 2017. Presidência da República. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/legislacao/politica-nacional-de-inteligencia-1/ENINT.pdf

Brasil. 2016. Política Nacional de Inteligência. Decreto nº 8.793, de 29 de junho de 2016. Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm (acesso em 10 de julho de 2025).

Cartwright, Barry, Richard Frank, George Weir, e Karmvir Padda. 2022. "Detecting and Responding to Hostile Disinformation Activities on Social Media Using Machine Learning and Deep Neural Networks." Neural Computing and Applications 34: 15141–15163. https://doi.org/10.1007/s00521-022-07296-0.

la Cour, Christina. 2020. "Theorising Digital Disinformation in International Relations." International Politics 57: 704–723. https://doi.org/10.1057/s41311-020-00215-x.

DiResta, Renée, Shelby Grossman, e Alexandra Siegel. 2021. "In-House vs. Outsourced Trolls: How Digital Mercenaries Shape State Influence Strategies." Political Communication 39, no. 2: 222–253. https://doi.org/10.1080/10584609.2021.1994065.

Duarte, Felipe Pathé. 2024. "'Information Disorder' Campaigns in Natural Hazards and Extreme Events – A Form of Foreign Influence and a Hybrid Threat?" Janus.net 15, no. 1: 322–334. https://doi.org/10.26619/1647-7251.15.1.18.

García Santamaría, Sara, Paolo Cossarini, Eva Campos-Domínguez, e Dolors Palau-Sampio. 2024. "Unraveling the Dynamics of Climate Disinformation: Understanding the Role of Vested Interests, Political Actors, and Technological Amplification." Observatorio (OBS) 18, no. 6. https://doi.org/10.15847/obsOBS18520242605.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Ivan, Cristina, Irena Chiru, e Rubén Arcos. 2021. "A Whole of Society Intelligence Approach: Critical Reassessment of the Tools and Means Used to Counter Information Warfare in the Digital Age." Intelligence and National Security 36, no. 4: 495–511. https://doi.org/10.1080/02684527.2021.1893072.

Işık, İrem, Ömer F. Bildik, e Tayanç T. Molla. 2022. "Securing Elections through International Law: A Tool for Combatting Disinformation Operations?" Journal of Strategic Security 15, no. 4: 106–125. https://doi.org/10.5038/1944-0472.15.4.2033.

Katagiri, Nori. 2023. "Democracy, Firms, and Cyber Punishment: What Cyberspace Challenge Do Democracies Face from the Private Sector?" Australian Journal of International Affairs 77, no. 5: 528–547. https://doi.org/10.1080/10357718.2023.2274443.

Kumar, Saurabh, Valerio La Gatta, Andrea Pugliese, Andrew Pulver, V. S. Subrahmanian, Jiazhi Zhang, e Youzhi Zhang. 2025. "Reinforcement-Learning Based Covert Social Influence Operations." In Proceedings of the ACM on Web Conference 2025 (WWW '25), 2435–2449. https://doi.org/10.1145/3696410.3714729.

Lapke, Michael, e Amy Browning. 2024. "Exploring the Intersection of Cyberthreats and Democratic Backsliding." AMCIS 2024 Proceedings 15. https://aisel.aisnet.org/amcis2024/soc_inclusion/social_inclusion/15.

López-Cantos, Francisco. 2024. "The Drone Warfare: Fact-Checking, Fake--Pictures and Necropolitics." Cogent Social Sciences 10, no. 1. https://doi.org/10.1080/23311886.2024.2426706.

Megiddo, Tamar. 2020. "Online Activism, Digital Domination, and the Rule of Trolls." Columbia Journal of Transnational Law 58: 394. https://doi.org/10.2139/ssrn.3459983.

Paterson, Thomas, e Lauren Hanley. 2020. "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'" Australian Journal of International Affairs 74, no. 4: 439–454. https://doi.org/10.1080/10357718.2020.1734772.

Saeidnia, Hamid Reza, Elaheh Hosseini, Brady Lund, Maral Alipour Tehrani, Sanaz Zaker, e Saba Molaei. 2025. "Artificial Intelligence in the Battle against Disinformation and Misinformation: A Systematic Review of Challenges and Approaches." Knowledge and Information Systems 67: 3139–3158. https://doi.org/10.1007/s10115-024-02337-7.

Smith, Tiffany. 2021. "The Infodemic as a Threat to Cybersecurity." The International Journal of Intelligence, Security, and Public Affairs 23, no. 3: 180–196. https://doi.org/10.1080/23800992.2021.1969140.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Vasist, Pramukh Nanjundaswamy, e Satish Krishnan. 2024. "Powered by Innovation, Derailed by Disinformation: A Multi-Country Analysis of the Influence of Online Political Disinformation on Nations' Innovation Performance." Technological Forecasting and Social Change 199: Article 123029. https://doi.org/10.1016/j.techfore.2023.123029.

Wagnsson, Charlotte, Albin Östervall, e Anton Angwald. 2025. "Naming the Enemy: How to Fortify Society against Foreign Disinformation while Avoiding Excessive Vigilance to Reliable Media." Humanities and Social Sciences Communications 12: 803. https://doi.org/10.1057/s41599-025-04844-6.

Watney, Murdoch. 2023. "Legal Response to Social Media Disinformation on National Level." In Proceedings of the 22nd European Conference on Cyber Warfare and Security, 525–532. https://doi.org/10.34190/eccws.22.1.1106.

Whyte, Christopher. 2020a. "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare." Journal of Cybersecurity 6, no. 1: Article tyaa013. https://doi.org/10.1093/cybsec/tyaa013.

Whyte, Christopher. 2020b. "Of Commissars, Cults and Conspiratorial Communities: The Role of Countercultural Spaces in 'Democracy Hacking' Campaigns." First Monday 25, no. 4. https://doi.org/10.5210/fm.v25i4.10241.

Whyte, Christopher. 2020c. "Protectors without Prerogative: The Challenge of Military Defense against Information Warfare." Journal of Advanced Military Studies 11: 166–184. https://doi.org/10.21140/mcuj.2020110108.

Wu, H. Denis. 2023. "Post-Truth Public Diplomacy: A Detrimental Trend of Cross-National Communication and How Open Societies Address It." The Journal of International Communication 29, no. 1: 20–38. https://doi.org/10.1080/13216597.2022.2162099.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Artigo curto

Tiago Fantini Felicetti[1]
ORCiD 0009-0001-4720-7960
José Roberto Pinho de Andrade Lima[2]
ORCiD 0000-0001-8232-2166

DESAFIOS NA FORMAÇÃO DE RECURSOS HUMANOS EM INTELIGÊNCIA ESTRATÉGICA DE DEFESA

https://doi.org/10.58960/rbi.2025.20.261

Felicetti, Tiago Fantini e José Roberto Pinho de Andrade de Lima. 2025. "Desafios na formação de recursos humanos em Inteligência Estratégica de Defesa," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.261. https://doi.org/10.58960/rbi.2025.20.261.

Recebido em 03/01/2025
Aprovado em 08/10/2025
Publicado em 15/10/2025

1 Oficial de Infantaria do Exército Brasileiro – Academia Militar das Agulhas Negras. Pós-graduado em Ciências Militares – Escola de Aperfeiçoamento de Oficiais. Pós-graduado em Inteligência Estratégica – Escola Superior de Defesa. Especializado em Operações e Pós-graduado em Análise de Inteligência Militar – Escola de Inteligência Militar do Exército.

2 Oficial Veterinário do Exército Brasileiro – Graduado em Medicina Veterinária pela UFBA – Mestre em Ciências Veterinárias pela Université de Montreal (Canadá) – Doutor em Saúde Pública pela UFBA – Pós-doutor em Saúde Global e Ambiental pela University of Florida (EUA).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

DESAFIOS NA FORMAÇÃO DE RECURSOS HUMANOS EM INTELIGÊNCIA ESTRATÉGICA DE DEFESA

Resumo

Este estudo analisa a estrutura de formação de recursos humanos do Exército Brasileiro para a Atividade de Inteligência Estratégica de Defesa. A metodologia baseou-se na análise do modelo atual e em sua comparação com estruturas internacionais. Foram identificadas lacunas que limitam o pleno desenvolvimento dos oficiais, especialmente a ausência de uma instituição de ensino superior voltada ao Sistema de Inteligência de Defesa. Essa deficiência compromete a unificação doutrinária e o crescimento profissional. Conclui-se pela necessidade de uma abordagem mais estruturada, sugerindo-se a criação de uma escola unificada de Inteligência de Defesa ou a centralização dos estudos pelo Ministério da Defesa.

Palavras-chave: Inteligência de Defesa, formação profissional, Exército Brasileiro, Doutrina Militar, Sistema de Inteligência de Defesa (SINDE).

CHALLENGES IN THE TRAINING OF HUMAN RESOURCES IN STRATEGIC DEFENSE INTELLIGENCE

Abstract

This study analyzes the Brazilian Army's human resources training structure for Strategic Defense Intelligence. The methodology was based on examining the current educational model and comparing it to international frameworks. There were gaps identified, which limit the full academic development of officers, particularly the absence of a higher education institution dedicated to the Defense Intelligence System. This handicap hinders doctrinal integration and professional growth within the Armed Forces. The study concludes that there is need for a more structured approach, and suggests creating a unified Defense Intelligence school, or centralizing the academic initiatives under the Ministry of Defense.

Keywords*: Defense Intelligence, skills training, Brazilian Army, military doctrine, Defense Intelligence System (SINDE).*

DESAFÍOS EN LA FORMACIÓN DE RECURSOS HUMANOS EN INTELIGENCIA ESTRATÉGICA DE DEFENSA

Resumen

El presente artículo tiene como propósito examinar la estructura de formación de recursos humanos del Ejército Brasileño en el ámbito de la Inteligencia Estratégica de Defensa. La investigación se fundamenta en el análisis del modelo vigente, complementado por una comparación con estructuras internacionales. Identificanse deficiencias que obstaculizan el desarrollo integral de los oficiales. Entre ellas, destaca la carencia de una institución de educación superior orientada al Sistema de Inteligencia de Defensa. La ausencia representa un desafío estratégico para la consolidación de una política formativa estructurada y centralizada. Así, se plantea la necesidad de implementar un enfoque más sistemático, mediante la creación de una escuela unificada de Inteligencia de Defensa o, alternativamente, la centralización de los programas formativos bajo la coordinación del Ministerio de Defensa.

Palabras clave: *Inteligencia de Defensa, profesionalización, Ejército Brasileño, doctrina militar, Sistema de Inteligencia de Defensa (SINDE).*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Introdução

O Exército Brasileiro (EB), como integrante do Sistema de Inteligência de Defesa (SINDE), possui longa tradição na formação de recursos humanos por meio de sua Escola de Inteligência Militar do Exército (EsIMEx). A trilha de capacitação adotada pela Força busca alinhar-se ao conceito de formação profissional em Inteligência proposto por Platt (1974), que defende uma sequência progressiva na educação, intercalada com a prática, para assegurar a maturação do conhecimento e a experiência profissional.

O SINDE, composto pelo Ministério da Defesa e pelas três Forças Singulares, conta com diferentes centros de formação, como a Escola Superior de Defesa (ESD) (Brasil 2021a; Brasil 2022b) e escolas próprias da Marinha e Aeronáutica. Contudo, o sistema ainda não dispõe de um estabelecimento de ensino superior, com cursos de graduação e pós-graduação, especificamente voltado para a Atividade de Inteligência de Defesa. Essa lacuna estrutural é em parte explicada pela não formalização da atividade como uma carreira, o que restringe o pleno desenvolvimento dos profissionais do setor (Uehara 2013).

Essa ausência de uma estrutura educacional superior específica para a Inteligência de Defesa compromete a consolidação de uma doutrina unificada, o intercâmbio de conhecimento entre as Forças e o desenvolvimento de capacidades analíticas avançadas. Em um cenário internacional caracterizado por ameaças assimétricas, guerras híbridas e crescente complexidade geopolítica, a falta de um corpo técnico-científico especializado enfraquece a capacidade do Brasil de antecipar riscos estratégicos e responder com agilidade a ameaças emergentes. Como aponta Lowenthal (2016), a eficácia da Inteligência Estratégica depende diretamente da formação continuada, da institucionalização do conhecimento e da profissionalização de seus quadros. Sem um sistema formativo robusto e centralizado, o país permanece vulnerável a defasagens tecnológicas, falhas de interpretação de sinais estratégicos e dependência de estruturas fragmentadas, o que compromete sua autonomia decisória em assuntos de defesa e segurança nacional.

O objetivo principal deste artigo é analisar a atual estrutura de formação dos oficiais do Exército Brasileiro e seu aproveitamento na Atividade de Inteligência Estratégica de Defesa. Para isso, o estudo buscou: 1) apresentar os aspectos do modelo de formação vigente no EB; 2) analisar a contribuição desses oficiais para a Inteligência Estratégica de Defesa; 3) comparar tal modelo com os adotados pelas demais Forças Singulares, pela Agência Brasileira de Inteligência (ABIN) e por países de referência, como Estados

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Unidos e Reino Unido; e, por fim; 4) apresentar sugestões para a melhoria da capacitação do profissional de Inteligência do Exército.

Formação de recursos humanos em Inteligência Estratégica de Defesa

A Atividade de Inteligência Estratégica de Defesa constitui o pilar para a formulação de políticas e o planejamento de alto nível no campo da segurança nacional. O conceito de Inteligência Estratégica, conforme definido por Platt (1974), abrange o conhecimento sobre as capacidades, vulnerabilidades e prováveis linhas de ação de atores externos, sendo essencial tanto para a segurança em tempos de paz quanto para a condução de operações militares. No contexto brasileiro, Gonçalves (2008) a específica como a atividade voltada para a produção de conhecimentos que subsidiam o Planejamento Político-Estratégico de Defesa, envolvendo segmentos que transcendem o escopo puramente militar. Essa visão é corroborada por Uehara (2013), que, referenciando o Pentágono, a descreve como a inteligência necessária para criar e implementar a estratégia nacional.

A relevância dessa atividade é formalmente reconhecida pela Estratégia Nacional de Defesa, que estabelece a "Capacidade de Gestão da Informação" como um de seus pilares. O objetivo é garantir "a obtenção, a produção e a difusão dos conhecimentos necessários ao processo decisório" em todos os níveis, contribuindo para a ação preventiva do Estado e para a eficácia das Forças Armadas (Brasil 2020a). Para operacionalizar essa capacidade, foi instituído o SINDE (Brasil 2002), um componente vital do Sistema Brasileiro de Inteligência (SISBIN).

Contudo, uma alteração normativa em 2021 (Brasil 2021b) removeu do órgão central do SINDE - à ocasião, a Subchefia de Inteligência de Defesa do Ministério da Defesa - a competência de promover o desenvolvimento unificado da doutrina de Inteligência e dos recursos humanos. Essa mudança resultou em uma lacuna sistêmica, em que não há mais uma instituição responsável pela coordenação e padronização da formação de pessoal. Segundo Uehara (2013), a ausência de coordenação prejudica o nivelamento de conhecimentos e pode gerar atritos. Corroborando essa visão, Santos (2020) aponta, como falhas críticas na capacidade do SINDE, a falta de uma "educação ampliada e conjunta" e a não estruturação de uma carreira formal de Inteligência de Defesa.

A formação dos profissionais que atuam no SINDE ocorre de maneira descen-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

tralizada, com cada instituição adotando seu próprio modelo e tecnologias educacionais.

No âmbito do Ministério da Defesa, a ESD oferece o Curso Superior de Inteligência Estratégica (CSIE) com o objetivo de "desenvolver competências para o exercício de funções na área de Inteligência Estratégica na Administração Pública" (Brasil 2022a). O curso se destaca por reunir civis e militares de diferentes órgãos do SISBIN, promovendo uma visão ampla da atividade. No entanto, sua contribuição para a formação específica de oficiais do Exército Brasileiro é limitada, com apenas 31 oficiais da ativa possuindo o curso, até 2023. Seu principal requisito de seleção é a experiência prévia na área, sendo destinado a oficiais superiores que, prioritariamente, possuam o Curso de Comando e Estado-Maior (CCEM).

O EB, pioneiro na formação de pessoal, estrutura sua capacitação através da EsIMEx, cuja missão é "especializar oficiais e graduados, habilitando-os ao desempenho de funções" dentro do Sistema de Inteligência do Exército (SIEx) (Brasil 2022b). A arquitetura de ensino é composta por três cursos principais para oficiais:

> 1) Curso Básico: focado em habilitar oficiais para o planejamento e execução de ações de busca e emprego de técnicas operacionais, em nível de equipe e grupo de operações (Brasil 2017);
>
> 2) Curso Intermediário: prepara oficiais para comandar órgãos de Inteligência até o nível de subunidade, e para realizar análises nos níveis operacional e tático (Brasil 2017a);
>
> 3) Curso Avançado: único curso da EsIMEx voltado ao nível estratégico, com o objetivo de habilitar oficiais superiores para funções de chefia em agências de Inteligência e para a realização de análises nos níveis estratégico e operacional (Brasil 2017b).

Apesar dessa estrutura, a formação não segue a trilha progressiva de conhecimento defendida por Platt (1974). Dados do Exército revelam que, dos 148 oficiais da ativa com o Curso Avançado, apenas 35 (menos de 24%) possuem o Curso Intermediário, evidenciando uma quebra na sequência lógica de capacitação.

Dessa forma, pode-se dizer que o Exército Brasileiro prepara, de forma adequada, apenas uma parcela de seus Oficiais para lidar com a Atividade de Inteligência, no nível estratégico, desenvolvida no âmbito do SIEx, colaborando para tentar reduzir ao mínimo as incertezas, além de contribuir com o SINDE e o SISBIN para a integração e o fortalecimento dos Sistemas, ressaltando assim a obrigatória colaboração do Exército para a consecução dos objetivos

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

nacionais, nos assuntos de Defesa.

A Marinha do Brasil (MB) inaugurou recentemente a Escola de Inteligência da Marinha (EsIMar), com o objetivo de aprimorar a profissionalização de seus militares, utilizando um rigoroso processo seletivo que avalia não apenas o conhecimento, mas também o perfil ético e social do candidato (Peçanha 2021). A Força Aérea Brasileira (FAB), por sua vez, ainda não possui uma escola própria, baseando sua capacitação em um programa interno para especializar analistas em Inteligência, Contrainteligência, Inteligência Cibernética e Pesquisa (Brasil 2019).

Em contraste, a Agência Brasileira de Inteligência (ABIN) possui um modelo consolidado através de sua Escola de Inteligência (Esint), que é responsável por todo o ciclo de vida do profissional: formação inicial (etapa obrigatória de concurso), capacitação continuada e aperfeiçoamento ao longo da carreira. A Esint também fórmula e revisa a Doutrina de Inteligência, servindo como um centro de excelência para todo o SISBIN (Brasil 2020b).

A análise dos modelos de formação das Forças Armadas dos Estados Unidos e do Reino Unido, a partir das informações disponíveis nos sites governamentais daqueles países, revela um requisito não funcional fundamental: a Inteligência é tratada como uma carreira desde o início. O ingresso ocorre por meio de academias militares ou programas de formação de oficiais, seguido por um treinamento intensivo e contínuo em escolas de Inteligência de Defesa ou até em universidades civis, como a National Intelligence University (NIU) nos EUA (DIA 2023; NIU 2023; USA 2023; DoD 2023).

No caso do Reino Unido, é preciso primeiro completar um treinamento básico em sua área escolhida. Em seguida, o Oficial é selecionado para o treinamento de Inteligência. Uma vez selecionado para trabalhar na área de Inteligência, o oficial passa por um treinamento intensivo em técnicas de coleta, análise e disseminação de informações nas Escolas de Inteligência de Defesa ou, até mesmo, em Universidades civis (BA 2023; UK 2023).

A formação contínua, incluindo cursos de idiomas e missões práticas, é uma constante, garantindo que o profissional se mantenha atualizado e experiente, um desafio persistente no modelo brasileiro.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Desafios, vulnerabilidades e a necessidade de uma estrutura unificada no Brasil

A estrutura de formação em Inteligência de Defesa no Brasil enfrenta desafios sistêmicos que comprometem sua eficácia. A principal vulnerabilidade é a ausência de uma carreira de Inteligência formal e unificada. No Exército, a dificuldade de criar uma "mentalidade de Inteligência" desde os cursos de formação já foi evidenciada. O Projeto ATENA, que visa ampliar o ensino de Inteligência nas escolas de formação, foi proposto em 2014 (Marques; Holcsik, 2015) e reafirmado em 2020, mas com previsão de conclusão apenas para 2029 (Brasil 2020c), demonstrando a lentidão na implementação de mudanças culturais e curriculares.

Outro desafio crítico é a valorização da experiência. Dados do EB mostram que, dos 148 oficiais com Curso Avançado, apenas 14 possuem o Curso Básico, indicando que a experiência operacional inicial não é um pré-requisito para a formação estratégica. Similarmente, assim como Lima (2017) observou na Marinha, o critério prioritário para o Curso Avançado no Exército é possuir o Curso de Altos Estudos Militares (Brasil 2017c), em detrimento de uma trajetória de carreira específica em Inteligência.

Essa fragmentação resulta em uma falta de "univocidade no currículo e no perfil 'profissiográfico' do analista", entre os principais cursos estratégicos do país, como o CSIE e o Curso Avançado da EsIMEx (Sá Junior; Mota 2012). O problema é agravado pelo rodízio frequente de pessoal, um obstáculo crônico nas Forças Armadas que impede o desenvolvimento de uma cultura funcional sólida e a retenção de conhecimento especializado.

A superação desses desafios exige uma reformulação estrutural. A especialização exigida pela Inteligência moderna, impulsionada por novas tecnologias, torna a qualificação de profissionais uma missão complexa. Diante da escassez de especialistas e do problema do rodízio de pessoal, emerge a proposta de uma solução mais permanente. Silveira (2008) sugere que uma opção para resolver a questão da formação seria "selecionar e preparar o militar desde o início da carreira, criando um quadro estável próprio: a chamada 'Arma de Inteligência'".

A criação de um quadro de carreira específico para a Inteligência de Defesa, inspirado em modelos como o da ABIN e de nações estrangeiras, centralizaria a formação, estabeleceria uma doutrina unificada e garantiria a progressão contínua do profissional. Tal estrutura permitiria a retenção de talentos e a

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

construção de uma memória institucional, fortalecendo a capacidade analítica do SINDE e, consequentemente, a segurança nacional. Essa abordagem transformaria a Inteligência de uma função temporária para uma profissão permanente e especializada, no âmbito da Defesa.

Diante dos desafios identificados, das boas práticas levantadas e de uma visão de futuro sustentável para Atividade de Inteligência, no nível estratégico do setor da Defesa nacional, apresenta-se a seguinte recomendação: a criação de uma Escola de Inteligência de Defesa, centralizada no Ministério da Defesa. Tal instituição seria responsável por unificar a Doutrina, oferecer formação continuada (graduação e pós-graduação) e gerir uma carreira específica para os profissionais das Forças Armadas. Alternativamente, caso a criação de uma nova escola não seja viável a curto prazo, recomenda-se que o Ministério da Defesa assuma a coordenação de estudos para a unificação doutrinária e curricular, promovendo maior sinergia entre as escolas existentes. Ambas as propostas convergem para a necessidade de se estruturar uma carreira de Inteligência de Defesa, garantindo a retenção de talentos e o fortalecimento do SINDE.

Conclusões

Este estudo se propôs a analisar a estrutura de formação de recursos humanos do Exército Brasileiro para a Atividade de Inteligência Estratégica de Defesa, comparando-a com outros modelos nacionais e internacionais a fim de propor melhorias.

A análise revelou um cenário complexo: embora o EB possua uma tradicional e robusta estrutura de capacitação por meio da EsIMEx, sua contribuição para o Sistema de Inteligência de Defesa (SINDE) é limitada por vulnerabilidades sistêmicas.

A principal contribuição deste trabalho é o diagnóstico de lacunas críticas que impedem o pleno aproveitamento dos oficiais de Inteligência. Constatou-se que a ausência de um estabelecimento de ensino superior unificado para a Defesa, a exemplo da Escola de Inteligência (Esint) da ABIN, restringe o desenvolvimento doutrinário e a padronização curricular entre as Forças Armadas. Além disso, a não formalização de uma carreira de Inteligência resulta em alta rotatividade de pessoal e na descontinuidade da especialização, um desafio crônico que enfraquece a memória institucional e a capacidade analítica de longo prazo. O estudo mostrou, ainda, que a progressão na carreira não segue uma trilha lógica de capacitação, priorizando a formação de estado-maior

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

em detrimento da especialização contínua em Inteligência.

Por fim, este trabalho abre caminhos para pesquisas futuras. Sugere-se a realização de um estudo de viabilidade para a implantação da Escola de Inteligência de Defesa, analisando custos, estrutura e modelos de governança. Outra linha de pesquisa pertinente seria uma análise curricular comparada dos cursos oferecidos pela EsIMEx, EsIMar e CSIE, visando identificar pontos de convergência para um futuro currículo unificado. Adicionalmente, estudos qualitativos, envolvendo entrevistas com analistas de Inteligência, poderiam aprofundar a compreensão sobre os impactos da rotatividade de pessoal e as expectativas de carreira, fornecendo subsídios valiosos para a formulação de políticas de gestão de recursos humanos para a Defesa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Referências

Brasil. 2002. Portaria Normativa Nº 295/MD, de 3 de junho de 2002. Institui o Sistema de Inteligência de Defesa, e dá outras providências. https:// arquivos/File/legislacao/emcfa/portarias/295a_2002.pdf. (Acesso em 24 de setembro de 2025).

Brasil. 2017. Portaria nº 471-EME, de 28 de novembro de 2017. Regula o Curso Básico de Inteligência para Oficiais. Brasília, DF. https://images/ arquivos/secoes/cursos/decex/esimex/Port_471-EME28NOV17.pdf. (Acesso em 24 de setembro de 2025).

Brasil. 2017a. Portaria nº 473-EME, de 28 de novembro de 2017. Regula o Curso Intermediário de Inteligência para Oficiais. https://arquivos/secoes/cursos/decex/esimex/Port_473-EME28NOV17.pdf. (Acesso em 24 de setembro de 2025).

Brasil. 2017b. Portaria nº 475-EME, de 28 de novembro de 2017. Regula o Curso Avançado de Inteligência para Oficiais. https://arquivos/secoes/ cursos/decex/esimex/Port_475-EME28NOV17.pdf. (Acesso em 24 de setembro de 2025).

Brasil. 2017c. Portaria nº 476-EME, de 28 de novembro de 2017. Estabelece as condições de funcionamento do Curso Avançado de Inteligência para Oficiais. https://images/arquivos/secoes/cursos/decex/esimex/ Port_476-EME28NOV17.pdf. (Acesso em 24 de setembro de 2025).

Brasil. 2019. Portaria nº 1.153/GC3, de 4 de julho de 2019. Reformula o Sistema de Inteligência da Aeronáutica. https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?. (Acesso em 24 de setembro de 2025).

Brasil. Ministério da Defesa. 2020a. Estratégia Nacional de Defesa. Brasília, DF. https://assuntos/copy_of_estado-e-defesa/estrategia-nacional--de-defesa. (Acesso em 24 de setembro de 2025).

Brasil. 2020b. Escola de Inteligência. https://www.gov.br/abin/pt-br/assuntos/ escola-de-inteligencia. (Acesso em 24 de setembro de 2025).

Brasil. 2020c. Portaria-EME/C Ex nº 243, de 18 de novembro de 2020. Aprova a Diretriz de Iniciação do Projeto ATENA e cria a Equipe para a realização do Estudo de Viabilidade Técnica, Econômica e Ambiental (EVTEA) para o Projeto (EB20-D-08.046). http://outras_publicacoes/01_diretrizes/04_eme/port_243_eme_18nov2020.html. (Acesso em 24 de setembro de 2025).

Brasil. 2021a. Decreto nº 10.806, de 23 de setembro de 2021. Cria a Escola Superior de Defesa. Brasília, DF. https://Ato2019-2022/2021/D10806. htm. (Acesso em 24 de setembro de 2025).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Brasil. 2021b. Portaria GM-MD Nº 3.914, de 22 de setembro de 2021. Dispõe sobre o Sistema de Inteligência de Defesa. https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3914&ANO=2021&SER=A. (Acesso em 24 de setembro de 2025).

Brasil. 2022a. Portaria GM-MD Nº 4.859, de 15 de setembro de 2022. Aprova a Diretriz para o Planejamento e a Execução das Atividades de Estudo, Pesquisa, Ensino, Extensão e Processo Seletivo dos Cursos da Escola Superior de Defesa - ESD para o ano de 2023. https://mdlegis.defesa.gov.br/norma_pdf/?NUM=4859&ANO=2022&SER=A. (Acesso em 24 de setembro de 2025).

Brasil. 2022b. Portaria nº 664, de 18 de novembro de 2022. Aprova o Regulamento da Escola de Inteligência Militar do Exército (R-65). http://www.sgex.eb.mil.br/sg8/001. (Acesso em 24 de setembro de 2025).

BA (British Army). 2023. ‘‘The British Army’’. https://www.army.mod.uk/. (Acesso em 24 de setembro de 2025).

DIA (Defense Intelligence Agency). 2023. ‘‘Defense Intelligence Agency’’. https://www.dia.mil/. (Acesso em 24 de setembro de 2025).

DoD (Department of Defense). 2023. ‘‘U.S. Department of Defense’’. https://www.defense.gov/. (Acesso em 24 de setembro de 2025).

Gonçalves. Joanisval Brito. 2008. ‘‘Sed Quis Custodiet Ipso Custodes? O controle da atividade de Inteligência em regimes democráticos: os casos de Brasil e Canadá’’. Tese de doutorado, Universidade de Brasília, Brasília, DF. http://repositorio.unb.br/handle/10482/1262.

Lima, Marcelo Corrêa. 2017. ‘‘A Inteligência Estratégica na Marinha do Brasil: uma contribuição para a capacitação de Analistas’’. Trabalho de Conclusão de Curso, Escola de Guerra Naval.

Lowenthal, Mark. 2016. Intelligence: From Secrets to Policy. 7th ed. Washington, DC: CQ Press.

Marques, Fernando Rodrigues e Eduardo Holcsik. 2015. ‘‘O Ensino de Inteligência nas Escolas de Formação: a função de combate Inteligência nas Operações no amplo espectro’’. Revista a Lucerna, VI: 3-15.

NIU (National Intelligence University). 2023 ‘‘National Intelligence University. https://ni-u.edu/wp/. (Acesso em 24 de setembro de 2025).

Peçanha, Wallace da Silva Henriques. 2021. ‘‘A Contrainteligência na preservação dos interesses do Estado – a importância da modernização do Sistema de Inteligência da Marinha para a tomada de decisão’’. Monografia, Escola de Guerra Naval.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.261
ISSN 2595-4717

Platt, Washington. 1974. A produção de informações estratégicas. Trad. Álvaro Galvão Pereira; Heitor Aquino Ferreira. Rio de Janeiro: BIBLIEX.

Sá Junior, Gerson e Ricardo Marques Mota. 2012. "Sugestões para a Inteligência de Defesa deste século". Coleção Meira Mattos, Revista das Ciências Militares 3, n. 27: s.p.

Santos, José Fernando D'Amorim. 2020. "As atuais capacidades de Inteligência de Defesa do Reino Unido e do Brasil: uma comparação". Trabalho de Conclusão de Curso, Escola Superior de Guerra-Campus Brasília.

Silveira, Jorge Armando de Almeida. 2008. "Sistema de Inteligência de Defesa: A importância da Inteligência Estratégica no âmbito do Ministério da Defesa". Revista da Escola Superior de Guerra 24, n. 49: 80-104.

Uehara, Satoru. 2013. "A capacitação para a atividade de Inteligência de Defesa: Escola de Inteligência de Defesa". Monografia, Escola Superior de Guerra.

UK (United Kingdom). 2023. "Ministry of Defence". https://www.gov.uk/government/organisations/ministry-of-defence. (Acesso em 24 de setembro de 2025).

USA (United States Army). 2023. "The United States Army". https://www.army.mil/. United States Army. (Acesso em 24 de setembro de 2025).

Esta revista foi impressa nas oficinas gráficas da ABIN em dezembro de 2025.

O texto e os títulos da obra foram compostos em Roboto Flex (fonte licenciada pelo Google Fonts).

CASA CIVIL

GOVERNO DO

BRASIL

DO LADO DO POVO BRASILEIRO