

# É DEVER DE TODO PROFISSIONAL DE INTELIGÊNCIA ALERTAR? Características e potencialidades de aplicação da Inteligência de Alerta

DOI: <https://doi.org/10.58960/rbi.2023.18.231>

Iêda Maria Toledo Silveira \*

## Resumo

Originalmente, a alteridade da Inteligência de Alerta (IA) ou da Inteligência Indiciária é o inimigo, o país inimigo, o exército inimigo. Como a proposta deste estudo é apoiar a tese de utilização da IA para além do universo militar, sugere-se que o inimigo seja substituído por adversário, elemento hostil, ameaça, fator adverso ou antagônico. Para a aplicação da Inteligência de Alerta, em uma dada situação, atores antagônicos, suas intenções, motivações e meios devem ser mapeados e permanentemente monitorados para, a partir de determinados indícios, integrarem a emissão de um alerta a fim de antecipar-se uma ameaça ou uma oportunidade. A IA é distinta da Inteligência Corrente, da Inteligência de Base ou da Inteligência Prospectiva e tem como principal aspecto doutrinário uma metodologia específica, traduzida neste trabalho como metodologia indiciária (*"Indications and Warning"* – I&W). Entendida em suas características distintas e aplicada adequadamente, a IA tem potencial de ampliar e aprimorar a qualidade do assessoramento realizado pela Inteligência no Brasil.

**Palavras-chave:** inteligência de alerta; inteligência indiciária; metodologia indiciária.

## IS IT THE DUTY OF EVERY INTELLIGENCE PROFESSIONAL TO WARN? Characteristics and possible applications of warning intelligence

### Abstract

*The otherness in Warning Intelligence (WI) or in Indications Intelligence (II) is originally the enemy, the enemy country, the enemy Army. As the purpose of this study is to support the thesis that WI should not be confined to the military universe, the concept of enemy will be replaced with adversary, hostile actor, threat, antagonistic or adversarial factor. In a given situation, the WI must identify and monitor antagonistic actors, their intentions, motivations and means in order to determine indications that will be part of a warning, anticipating a threat or an opportunity. The II is different from Current Intelligence, from Basic Intelligence or from Estimative Intelligence; the II has a specific methodology known as "Indications and Warning" (I&W) as main doctrinal aspect. If the WI is understood in all its distinctive characteristics and properly applied, it has the potential to expand and enhance the quality of Intelligence in Brazil.*

**Keywords:** warning intelligence; indications intelligence; indications and warning (I&W) methodology.

---

\* Bacharel e Licenciada em Geografia pela Universidade de São Paulo (USP). Bacharel em História pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Mestre em História Social pela USP. Oficial de Inteligência da Agência Brasileira de Inteligência (Abin).

## ¿ES DEBER DE TODO PROFESIONAL DE INTELIGENCIA ALERTAR?

### Características y potenciales de aplicación de la Inteligencia de Alerta

#### Resumen

*Originalmente, la alteridad de la Inteligencia de Alerta (IA) o de la Inteligencia Indiciaria (II) es el enemigo, el país enemigo, el ejército enemigo. Como la propuesta aquí es defender la tesis de utilización de la IA no solamente para el universo militar, se sugiere que el enemigo sea sustituido por adversario, elemento hostil, factor adverso o antagónico. Para la aplicación de la Inteligencia de Alerta en una dada situación, actores antagónicos, sus intenciones, motivaciones y medios deben ser mapeados y permanentemente monitoreados para, a partir de determinados indicios, hacer parte de la emisión de una alerta con el objetivo de anticipar amenazas u oportunidades. La IA es distinta de la Inteligencia Actual, de la Inteligencia Básica o de la Inteligencia Prospectiva, y la primera tiene como principal aspecto doctrinario una metodología específica que ha sido traducida aquí como metodología indiciaria ("Indications and Warning" – I&W). Entendida en sus características distintivas y aplicada de manera adecuada, la IA tiene el potencial de ampliar y mejorar la calidad del asesoramiento de Inteligencia en Brasil.*

**Palabras clave:** inteligencia de alerta; inteligencia indiciaria; metodología indiciaria.

## Introdução

*“You did not tell me this was going to happen. We were not led to expect this and were surprised”*. Cynthia Grabo, sobre a crítica mais comum dos tomadores de decisão em relação à Inteligência (2015, p. 42).

O objetivo desse estudo é interpretar a vertente analítica descrita pela Comunidade de Inteligência dos Estados Unidos da América (EUA) como *Warning Intelligence* ou *Indications Intelligence*, traduzidas como Inteligência de Alerta (IA) ou Inteligência Indiciária, e analisar como a IA pode contribuir para as atribuições de assessoramento do Sistema Brasileiro de Inteligência (Sisbin). Avaliar a IA obriga a tratar de seus tangenciamentos com a Inteligência Corrente (IC) e a Inteligência Prospectiva (IP<sup>1</sup>), ou mesmo com a Inteligência de Base (IB – *“Basic Intelligence”*). Desse modo, complementarmente, a ótica comparativa fará parte deste trabalho, sobretudo pela necessidade de diferenciação entre IA e IC. A hipótese inicial é que a distinção entre essas tipologias da Inteligência e a própria caracterização da IA podem se dar à luz de uma perspectiva temporal: do passado aos futuros possíveis. Como será demonstrado, a hipótese pôde ser comprovada.

Além desse recorte cronológico para separar os ramos da Inteligência, foram abordados

mais dois enfoques temporais: os fatos históricos que marcam o nascimento e a trajetória da Inteligência de Alerta; e a linha do tempo utilizada pelo profissional de Inteligência para a coleta, a análise da trajetória e o assessoramento.

Toda a fundamentação da IA está nas clássicas balizas historiográficas das obras de Cynthia Grabo, que convergiram para o *Handbook of Warning Intelligence*, periodicamente atualizadas desde seu ofício como analista nos anos 1940 a 1970, até 2015, quando seus manuscritos foram totalmente desclassificados pelo governo estadunidense. Como contraponto e, ao mesmo tempo, continuidade da interpretação da IA, está o livro de John A. Gentry e Joseph S. Gordon, *Strategic Warning Intelligence* (2019), que amplia o espectro metodológico e temático da Inteligência de Alerta, com ênfase no nível estratégico e não mais centrado em assuntos militares. Gentry e Gordon, acadêmicos e, respectivamente, ex-analistas da CIA e da Agência de Inteligência de Defesa (Defense Intelligence Agency -DIA), utilizam ampla bibliografia sobre Inteligência e IA, esta última bastante atualizada desde o livro de Grabo, datado do início dos anos 1970.

Adicionalmente, alguns artigos serviram como referência dialógica para a explicação do método indiciário, sobretudo em referência aos aprimoramentos necessários

1 Ao compararem a Inteligência de Alerta com outras tipologias da Inteligência, como a IC (*“Current Intelligence”*) ou a IB (*“Basic Intelligence”*), os principais autores analisados também diferenciam a IA da Estimativa (*“Estimative Intelligence”*). No entanto, como, para a Doutrina de Inteligência no Brasil, estimativa é um tipo documental, e não um ramo da Inteligência, optou-se por traduzir *“Estimative Intelligence”* como Inteligência Prospectiva.

para o assessoramento de natureza antecipatória.

Além da introdução e do encerramento, o artigo está dividido em quatro seções: uma primeira aborda a IA sob as perspectivas histórica e historiográfica; na segunda, explica-se o método indiciário e as características e atributos que fazem um bom analista de IA e, na sequência, analisa-se a Inteligência Indiciária em seu papel de assessoramento. Por fim, há um mapa com os principais conceitos e características que integram o Ciclo de Produção e Difusão da Inteligência de Alerta, conforme proposto neste estudo.

## A Inteligência de Alerta em perspectiva histórica e historiográfica

A concepção de Inteligência de Alerta ou Indiciária, concernente àquilo que o adversário está prestes a realizar, foi sendo construída por imposição dos acontecimentos e das necessidades dos usuários. Nascida formalmente após a 2ª. Guerra Mundial, a IA torna-se estratégica durante a Guerra Fria, como instrumento de antecipação e monitoramento dos movimentos dos países integrantes do bloco soviético e permanece atual no contexto das guerras assimétricas.

Na linha do tempo que delimita a trajetória de países e indivíduos, o ataque do Japão a Pearl Harbor, em 1941, significou um múltiplo ponto de inflexão: determinou

não apenas o ingresso dos EUA na 2ª. Guerra Mundial, mas também a gestação do que ficaria conhecida, na Comunidade de Inteligência dos Estados Unidos, como IA ou Inteligência Indiciária. Era também o começo das atividades de Cynthia Grabo como profissional de Inteligência, que duraram de 1942 a 1980. Ela fora recrutada pela Inteligência do Exército depois do ataque japonês; tornou-se especialista em IA a partir de 1949 e, entre 1950 e 1975, atuou como pesquisadora sênior no *National Indications Center*, uma unidade entre agências, e, em sua organização sucessora, o *Strategic Warning Staff*, que não existe mais. A vida da autora estadunidense é indissociada da história e da metodologia da Inteligência de Alerta.

A experiência e o conhecimento adquiridos por Grabo foram reunidos na publicação da DIA *Handbook of Warning Intelligence*, três volumes escritos de 1972 a 1974 (433 páginas), mas que permaneceram por décadas indisponíveis ao público. Apenas em 2002, Grabo viu parte de sua obra ser desclassificada pelo *Joint Military Intelligence Collegé's Center for Strategic Intelligence Research*, sob o nome de *Anticipating Surprise: Analysis for Strategic Warning* (com apenas 175 páginas). Até então, a obra, escrita para ensinar novos analistas a como ler, escrever e analisar IA, era classificada como secreta e permanecera como propriedade do governo estadunidense.

Essa decisão pela desclassificação parcial, em 2002, não foi coincidência. Tanto o ataque a Pearl Harbor, em 1941, quanto às Torres Gêmeas em Nova Iorque e ao Pentágono, 60 anos depois, são considerados problemas de alerta (“*warning problems*”): representaram falhas de antecipação em todas as dimensões da ameaça inimiga, ainda que tenham sido de naturezas distintas. No primeiro caso, o clássico exemplo de antagonismo interestatal, ainda que sem declaração formal de guerra; no segundo, o conflito entre atores estatais e atores não estatais: dois ataques-surpresa.

Apesar do reconhecimento do valor dessa perspectiva metodológica para o assessoramento de Inteligência, dos vários artigos sobre IA escritos a partir dos anos 2000, e da persistência da autora em ver sua obra publicada na íntegra, apenas em 2015, surgiria a versão completa e desclassificada do *Handbook of Warning Intelligence*, utilizada aqui como substrato para a caracterização do tema. Conforme a referência bibliográfica, a obra foi publicada com Jan Goldman, professor de Inteligência e Segurança Nacional nos EUA, pois Grabo falecera em 2014, aos 98 anos.

## Aspectos axiológicos da Inteligência de Alerta

Após os atentados de 11 de setembro de 2001, o mundo parecia ter alterado a

natureza do problema de alerta: primeiro, com o colapso do comunismo na URSS e nos países do leste europeu; depois, com a emergência da ameaça terrorista em solo estadunidense. A despeito disso, os problemas analíticos afetos à IA, bem como a natureza de suas falhas, permaneciam os mesmos: percepção equivocada das ameaças emergentes; coleta inadequada de informações sobre essas mesmas ameaças; colapso da comunicação entre agentes de campo, analistas e agências de Inteligência; desconsideração de pontos de vista divergentes (dissenso); vulnerabilidade ao engano e à dissimulação (“*denial and deception*” – D&D – GRABO, 2002).

Apesar da permanência desses mesmos desafios, a definição da Inteligência de Alerta não permaneceria a mesma ao longo da história e viria a ser ampliada para além da antecipação de uma ameaça externa iminente pelas mãos do analista sênior da CIA Jack Davis, após os ataques de 11 de setembro. Primeiro, o autor define a Inteligência de Alerta, principalmente, em linha com dois aspectos consoantes à tradição de Grabo: a) a IA só se efetiva na comunicação com o cliente; sem a expressa ciência do decisor, ou a IA não existe ou fracassa; b) o objetivo do alerta é “prevenir a surpresa estratégica” (DAVIS, 2002 A, p. 3).

Em seguida, em um aprofundamento do conceito, Davis (2002 A) destaca o elemento inédito que seria, décadas

depois, reconhecido como mérito seu em outras interpretações sobre a IA. Para o autor estadunidense, mais do que avisar o cliente sobre algo que ocorrerá, é preciso alertá-lo para que tome todas as medidas cabíveis e possíveis caso a ameaça de fato se concretize, ou seja, a surpresa pode ser inevitável (DAVIS, 2002 A).

Essa ênfase na prontidão (*“readiness”, “preparedness”*) para afastar ou minimizar prováveis danos se tornaria central no conceito lapidado pelo mesmo autor em artigos subsequentes. Davis (2003) conclui que análises críticas sobre a missão da IA devem reconhecer a prioridade em se evitar ou limitar o dano previsto, e não, de forma talvez pouco realista, buscar evitar a surpresa, como estava em sua primeira definição. Posteriormente, repete que a história comprova a tese da dificuldade em se evitar surpresas, sobretudo as táticas (DAVIS, 2007).

Na década seguinte, outras interpretações mantiveram essa conceituação do autor sobre a Inteligência de Alerta. Kimmelman (2017) inspirou-se na referência conceitual e nos objetivos da IA definidos por Davis para adaptar a metodologia aos desafios da segurança doméstica. Já Gentry e Gordon (2019), na obra que é o outro substrato basilar desse artigo, citaram Davis ao enfatizar a natureza do assessoramento de alerta, ou seja, assistir os decisores na adoção “de medidas defensivas e preemptivas contra ameaças futuras, e de

ações de defesa contra ameaças iminentes” (GENTRY & GORDON, 2019, p. 11).

Observa-se, assim, como a antecipação da ameaça, a comunicação com o usuário e a prontidão de resposta complementam o princípio da oportunidade, tal como entendido pela Doutrina Nacional de Inteligência (BRASIL, 2016).

## Alertas estratégicos e alertas táticos

A Inteligência de Alerta estratégico é diferenciada da Inteligência de Alerta tático em termos de espectro temporal, objeto e forma de assessoramento. Para alguns autores, apenas o alerta estratégico está no campo da Inteligência de Estado.

Em Grabo (2015), não aparece o termo “estratégico” no título, talvez porque, para ela, o alerta tático não seria Inteligência de fato. Diferenciados em termos do alcance temporal, a autora afirma que o alerta estratégico é relativamente de longo prazo, emitido com antecedência de semanas ou meses: “Na prática, não é o reconhecimento da iminência da ação, mas o reconhecimento da probabilidade de ocorrência da ação” (GRABO, 2015, p. 11-12). Ademais, a função própria da IA seria estratégica, no sentido já descrito: ou o alerta é emitido com antecedência suficiente para o decisor agir – independentemente do adjetivo que o acompanhe – ou terá falhado.

Em Gentry & Gordon (2019), o qualificador “estratégico” está no título, e a diferenciação clarifica-se quando analisam os atentados de 11 de setembro. Em sua avaliação, os ataques surpresa ocorreram por uma falha de Inteligência de Alerta tático, pois, em termos estratégicos, há muito o governo estadunidense estava avisado de que seus interesses eram alvo da al-Qaeda. Assim como Grabo, distinguem o alerta estratégico pela natureza do assessoramento: apoia políticos sêniores e chefes militares em nível decisório nacional, e é distinto, portanto, do nível operacional ou tático. Por isso, quando mencionam alertas, afirmam sempre referir-se aos estratégicos, pois os táticos dizem respeito à notificação de uma ameaça militar iminente.

Os dois autores, mesmo em reconhecimento à crescente dedicação dos serviços de Inteligência ao contraterrorismo (CT) depois do 11 de setembro, mantêm a instância tática fora do âmbito da Inteligência. Admitem que muitas agências criaram o papel do “*targeting analyst*”, em apoio às operações de CT, mas “essas funções se sobrepõem e às vezes causam fricção dentro das organizações analíticas” (GENTRY & GORDON, 2019, p. 12).

Por sua vez, Davis (2003) diferencia os níveis tático e estratégico, mas os vê como complementares e típicos da Inteligência. Por um lado, coloca CT e crime organizado no nível dos alertas táticos, ao lado de

ataques militares, ameaças relativas a armas de destruição em massa e crises políticas externas. Segundo o autor, a IA tática envolve diagnósticos sobre incidentes específicos, perpetradores, alvos, modalidades e *timing*, pois responde previamente às questões “quando, onde e como” um potencial adversário atacará. O autor não questiona, portanto, sua natureza de Inteligência e destaca a interligação entre ambos: “um bom alerta estratégico tem o potencial de aprimorar tanto o alerta tático quanto a prontidão”. E vai além: “um alerta estratégico robusto serve como suplemento analítico indispensável ao alerta tático” (DAVIS, 2003, p. 3-4). Ele insistiria nessa mesma correlação anos mais tarde (DAVIS, 2007).

Além do fator cronológico (curto e longo prazos) e do tipo de assessoramento, outro binômio que caracteriza alertas táticos e estratégicos refere-se a seus objetos. Alertas táticos referem-se a aspectos tangíveis, a quebra-cabeças, como os que explicam o trabalho dos profissionais de CT. Já “o alerta estratégico é sobre adivinhar o significado de importantes mistérios da arena internacional (...), que são questões analíticas para as quais ainda não há respostas objetivas” (GENTRY & GORDON, 2019, p. 21-22).

## O ciclo de Inteligência de Alerta

Em maior ou menor grau, os autores

que se dedicaram à IA reconhecem que uma das peculiaridades complexas dessa corrente analítica reside na articulação entre todos os atores envolvidos no que será aqui definido como Ciclo de Produção e Difusão da Inteligência de Alerta.

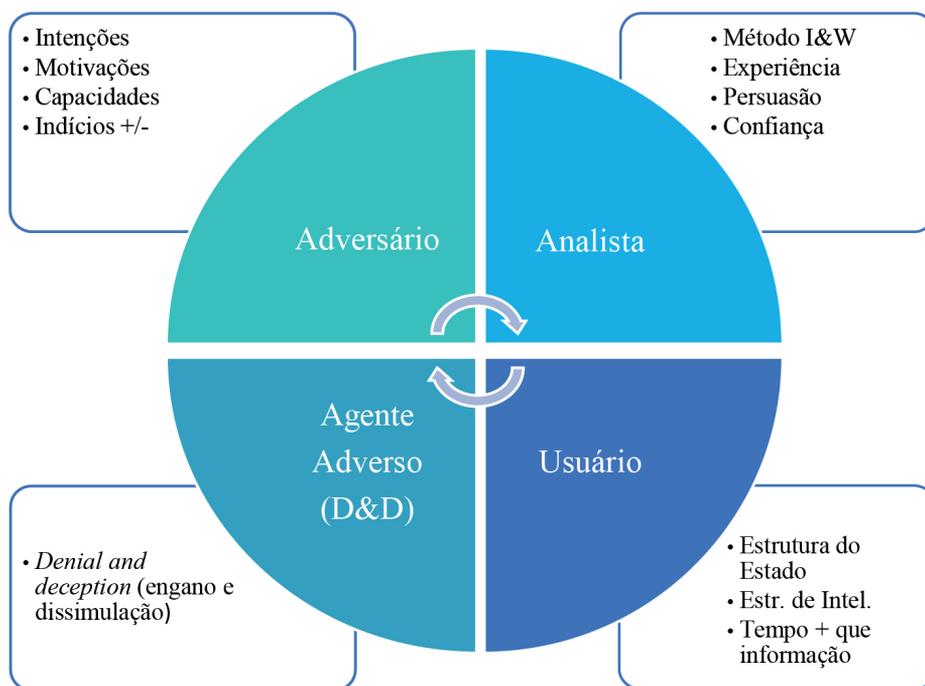
Davis (2003) defende uma ampla atuação dos usuários no processo do alerta: alocação de recursos; definição de temas e parâmetros analíticos; indicação de técnicas indiciárias; e seleção e monitoramento de indicadores de mudanças na probabilidade, no impacto, no *timing* e na descrição das ameaças. Para “a desconexão entre produtores e consumidores de alertas estratégicos ser superada”, esses deveriam ser “responsabilidade” de todo o governo, e

não apenas da Inteligência (DAVIS, 2003, p. 13-15).

Por sua vez, Wirtz (2013), autor de inúmeros livros sobre Inteligência e controle de armamentos, também salienta a mesma importância da integração entre os atores quando menciona um dos desafios da metodologia indiciária: ser implementada ao longo de todo o ciclo de Inteligência – coleta, análise e resposta – para ser efetiva.

Nesse sentido, propõe-se aqui a seguinte configuração para o Ciclo de Produção e Difusão da Inteligência de Indiciária, com foco nos atores: analista e usuário, de um lado, e adversário e agente adverso, de outro (Figura 1):

**Figura 1 – Ciclo de Inteligência de alerta (foco nos atores)**



Fonte: elaborado pela autora.

A tarefa do analista de IA, com base no método indiciário, é desvendar as intenções, motivações e capacidades do adversário. Os indícios levantados durante o trabalho analítico podem ser positivos ou negativos, no sentido de confirmar ou não as inferências realizadas. Segundo Grabo (2015), ao buscar-se desvendar o inimigo, deve-se fazer o cruzamento entre indícios positivos e negativos, ou seja, analisar o que ele fez e o que nunca fez. Em linha com a autora, algumas perguntas podem ser feitas para se chegar à mente (intenções e motivações) do adversário: ele está comprometido com os objetivos declarados?; sua meta pode ser atingida ou o problema solucionado pela via negociadora?; todas as outras opções foram eliminadas, antes de uma suposta ameaça militar ou retaliação?; o fator de risco é baixo ou pelo menos tolerável?

Por sua vez, o produto da Inteligência Indiciária tem de ser persuasivo o suficiente para chamar a atenção do usuário, ganhar sua confiança e mobilizá-lo para a ação (Figura 1). O desafio é justamente chegar ao cliente, para quem o tempo pode ser mais importante que o próprio acesso à informação. Nesse sentido, para Wirtz (2013), os decisores não devem ser prevenidos sobre um único evento, mas assessorados em toda uma análise de risco sobre a ameaça crescente (*“risk assessment”*), de modo que o aparato do Estado possa agir, ou seja, “desviar, deter ou atrapalhar” a ameaça (DAVIS, 2003, p. 12).

Esse contato direto da Inteligência Indiciária com o cliente dependerá de como essa corrente analítica está inserida nas organizações de Inteligência e na própria estrutura do Estado (Figura 1). Muitas vezes, uma das limitações do analista é “desconhecer o que outras áreas do governo estão pensando ou fazendo a respeito do problema de alerta”, caso esse já tenha sido identificado (GENTRY & GORDON, 2019, p. 157).

As duas obras angulares aqui utilizadas abordam o papel que o adversário (às vezes, aliado) exerce na negação da informação, na dissimulação, na desinformação, ou nos “sinais da mentira” (D&D – Figura 1), com o intuito de criar o elemento surpresa. Grabo (2015) destaca a importância da contrainteligência e de outras estratégias de negação à informação pelos países inimigos, como o controle da mídia. Acerca da coleta de dados sobre espionagem, afirma: “sua relevância deriva do fato de que os serviços de segurança e suas ações funcionam como um espelho que reflete os objetivos e interesses do líder do país inimigo sobre importantes assuntos internacionais” (GRABO, 2015, p. 223).

Finalmente, Gentry & Gordon (2019) lamentaram que, ao menos no momento em que escreviam, IA e contrainteligência (*“counter-deception”*) permaneciam em estruturas organizacionais separadas nos EUA. “(...) Porque alerta, e engano e dissimulação estão intimamente

relacionados, é importante os profissionais indiciários conhecerem técnicas de D&D e métodos de contrainteligência” (GENTRY & GORDON, 2019, p. 4). Também atribuíram às redes sociais papel fundamental de desinformação nos dias atuais.

## O método indiciário

Já se observou que a metodologia indiciária (*“Indications and Warning”* – I&W) foi tecida durante a Guerra Fria, para buscar-se antecipar um ataque militar surpresa por parte da URSS e dos seus aliados. Ou seja, a metodologia nasceu durante a guerra, sobretudo para períodos de guerra, baseada no antagonismo entre países aliados e inimigos. No entanto, a continuidade do uso das técnicas de I&W e a análise atual sobre o tema demonstram que esses mesmos princípios metodológicos podem ser aplicados a conflitos assimétricos ou a temáticas não-militares, por vezes com adaptações, mas não sem polêmica.

Com o fim da Guerra Fria, muitos fizeram e ainda fazem objeção à capacidade de antecipação da metodologia indiciária, em particular, em relação a dois aspectos. Por um lado, pelo fato de os desafios contemporâneos, como os impostos por atores não estatais, gerarem indícios fracos ou pouco significativos para serem submetidos às técnicas tradicionais de I&W. Células terroristas, por exemplo, emitem sinais tíbios ou muito dissimulados

de antecipação da ameaça comparados, por exemplo, a unidades militares inteiras; porém, ainda assim, emitimos, e a comunidade de Inteligência pode identificá-los. Por outro lado, ameaças vindas de atores não estatais são “distintas, imprevisíveis, diabólicas e inovadoras” (WIRTZ, 2013, p. 555-556 e 561) em relação àquelas provenientes de autores estatais; portanto, identificar com antecedência locais, métodos e alvos de ataques seria mais difícil. Gentry & Gordon (2019) seguem essa mesma linha de incredulidade acerca da eficácia da tradicional metodologia da Inteligência de Alerta para temas de segurança doméstica (*“homeland security”*), como CT.

Defende-se aqui, porém, inclusive para o caso de ameaças terroristas, que a metodologia é aplicável, porque o “quesito imaginação” não falta a analistas de Inteligência para antecipar ameaças prováveis (WIRTZ, 2013, p. 556). Kimmelman (2017) explora, adapta e atualiza sua funcionalidade para temas de segurança doméstica, o que demonstra que as técnicas de I&W podem ser mais um instrumento de natureza preventiva em CT, em complemento ao estudo de Ribeiro (2019).

Por sua vez, Grabo (2015) insiste no caráter didático de “análises *post-mortem*” (GRABO, 2015, p. 6-8, 70 e 84), para se aprender com fatos que representaram grandes fracassos de alerta (o mesmo o

faria Davis mais tarde – 2002 A). O ataque da Coreia do Norte à Coreia do Sul, e a intervenção chinesa na Coreia, em 1950, a revolta da Hungria e a crise do canal de Suez, em 1956, a crise dos mísseis de Cuba, em 1962, e a invasão da Tchecoslováquia pela URSS, em 1968, envolveram tropas estadunidenses e foram marcadas por preparações e movimentações militares, ainda que secretas, algumas ações de D&D, grande variedade de indícios políticos e, com exceção ao caso cubano, chegaram a ser conflitos militares de fato. Portanto, arquivos de alertas de longa duração – fracassados ou não –, ao contrário daqueles de IC, que logo se tornam desatualizados, melhoram com o tempo. Manter arquivos com essas crises é uma das coisas mais úteis que uma unidade de Inteligência de Alerta pode fazer (GRABO, 2015).

Assim como os estadunidenses, os britânicos analisam seus fracassos e sucessos na detecção de crises e ameaças. Ao contrário dos profissionais estadunidenses, os britânicos anteciparam as crises do canal de Suez e dos mísseis em Cuba. No entanto, também falharam ao não prever a Guerra da Coreia, a invasão da Tchecoslováquia, a Guerra do Yom Kippur (1973) e a invasão das Malvinas (1982). Por sua vez, o sistema de Inteligência japonês foi totalmente reestruturado e fortalecido pelo então primeiro-ministro Shinzo Abe, depois da falha da antecipação do lançamento de mísseis norte-coreanos sobre o Japão, em 2008 (GENTRY & GORDON, 2019).

E quando a Inteligência Indiciária antecipa uma crise, e o decisor a evita ou a debela, inclusive pela dissuasão do inimigo? Não é difícil imaginar que não há tantos registros sobre o que é denominado “paradoxo do alerta” ou “dilema do alerta”. Afinal, a complexidade da IA vem também da dificuldade da caracterização ou até da identificação do que seria seu sucesso, pois sempre pode alegar-se que o inimigo não teria agido de nenhuma forma (atacado ou ameaçado), independentemente do alerta. Será que os soviéticos não invadiram a Polônia em 1980, como fizeram com a Hungria e a Tchecoslováquia, porque a CIA alertou os presidentes Jimmy Carter e Ronald Reagan, e esses, por sua vez, ameaçaram a URSS com sanções, ou Leonid Brezhnev estava blefando desde o início? A análise histórica dos desempenhos da IA não apresenta, portanto, um simples resultado dicotômico entre acertos e erros (GENTRY & GORDON, 2019).

Em contrapartida, ao citarem Mark Lowenthal, eminente autor sobre Inteligência e segurança nacional, os autores estadunidenses destacam dois sucessos inequívocos da IA, pela pronta e assertiva resposta dos usuários: os assessoramentos que levaram o Presidente George H. Bush a enviar um representante de segurança nacional para evitar a guerra entre Índia e Paquistão, em 1990; e o Presidente George W. Bush, em 2003, a negociar com o líder líbio Muammar el-Qaddafi para que esse pusesse fim a seu programa de armas de

destruição em massa (LOWENTHAL *apud* GENTRY & GORDON, 2019).

## A metodologia I&W: fundamentos conceituais e diferenciais

A metodologia de *Indications and Warning*

(I&W) ou, como foi traduzida aqui, metodologia indiciária ou de alerta, parte do conceito central de indício. Para Grabo (2015), essa definição é acompanhada de outras igualmente fundamentais, sintetizadas e explicadas neste estudo a partir da ilustração (Figura 2):

Figura 2 - Níveis de apreensão da realidade pelo analista de IA



Fonte: elaborado pela autora.

O real, representado pela clássica imagem do iceberg, percebido inicialmente apenas em sua pequena porção superficial, permite caracterizar o indício, do verbo indicar, que significa indicação, sinal, sugestão, grau de inferência (GRABO, 2015). Como traduzido aqui, o indício passa justamente a ideia de que se trata de um nível inferior à certeza e, portanto, à evidência, como está representada na Figura 2.

Já indicador é diferente de indício e tem um sentido aproximado do que se utiliza

em vários ramos do conhecimento, inclusive na Inteligência. Seleciona-se um indicador para monitorar a expectativa de que certa ameaça tem potencial de ocorrer. Grabo (2015) defende a distinção criteriosa entre os dois conceitos: “Um indicador é um passo conhecido ou hipotético que o inimigo pode ou deve tomar em preparação para as hostilidades” (GRABO, 2015, p.10 e 59). Em seguida, indicadores devem ser compilados em listas, que funcionarão como um conjunto de expectativas. Além de “monitoráveis”, os indicadores devem

ser “preditivos, descritíveis, inequívocos e coletáveis” (GENTRY & GORDON, 2019, p. 133).

Grabo (2015) enfatizou, ainda, que, para se chegar a uma interpretação de Inteligência de Alerta, o analista terá utilizado quase sempre inferências. Por isso, a metodologia indiciária é indutiva: o profissional de IA chegará a suas conclusões a partir de fatos, ou melhor, com base no que ele pensa sobre os fatos: as conclusões resultantes de juízos e raciocínios<sup>2</sup> não serão alcançadas diretamente dos fatos, pois todo “processo é altamente subjetivo.” Como o analista tem acesso apenas a indícios (“fragmentos ou migalhas” da realidade), ele pode ter de chegar a conclusões mais abrangentes (inferências) sobre as pretensões do inimigo. Para ela, “a subjetividade será ainda mais necessária no exame de questões de natureza política e de propaganda, do que em assuntos militares” (GRABO, 2015, p. 91 e 93).

Gentry & Gordon (2019) afirmam que a metodologia indiciária, entendida como “técnica ou viés de análise”, evoluiu ao longo do tempo e assumiu “armadilhas de doutrina de Inteligência” (GENTRY e GORDON, 2019, p. 130-131), que podem ser entendidas como aquelas enfrentadas pelo analista de IA ao buscar desvendar a realidade.

Ainda assim, em Grabo já é possível identificar a formalidade do método e a busca por sua sistematização, representadas por etapas que o profissional de IA deve seguir no que é proposto aqui como Ciclo de Produção e Difusão da Inteligência Alerta (Figura 3): (1) reunião de dados e informações → (2) isolamento dos indícios mais relevantes e identificação de quais podem ser as intenções do adversário (aqui também poderia entrar o início da seleção de indicadores) → (3) avaliação da validade, do significado e da significância dos indícios, e análise de como podem estar relacionados com os fatos mais relevantes para caracterizar a ameaça → (4) interpretação de evidências que podem indicar as intenções do adversário → (5) preparação de *briefing* oral ou escrito para o decisor. Em resumo, o método permite a formação de juízos e raciocínios sobre indícios e evidências, para se chegar a juízos e raciocínios sobre os possíveis cursos de ação dos adversários e agentes adversos.

2 O termo utilizado por Grabo (2015) é “*judgement*”. Como, às vezes, ela separa *analyses* e *judgements*, aqui se optou por traduzir “*judgement*” como juízo e raciocínio, em referência à diferenciação feita pela Doutrina Nacional de Inteligência, na descrição das formas racionais e dos tipos de conhecimento (GRABO, 2015, p. 53 e 58).

Figura 3 – Ciclo de Inteligência de Alerta (foco no método)



Nota: Nenhum dos autores utiliza o conceito de Ciclo de IA. A proposta é da autora (vide p. 5 a 7).

Fonte: Esquema elaborado pela autora com base em Grabo (2015, p. 77) e Gentry & Gordon (2019, p. 130-133).

Antes, para uso exclusivamente militar, o analista aplicava o método da seguinte maneira: identificava uma “situação ruim” que já tinha evoluído ou poderia evoluir para hostilidades contra o país ou contra os interesses nacionais e monitorava a ameaça com indicadores. Hoje, uma “situação ruim” é denominada pelo Departamento de Defesa dos EUA ou pela Organização do Tratado do Atlântico Norte (Otan) como “*end-state*”. São definidos, a partir da probabilidade de ataque do País A sobre o País B, uma série de cenários mais plausíveis sobre como a hostilidade pode se materializar (Figura 3). Em geral, são construídos de três a cinco cenários, entre os mais e menos prováveis. Gentry & Gordon (2019, p. 131-132) não recomendam que se utilize o “*worst case*

*scenario*” (pior cenário), pois acreditam que ele antecipa possibilidades antes do efetivo trabalho de análise estar completo.

Para cada cenário, os analistas indicam um caminho que pode levar ao “*end-state*”. Na medida do possível, os diferentes cenários devem ter um conjunto distinto de indicadores, entre militares, políticos, econômicos, sociais, tecnológicos etc. A etapa da reunião (Figura 3-1) deve ser constante para possibilitar a atualização oportuna dos cenários. “Quando os eventos [evidências] associados a um indicador mudam, o analista tem o indício de um possível movimento em direção (ou contrário) ao ‘*end-state*’” (GENTRY & GORDON, 2019, p. 133. Os grifos são dos autores) – Figura 3-2 e 3-4.

Por sua vez, interpretou-se neste estudo que os indícios, por sua natureza menos concreta, devem ser interpretados em toda sua expressão: na essência, como substantivo (significado) e, na qualidade, como adjetivo ou elementos descritores (significância). Assim estariam completam a validação e a qualificação do indício – Figura 3-3.

Gentry & Gordon (2019) defendem que há uma habilidade essencial ao profissional que aplica o método indiciário e que tem relação direta com a análise da trajetória (inflexões na linha do tempo): perceber mudanças e integrar novas informações, mesmo não-confirmadas, à interpretação em andamento. Por isso, explicam, consoante com Grabo (2015), que especialistas temáticos não seriam os melhores para identificar mudanças, porque ficam apegados a seus pontos de vista. Assim, não seria o analista de Bolívia, ao menos não sozinho, o mais indicado a ter observado a necessidade de alerta.

O exame do passado é essencial para a projeção do futuro. A analogia com os esportes olímpicos de arremesso de pesos ou dardos mostra que, quanto maior o posicionamento da mão para trás, maior o impulso para se atingir longas distâncias, mas só até certo limite. O desafio do analista, portanto, é compreender o quanto é preciso voltar ao passado para interpretar um indício no presente que se mostra com potencial de ameaça no futuro. Sem dúvida

essa é uma forma de se reduzir as incertezas (Figura 2).

Boa parte da bibliografia caracteriza a metodologia indiciária como a detecção de anomalias dentro de padrões de normalidade: “uma cronologia é uma detectora de anomalias – e enquanto nem todas as anomalias levam a crises, todas as crises são feitas de anomalias” (GRABO, 2015, p. 69). Wirtz explica: “... a detecção de anomalias requer um estudo sustentado, de forma que os padrões de atividade que refletem a normalidade possam ser identificados” (WIRTZ, 2013, p. 558-559). Já Gentry & Gordon (2019) avaliam que a anomalia pode vir a ser um indício no futuro (Figura 3-3 e 3-4) e valorizam, igualmente, a construção de cronologias.

## **Tempos da Inteligência e vertentes de análise**

James Williams, antigo diretor da AID, no prefácio da obra de Grabo (2002), destacou que a Inteligência de Alerta difere da Inteligência Corrente e da Inteligência Prospectiva, porque “...aceita a presunção da surpresa e da Inteligência incompleta, e requer pesquisa exhaustiva...”. Afirmou que o desafio da Inteligência de Alerta é sua incompletude: relação não evidente entre eventos, sinais iniciais baseados em evidências fragmentadas ou relatórios contraditórios. Nessa diferenciação, Williams reforça a intangibilidade da IA, que não “é uma compilação de fatos. É uma

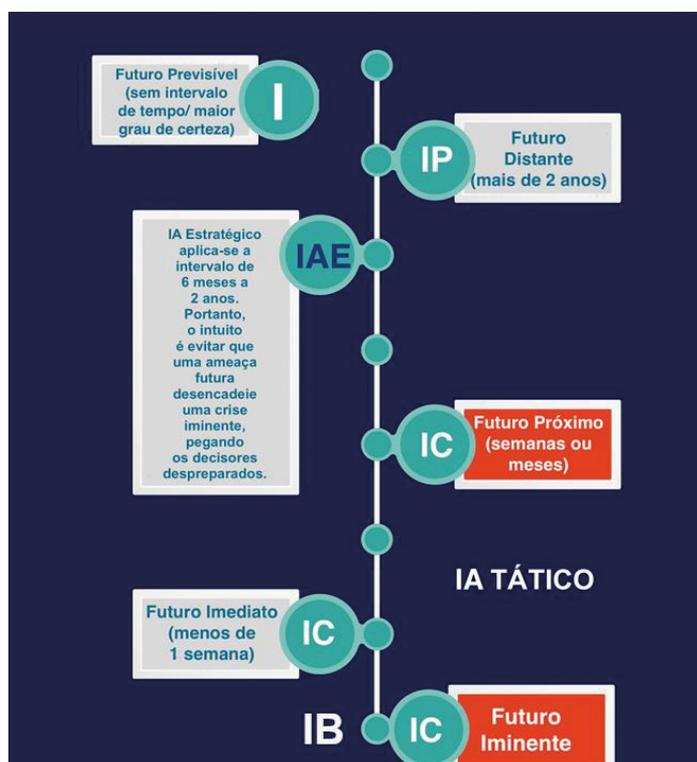
abstração, o intangível, uma percepção ou uma crença”. Uma intuição.

“advogado do diabo” (GRABO, 2015, p. 82).

São a intensidade e a complexidade que diferenciam a IA (GRABO, 2015). Ademais, o analista indiciário está atento à possibilidade – por mais remota que seja – de o adversário iniciar preparativos para uma ação hostil. Assim, o profissional de IA estará à frente dos demais do sistema de Inteligência, funcionando como o

A partir da autora estadunidense, pôde-se propor recortes temporais específicos para cada uma das tipologias da Inteligência (Figura 4), em complemento à análise de Faria (2017) sobre estudos de futuro e seu papel na melhoria da qualidade do assessoramento.

**Figura 4 – tempos da Inteligência**



Nota 1: As siglas representam:

- IB (Inteligência de Base);
- IC (Inteligência Corrente – nas três referências);
- IAT (Inteligência de Alerta Tático);
- IAE (Inteligência de Alerta Estratégico);
- IP (Inteligência Prospectiva) e
- I (Inteligência).

Nota 2: A diferenciação entre os tempos é de Grabo, mas a correlação com as vertentes da Inteligência é da autora.

Nota 3: A identificação e a delimitação temporal da IAE são de Gentry & Gordon.

Nota 4: A identificação e a caracterização de Futuro Distante para a Inteligência Prospectiva (IP) é da autora.

Fonte: Elaborado pela autora, com base em Grabo (2015) e Gentry & Gordon (2019).

Os ramos da Inteligência distribuem-se ao longo da trajetória que vai do mais próximo do presente ao futuro distante. A Inteligência Corrente foca no que está prestes a ocorrer, até cerca de uma semana adiante, ou mesmo poucas semanas. A principal característica da IC revela ainda a necessidade de consideração do passado recente. Hulnick (2008), também analista da CIA, ao tratar de todas as vertentes da Inteligência no assessoramento, comparou a IC à atividade jornalística: “...envolve reportes diários sobre o que aconteceu ontem, sobre o que está ocorrendo hoje, e sobre o que sucederá amanhã” (HULNICK, 2008, p. 224-225). Conclui que, apesar de ser demandada pelos clientes ao iniciar o dia, contraditoriamente, a IC é objeto de crítica por sua natureza menos analítica e mais descritiva ou narrativa. Já a Inteligência de Base, consolidação de temas basilares, (“uma compilação enciclopédica” – HULNICK, 2008, p. 225), trata de assuntos encerrados ou com desdobramentos de curto prazo.

A Inteligência de Alerta, por sua vez, aparece relacionada a praticamente todos os espectros de tempo da Figura 4. A partir do futuro iminente até o futuro próximo (de semanas ou meses), podem ser emitidos alertas táticos, e o futuro próximo também pode ser objeto de alertas estratégicos. Grabo (2015) define, ainda, o futuro previsível, não a partir de um limite cronológico, mas do grau de certeza do analista (por essa razão, aparece solto na

linha do tempo).

Depois de apresentar propostas de vários autores para intervalos temporais de IA, Gentry & Gordon (2019) sugerem que o alerta estratégico se aplique a um período de seis meses a dois anos. A proposta permanece focada na antecipação de crises iminentes, como inúmeras vezes destacou Grabo (2015), no sentido de que cabe ao analista indiciário apresentar os fundamentos para se evitar ou minimizar uma crise que se apresenta, no momento ou em algum ponto futuro, como inevitável. Como a autora diferencia os alertas táticos e estratégicos também pelo tempo, pois esses últimos seriam de longo prazo, entende-se que sua insistência em se referir a alertas de crises iminentes (“*impending crisis*” – GRABO, 2015, p. 25, 53, 68 e 85) seja mais para dar um sentido de urgência e inevitabilidade, do que de proximidade temporal com o presente. Certamente, a iminência também pode se aplicar ao intervalo de poucas semanas ou meses. De todo modo, segundo ela, se a IA não escolher suas crises, não se diferencia da IC.

Davis (2003, p. 3) enfatiza os “perigos iminentes e potenciais”; Gentry & Gordon (2019, p. 12, 18, 94, 133 e 136) também mencionam “eventos e crises iminentes”, mas parecem preferir “problemas de alerta emergentes”. Outras técnicas complementam a I&A e deixam o profissional de Inteligência atento e imaginativo para identificar o mais

longe, em distância e tempo, “tendências emergentes de relevância” (GENTRY & GORDON, 2019, p. 149). Segundo os autores, porém, o ambiente de muita incerteza torna esse recorte analítico o mais desafiador de todos.

Por fim, a Inteligência Prospectiva é considerada por Hulnick (2008, p. 227) a categoria mais “...controversa e que envolve juízos e raciocínios simultâneos sobre o futuro e sobre a análise de Inteligência gerada para apoiar a Política”. Aqui, reconhece-se que é sobretudo a metodologia a distinguir a IA da Inteligência Prospectiva, mas a proposta também é, para efeitos didáticos e metodológicos próprios, delimitar a IP para um período superior a dois anos (Figura 4), evitar sobreposições temporais indesejáveis

e facilitar delimitações procedimentais.

## Como é o bom analista de IA?

As duas obras principais utilizadas nesse estudo têm capítulos específicos e várias outras seções dedicadas a analisar as características cognitivas, intelectuais e de temperamento e caráter que fazem um bom profissional do método indiciário. Gentry & Gordon (2019) admitem que o que Grabo (2015) descrevera décadas atrás permanece válido até hoje.

Nesse estudo, foram selecionados (Figura 5) os atributos comportamentais e intelectuais considerados mais relevantes para a aplicação eficiente da metodologia de I&A:

Figura 5 – Bons analistas indiciários demonstram...



Legenda: T – diz respeito aos atributos de temperamento e comportamento. I – refere-se às características intelectuais e cognitivas desejáveis.

Fonte: esquema elaborado pela autora, com base em Grabo (2015) e em Gentry & Gordon (2019).

Gentry & Gordon (2019) resumem o diferencial do analista indiciário pela necessidade de apresentarem um “pensamento excepcional” (GENTRY & GORDON, 2019, p. 148 e 218). Acompanham Davis (2003) quando este afirma que o ofício do profissional de alerta é conseguir desenvolver uma “análise alternativa”, ao avaliar ameaças que, para a maioria, são improváveis ou indeterminadas (DAVIS, 2003, p. 9; e DAVIS, 2007, p. 181-182).

Outro aspecto fundamental para todos é a preferência por analistas mais antigos na carreira, mais experientes e com alguma especialização antes de se dedicarem à Inteligência de Alerta.

Os demais traços de caráter levantados por Grabo (2015), Gentry & Gordon (2019) foram considerados neste estudo igualmente necessários para todos os profissionais de Inteligência: ser confiável e perspicaz; demonstrar interesse e motivação; ter senso de responsabilidade, disposição para o trabalho duro e iniciativa.

Sobre características e habilidades intelectuais, os três autores apontaram, igualmente, a necessidade de objetividade, sofisticação analítica, capacidade para reconhecer o que é importante, competência criativa, perspectiva intelectual heterodoxa e questionadora, e capacidade de fazer apresentações lógicas e convincentes.

## **A Inteligência Indiciária e seu papel no assessoramento**

Alertar é mais que informar. Esta distinção, nada simples, talvez seja o grande diferencial da IA nas organizações. O produto resultante da metodologia I&W implica ação para o ciclo da IA fechar-se (Figuras 1 e 3.5). A depender da circunstância e da natureza da ameaça ou da oportunidade, espera-se do decisor iniciativa, e não apenas reação à ação adversária. Mesmo que o usuário resolva não agir, tal decisão precisa ser consciente, o que difere da inação ou do desconhecimento da iminência das hostilidades.

Volta-se, assim, diversamente, ao imperativo do tempo: o sentido de oportunidade da IA é, de fato, peculiar. Não basta informar antes de o evento ocorrer; é preciso alertar para permitir a decisão. Essa análise oportuna é denominada “*action*” ou “*implementation analysis*” (GENTRY & GORDON, 2019, p. 212; e DAVIS, 2003, p. 12), cuja complexidade decorre do fato de que o tempo da Política não é o tempo da Inteligência.

## **A complexa relação entre Inteligência de Alerta e instância decisória**

Com a perspectiva do cliente, completa-se o outro problema que o analista indiciário encara: “Os profissionais enfrentam dois desafios especiais no que diz respeito ao

alerta estratégico: superar seu próprio *mindset* e o dos usuários” (DAVIS, 2002 A, p. 3).

As falhas da Inteligência de Alerta podem resultar de limitações do método e das capacidades dos analistas, mas também das experiências, habilidades, preferências e dos interesses dos clientes. Quando Hulnick (2005) centrou seu estudo em IA e CT, e analisou fracassos e sucessos dessa corrente analítica nos EUA, abordou, na realidade, as falhas de percepção da relevância do alerta pelo usuário. Mais tarde, concluiu: no que diz respeito a alertas, as conexões entre Inteligência e Política têm um aspecto distintivo que vai além de saber do que os decisores precisam; é necessário garantir que eles estejam entendendo o que estão vendo, ou seja, que uma crise se avizinha (HULNICK, 2008).

A bibliografia é farta ao explorar formas de superação dos entraves postos pelos usuários: conhecer suas idiosincrasias; conquistar sua confiança e criar formas de persuadi-los (Figura 1); mostrar a relevância e a qualidade da Inteligência frente a outros produtos de assessoramento, em especial aqueles da instância política; ajudá-lo a superar o viés da falta de objetividade. Segundo Davis (2002 A e 2003), o próprio cliente pode sentir-se confiante em contribuir para a seleção dos problemas de alerta, juntamente com os órgãos de Inteligência. Assim, facilita-se a abertura de canais diretos de comunicação,

e os alertas estratégicos tornam-se assunto governamental mais do que responsabilidade exclusiva da Inteligência, o que tanto Davis (2003) quanto Gentry & Gordon (2019) identificaram no modelo inglês do *Joint Intelligence Committee* (JIC – Tabela 1).

O desafio, no entanto, é que essa aproximação não leve à “politização da Inteligência” (DAVIS, 2002 B e 2003, p. 15; GENTRY & GORDON, 2019, p. 204). Os três autores admitem que essa preocupação é herança de Sherman Kent, mas defendem ser necessário aos profissionais de Inteligência conhecerem o governo estadunidense e seus representantes tanto quanto conhecem governos de países inimigos ou aliados. “Quanto mais os analistas souberem sobre o processo decisório norte-americano, e quanto mais compreenderem os desafios enfrentados pelos decisores, melhor posicionada estará a Inteligência em sua atribuição de prover alertas estratégicos” (DAVIS, 2002 A, p. 9).

Em linha com Kent, na divisão de trabalho entre analistas e decisores, “o papel do oficial de Inteligência na *‘action analysis’* é identificar e analisar; já os formuladores de política têm a responsabilidade profissional de recomendar e escolher” (DAVIS, 2003, p. 12). O contato direto deve permanecer para melhor guiar os planos de contingência e evitar as atitudes do “*wait and see*” ou “*so-what?*” (WIRTZ, 2013, p. 557).

Davis (2003) destaca que a reticência

ou a demora dos usuários em levar em consideração alertas, mesmo bem fundamentados, decorre de distrações com temas politicamente mais prementes, e da lembrança de “falsos positivos” e dos altos custos pagos ao se adotar medidas contra hostilidades que não se realizaram (DAVIS, 2003, p. 4).

Por sua vez, a aplicação adequada do método não é menos relevante. Davis (2003, p. 8) conclui: “(...) É o balanço favorável entre evidência e inferência que galvaniza os clientes para a ação”. Seguir um método ajuda o cliente a ser melhor assessorado, pois ele mesmo pode: estimular posições divergentes; fazer perguntas certas; explicar a necessidade da informação; compartilhar o que não precisa ser negado ou compartimentado (GRABO, 2015); e estar aberto a novos assuntos ou temas inesperados (WIRTZ, 2013), para além de suas preferências políticas ou pessoais.

## **Arranjos institucionais para o assessoramento da Inteligência Indiciária**

Há décadas, Grabo apontara o desafio, atual, das organizações de competir com os assessorados que “...se valem de sua própria Inteligência” (GRABO, 2015, p. 27), o que recoloca a questão muito bem trabalhada por Gentry & Gordon (2019) sobre como os Estados podem integrar de forma mais eficiente a Inteligência de Alerta em seus

arranjos institucionais.

O quadro comparativo a seguir abrange variações históricas e geográficas, ou seja, sintetiza como diferentes países, ao longo do tempo, deram maior ou menor espaço à Inteligência Indiciária, experiência que nos ensina um conjunto de vantagens e desvantagens resultantes da adoção de cada um dos modelos: 1) cada especialista temático tem a tarefa adicional de aplicar a Inteligência de Alerta; 2) há uma organização especializada em IA; 3) existem estruturas híbridas entre os tipos 1 e 2; 4) os alertas são responsabilidade de todo o aparelho de Estado.

Percebe-se, além disso, pelo quadro-síntese, que alguns países concentram a Inteligência de Alerta em temas mais típicos de segurança doméstica, como contraterrorismo. Gentry & Gordon (2019) são entusiastas, por exemplo, da aplicação da metodologia indiciária que o serviço holandês faz para a emissão de alertas táticos e estratégicos voltados a CT.

Quadro 1 – Estruturas governamentais de Inteligência de Alerta

	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
 <p><b>1 – Cada analista tem a tarefa adicional de IA.</b></p>	<p>Adotado em países com múltiplas agências, como os EUA, ou em Estados menores, com serviços de Inteligência modestos.</p> <p>Há um modelo “moderado ou híbrido” (CIA), que aceita o papel separado de alerta de outras organizações.</p> <p>E existe uma versão “rígida”, em que todos os analistas devem reportar, pelos canais tradicionais, ameaças e oportunidades durante seus trabalhos de coleta, IC ou IP. A ideia é que todo profissional deve realizar “Inteligência antecipatória”, algo muito ironizado e criticado pelos autores.</p>	<p>Todos os assuntos considerados importantes pela Inteligência são monitorados.</p> <p>Todo o serviço e seus analistas estão, em princípio, disponíveis para tratar de temas de alerta.</p> <p>A relação de confiança entre serviço e usuário está estabelecida para todo tipo de assessoramento, inclusive para os problemas de alerta.</p> <p>Muitos profissionais de reconhecida capacidade acreditam nesse modelo.</p>	<p>Analistas são consumidos pela rotina e não têm tempo para IA;</p> <p>O caminho regular de revisão aumenta o tempo de difusão;</p> <p>O caminho regular, em documentos tradicionais, deixa os assuntos de alerta soltos;</p> <p>Pode faltar credibilidade ao produto;</p> <p>Temas de alerta são raros <i>vis-à-vis</i> à IC;</p> <p>Faltam os atributos necessários ao analista de IA;</p> <p>Visões tradicionais e conservadoras dos analistas temáticos preponderam sobre a IA.</p>
 <p><b>2 – Organizações especializadas em IA</b></p>	<p>Atribui a uma organização a responsabilidade pelos alertas: EUA (anos 1950 e 1960), ou Austrália (Sistema de Defesa de Alerta).</p> <p>Na Bélgica e na Holanda, os alertas dedicam-se a CT. Na União Europeia, há um Centro de Análise de Inteligência também com responsabilidades de “early warning”.</p>	<p>Uma estrutura exclusiva voltada a alertas permite dedicação, especialização, prioridade na coleta e no treinamento, com foco em usuários que, provavelmente, conhecem e aguardam esse produto específico de Inteligência.</p>	<p>Não é fácil atrair profissionais que queiram se dedicar apenas a IA;</p> <p>Analistas não podem contar com as unidades temáticas, a não ser que haja troca efetiva entre agências.</p> <p>Casos de alerta tendem a ser escassos, o que pode parecer aos demais que é uma unidade improdutiva.</p>
 <p><b>3 – Estruturas híbridas (2 e 3)</b></p>	<p>Combina o que há de melhor da versão “moderada” do 1º modelo com o 2º: unidades dedicadas a alertas que funcionam como ponto focal, de articulação e coordenação com áreas temáticas especializadas. Seguido pelo Japão atualmente.</p>	<p>Uma unidade voltada a IA e que trabalha de forma articulada com unidades temáticas ou especializadas em outras metodologias (IC, IB, IP e D&amp;D) tende a aproveitar a qualificação de cada uma e a minimizar as respectivas fragilidades.</p>	<p>Como mostra a história estadunidense (<i>National Intelligence Office for Warning – NIO/W – 1979-2011</i>), esse modelo fica muito dependente das peculiaridades da personalidade do coordenador da unidade de IA.</p>

	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
 4 – Alertas são de todo governo	Vários órgãos de governo, e não apenas a Inteligência, respondem por situações de alerta, como ocorre no Reino Unido (JIC) e em Cingapura.	Maior capacidade de coleta e várias expertises para a identificação de temas de alerta.  Reduz a distinção entre “produtores” e “clientes” da Inteligência de Alerta.	Muito dependente de relações próximas entre agências governamentais muitas vezes bem distintas. Essa integração precisa funcionar para o modelo dar certo.

Fonte: elaborada pela autora, com base em Gentry & Gordon (2019, p. 54 a 108, e 215 a 240).

Os autores revelam sua preferência pelo modelo 3, mas admitem que não há um tipo ideal de inserção da Inteligência Indiciária. O problema é que, a depender de seu baixo grau de integração ou de seu elevado isolamento em relação ao restante das instituições ou estruturas do Estado, a eficiência do alerta é negativamente afetada. As razões para essas variações nos tipos organizacionais certamente não estão relacionadas apenas a preocupações com a qualidade do trabalho, mas são também de natureza burocrática, política, pessoal (do gestor ou dirigente) e, talvez, acima de tudo, resultam dos fatores confiança e preferência: confiança, ou não, na capacidade da IA em, de fato, preparar o Estado para lidar com situações inesperadas e ameaçadoras; preferência por assuntos mais prementes, de curto prazo, ou seja, crença na maior necessidade da Inteligência Corrente.

A extinção do *National Intelligence Office for Warning* (NIO/W), em 2011, revela que os próprios EUA acabaram por mostrar certo descrédito em relação à IA,

ao apoiar, na última década, sobretudo o modelo 2 “rígido” (Tabela 1). Depois de tantas reestruturações da Inteligência estadunidense após 11 de setembro, o que se verificou foi o escrutínio constante da IA – refletido em seus reposicionamentos na estrutura governamental – e o crescimento exponencial do espaço da Inteligência Corrente, inclusive com a perda da *expertise* dos analistas de pensarem a partir de uma linha do tempo ampliada e avaliarem diversos futuros possíveis (Figura 4).

Gentry & Gordon (2019) valem-se de dois colegas sêniores da CIA para enfatizar sua crítica ácida à tirania da IC entre estadunidenses, australianos e britânicos: Douglas MacEachin (2002) refere-se à “armadilha da Inteligência Corrente” (MACEACHIN *apud* GENTRY & GORDON, 2019, p. 218), coloquialmente explicada com a metáfora da “*fábula do sapo fervente*”: o sapo e os que o cercam ignoram que a água está aquecendo lentamente, até ser tarde demais e a crise estar instaurada. Por sua vez, Carl Ford (2006) confessa: “Se eu tiver de apontar um problema específico

que explica porque estamos fazendo um trabalho tão ruim em Inteligência, é o foco obstinado em relatórios de Inteligência Corrente” (FORD, *apud* GENTRY & GORDON, 2019, p. 217). E esse foco seria decorrência justamente do imediatismo e das preferências dos usuários.

Seguindo a tradição de Grabo (2015), para Gentry & Gordon (2019), o ideal seria haver um equilíbrio entre as tipologias e uma integração das especialidades em prol da qualidade da produção e do assessoramento de Inteligência, o que fica nítido na Tabela 1, com seu entusiasmo pelo modelo 3. Para ambos, pode tranquilamente ocorrer que temas de Inteligência Corrente se convertam em problemas de alerta; no entanto, o que não pode absolutamente acontecer é a Inteligência Indiciária acabar se transformando em IC, e os analistas de IA não perceberem que o tema de alerta não é mais pertinente.

## Considerações finais

É dever de todo profissional de Inteligência alertar? Sim e não!

Não, porque, primeiro, o ofício indiciário é particular no universo da Inteligência e é caracterizado por objetivos definidos, metodologia própria, recortes temporais claros e uma aproximação bastante peculiar entre os atores envolvidos: produtor da informação, adversário, agente adverso e usuário.

Em segundo lugar, idealmente, o profissional de Inteligência deve apresentar um perfil muito específico, com experiência, comportamentos e habilidades desenvolvidas especialmente para conseguir superar as armadilhas colocadas pelo trabalho com indícios e inferências, ou seja, com uma perspectiva analítica, por definição, menos tangível que outras tipologias e cujo objeto são preferencialmente os mistérios. Por fim, a Inteligência de Alerta pode ser atribuição apenas de uma organização ou unidade especializada no serviço de Inteligência, dedicada, exclusivamente, à aplicação das técnicas de I&A.

Ao mesmo tempo, sim, pode vir a ser dever de todo profissional de Inteligência alertar, caso essa seja a decisão do órgão finalístico, ou seja, dividir a responsabilidade de identificação e acompanhamento de problemas de alerta entre todos os analistas, com ou sem articulação com uma unidade de Inteligência de Alerta específica. O diferencial continuará sendo a necessidade de capacitação dos profissionais para a aplicação do método indiciário.

O Brasil, com suas agências especializadas ou em conjunto, como Sisbin, tem maturidade para selecionar e monitorar temas de alertas táticos e estratégicos, e definir assuntos emergentes entre aqueles mais tradicionais, relativos a ameaças e oportunidades para o país. O amadurecimento do sistema brasileiro

permite que sejam testados distintos arranjos institucionais para a inserção da IA à estrutura do Estado. A integração entre os órgãos também possibilita a troca de experiências entre profissionais que apliquem metodologias típicas das diferentes vertentes da Inteligência: Inteligência Indiciária, Inteligência Corrente, Inteligência de Base e Inteligência Prospectiva, sem necessidade ou risco de predominância de um ramo,

em detrimento de outro.

Dessa forma, saem beneficiados profissionais e órgãos de Inteligência, com a preservação da autenticidade de seu ofício, e clientes, com a qualidade do assessoramento, fruto da capacidade de antecipação, da comunicação eficaz, da prontidão e de produtos oportunos e diversificados.

Figura 6 – Ciclo de Inteligência de Alerta: universo conceitual e características



Fonte: elaborado pela autora

## Referências

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

DAVIS, Jack. Strategic Warning: If Surprise is Inevitable, What Role for Analysis? *The Sherman Kent Center for Intelligence Analysis Occasional Papers: Volume 2, no. 1*, 2003. Disponível em <https://www.hsdl.org/?abstract&did=442470>. Acesso em: 11 jul. 2022.

DAVIS, Jack. Sherman Kent and the Profession of Intelligence Analysis. *The Sherman Kent Center for Intelligence Analysis Occasional Papers: Volume 1, no. 5*. Sherman Kent Center, 2002. Disponível em <https://www.hsdl.org/?view&did=442468>. Acesso em: 12 ago. 2022.

DAVIS, Jack. Improving CIA Analytic Performance: Strategic Warning. *The Sherman Kent Center for Intelligence Analysis. Occasional Papers: Volume 1, no. 1*. Sherman Kent Center, 2002. Disponível em <https://www.hsdl.org/?abstract&did=449505>. Acesso em: 11 jul. 2022.

DAVIS, Jack. Strategic Warning: Intelligence support in a world of uncertainty and surprise in *Handbook of Intelligence Studies*. Lock K. Johnson. Disponível em <https://www.routledgehandbooks.com/doi/10.4324/9780203089323.ch13>. Acesso em: 11 ago. 2022.

FARIA, Bruno. *Estudos de futuro aplicados à Atividade de Inteligência: possibilidades*. Conclusão de Curso (Aperfeiçoamento em Inteligência). ABIN/ ESINT, 2017.

GENTRY, John A. & GORDON, Joseph S. *Strategic Warning Intelligence: History, Challenges, and Prospects*. Georgetown University Press, 2019.

GRABO, Cynthia with Jan Goldman. *Handbook of Warning Intelligence*. Complete and Declassified Edition. Rowman & Littlefield, 2015.

GRABO, Cynthia. *Anticipating Surprise: Analysis for Strategic Warning*. Joint Military Intelligence College's Center for Strategic Intelligence Research. Defense Intelligence Agency, 2002.

HULNICK, Arthur S. The intelligence producer – policy consumer linkage: A theoretical approach. *Intelligence and National Security*, 1:2, 2008. Disponível em <https://pt.booksc>.

org/book/39636362/4cd38b. Acesso em: 26 ago. 2022.

HULNICK, Arthur S. Indications and Warning for Homeland Security: Seeking a New Paradigm. *International Journal of Intelligence and Counterintelligence*, 18, 2005. Disponível em <https://pt.booksc.org/book/29907550/7be597>. Acesso em: 11 jul. 2022.

KIMMELMAN, Susann. *Indications and Warning Methodology for Strategic Intelligence*. Naval Postgraduate School (U.S.). Monterey, Califórnia, 2017. Disponível em <https://www.hsdl.org/?abstract&did=808274>. Acesso em: 11 jul. 2022.

MAISONNAVE, Fabiano. Morales invade Petrobras e nacionaliza gás. *Folha de São Paulo*, 2 maio 2006. Disponível em <https://www1.folha.uol.com.br/fsp/dinheiro/f0205200602.htm>. Acesso em: 30 jul. 2002.

RIBEIRO, Alexandre Carreira. *Uso de Ferramentas de Análise de Risco na Prevenção ao Terrorismo no Brasil*. Conclusão de Curso (Aperfeiçoamento em Inteligência). ABIN/ESINT, 2019.

WIRTZ, James J. Indications and Warning in an Age of Uncertainty, *International Journal of Intelligence and CounterIntelligence*, 26, no. 3, 2013. Disponível em <https://core.ac.uk/download/pdf/36739628.pdf>. Acesso em: 27 jul. 2022.