MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

GAB CMT EX – CIE

ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO

CURSO AVANÇADO DE INTELIGÊNCIA PARA OFICIAIS

TRABALHO DE CONCLUSÃO DE CURSO (TCC)

A APLICAÇÃO DA TÉCNICA DE AVALIAÇÃO DE DADOS (TAD) DA INTELIGÊNCIA DA FONTE CIBERNÉTICA NO ÂMBITO DO SIEx

Brasília

2022

Ten Cel RAFAEL DE UZEDA ALMEIDA **PINTO**

A APLICAÇÃO DA TÉCNICA DE AVALIAÇÃO DE DADOS (TAD) DA INTELIGÊNCIA DA FONTE CIBERNÉTICA NO ÂMBITO DO SIEX

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como pré-requisito para a obtenção do Grau Pós-graduação Lato Sensu de especialização em **Análise de Inteligência.**

Orientador: CEL ALEXANDRE **ROBERTO** DA SILVA

Brasília

2022

CATALOGAÇÃO NA FONTE
BIBLIOTECA CEL FORRER GARCIA

P731a Pinto, Rafael de Uzêda Almeida

A aplicação da técnica de avaliação de dados (TAD) da inteligência da fonte cibernética no âmbito do SIEx/ Rafael de Uzêda Almeida Pinto. - Brasília, 2022.
32 fl.

Orientador: Alexandre Roberto da Silva.
Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência) - Escola de Inteligência Militar do Exército (EsIMEx), Brasília – DF, 2022.

1. Técnica de Avaliação de Dados 2. CYBINT 3. SIEx I. Título.

Ten Cel RAFAEL DE UZEDA ALMEIDA **PINTO**

A APLICAÇÃO DA TÉCNICA DE AVALIAÇÃO DE DADOS (TAD) DA INTELIGÊNCIA DA FONTE CIBERNÉTICA NO ÂMBITO DO SIEX

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como pré-requisito para a obtenção do Grau Pós-graduação Lato Sensu de especialização em **Análise de Inteligência.**

Aprovado em _____de _____de 2022.

COMISSÃO DE AVALIAÇÃO:

_____

ALEXANDRE ROBERTO DA SILVA - Cel -Presidente

Escola de Inteligência Militar do Exército

_____

MÁRCIO FERNANDES DO NASCIMENTO - Cel - Membro

Escola de Inteligência Militar do Exército

RESUMO

Nas últimas duas décadas o Sistemade Inteligência do Exército (SIEx) incorporou às suas capacidades de obtenção de dados fontes das mais variáveis origens. Esse processo trouxe uma discussão sobre o como avaliar fontes das diversas origens. As fontes tecnológicas nasceram não só da necessidade de novos meios de obtenção, mas também pela evolução tecnológica na era da informação. O fluxo de dados que antes era desempenhado pela interrelação humana, passa a ter características de interação homem-máquina nunca visto antes na atividade de inteligência. As novas tecnologias incorporadas ao SIEx permitiram atingir um novo patamar na produção de conhecimento. Dentre essas novas fontes adotadas pelo Exército Brasileiro (EB) está a fonte cibernética (*CYBINT*). Sendo uma das mais novas capacidades incorporadas ao SIEx e uma das mais técnicas, a *CYBINT* possui características que sugerem uma revisão na Técnica de Avaliação de Dados (TAD) atualmente adotada pelo EB, uma vez que ela foi concebida para fontes humanas (*HUMINT*). A TAD tradicional, de uma maneira geral, é feita separando o conteúdo da fonte e, é nessa última análise (a da fonte, onde reside o principal óbice para avaliação de fontes tecnológicas. Este trabalho visa apresentar uma solução de avaliação de dados da fonte cibernética, ao mesmo tempo que realiza uma revisão conceitual sobre o tema.

Palavras-chave: Técnica de Avaliação de Dados. *CYBINT*. SIEx.

ABSTRACT

Over the last two decades, the Army Intelligence System (SIEx) has incorporated sources from the most varied sources into its capabilities for obtaining data. This process brought about a discussion about how to evaluate sources of different origins. Technological sources were born not only from the need for new means of obtaining, but also from technological evolution in the information age. The flow of data that was previously performed by human interrelationships now has characteristics of human-machine interaction never seen before in intelligence activity. The new technologies incorporated into SIEx allowed us to reach a new level in knowledge production. Among these new sources adopted by EB is the cyber source (CYBINT). Being one of the newest capabilities incorporated into SIEx and one of the most technical, CYBINT has characteristics that suggest a review of the Data Assessment Technique (TAD) currently adopted by EB, since it was designed for human sources (HUMINT). Traditional TAD, in general, is done by separating the content from the source and it is in this last analysis (that of the source) where the main obstacle to evaluating technological sources lies. This work aims to present a source Data Evaluation solution Cybernetics, at the same time as carrying out a conceptual review on the topic.

Keywords: Data Evaluation Technique. CYBINT. SIEx.

SUMÁRIO

1 INTRODUÇÃO

A avaliação de dados para a atividade de inteligência é fundamental. Ao longo da história é possível identificar erros de avaliação de dados que resultaram em decisões equivocadas e efeitos desastrosos, como no ataque a Pearl Harbour na 2ª Guerra Mundial e, mais recentemente, nos ataques terroristas de 11 de setembro de 2001.

> A Técnica de Avaliação de Dados (TAD) é a técnica que possibilita a avaliação do dado por meio do julgamento da fonte e do julgamento de seu conteúdo. O julgamento da fonte tem a finalidade de estabelecer o grau de sua idoneidade e o julgamento do conteúdo representa o grau de veracidade do dado (Brasil, 2015b, p. 47).
> A TAD tem por finalidade estabelecer os procedimentos para a aferição da credibilidade de dados, matéria-prima para a produção do conhecimento, condição essencial para que possam ser utilizados na elaboração dos diversos tipos de conhecimento de Inteligência (Brasil, 2019, p. 32).

O processamento e a avaliação dos dados para a produção do conhecimento de inteligência durante o século XX teve seu foco voltado às fontes humanas, visto que foi e continua sendo a base do trabalho de busca dos serviços especializados em produzir conhecimentos no mundo todo.

Porém com a chegada da Era da Informação, do advento de novas tecnologias e, principalmente da criação do espaço cibernético, surge no mundo a possibilidade gigantesca de aquisição de dados, tanto em quantidade quanto em qualidade, pelos profissionais de inteligência, que antes era extremamente restrito e exigia um esforço de busca muito maior.

Em se tratando de busca de dados é imprescindível destacar a importância irrefutável das fontes de informação que, com o advento da Internet, se tornaram imensuráveis. É devido a esse grande número de fontes de informação disponíveis na Rede mundial de computadores, que se tornou importantíssimo a elaboração de critérios que avaliem tanto as fontes que originaram os dados quanto o conteúdo que nela transitam para que diminuir as incertezas dos decisores.

Desta forma, este trabalho buscou analisar de que forma pode-se realizar a avaliação dos dados obtidos por intermédio da fonte cibernética no SIEx e apresentar uma sugestão para sistematizar esse procedimento.

2 O AMBIENTE CIBERNÉTICO E A INTELIGÊNCIA CIBERNÉTICA

2.1 O AMBIENTE CIBERNÉTICO

Pode-se conceituar o espaço cibernético como aquele que é composto pela combinação de aspectos informacionais, virtuais e de estruturas físicas. Clarke (2010) é um dos autores que considera, na conceituação do espaço cibernético, aspectos tangíveis e intangíveis (Portela, 2016, p. 92).

O autor conceitua o espaço cibernético como toda a rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles. Para esse autor, a adição de aspectos físicos que estão desvinculados da internet ao conceito de espaço cibernético é justificada pelos próprios aspectos informacionais. Por exemplo, encontramos em computadores não conectados na internet informações sobre flutuações de dinheiro, transações de créditos, comércio e até sistemas de controle de geradores e outras estruturas críticas (Portela, 2016, p. 92).

> Entretanto, cabe ressaltar que, no conceito acima, Clarke (2012) não aborda a figura dos usuários, que são observados na visão de Ventre (2011) sobre o espaço cibernético. Para esse pesquisador, o espaço cibernético é resultado da soma de três camadas elementares: *hardware*, *software* e *peopleware*. Essa composição nos permite inferir a definição do espaço cibernético abordada por Daniel Ventre (2011): conjunto de equipamentos físicos (*hardware*), que sustenta uma dimensão virtual com programas, sistemas, aplicativos e informações (*software*), cuja manipulação se dá por uma camada cognitiva de usuários (*peopleware*) (Portela, 2016, p. 92).

Cabe ressaltar que o espaço cibernético não pode ser confundido com a cibernética, que estuda a organização e relações de controle de sistemas, conforme apontado por Heylighen e Joslyn (2001), ou seja, ela não é sinônimo de espaço cibernético. Outra diferenciação necessária é entre o espaço cibernético e a *internet*. Conforme Clarke (2012), a *internet* e espaço cibernético não são sinônimos, pois toda a internet faz parte do espaço cibernético, mas nem todo espaço cibernético está conectado na *internet* (Portela, 2016, p. 93).

Desta forma, o espaço cibernético não é natural, como por exemplo, os espaços terrestre e aéreo, e sim um espaço elaboradoe criado pelo homem. Em virtude disso, esse espaço é distinto dos demais no que tange a interconectividade., o espaço cibernético transpassa todos os demais (Portela, 2016, p. 93 apud Ventre, 2011).

Conforme a Doutrina Nacional da Atividade de Inteligência (Brasília, DF, 2016b, p. 90), "Ciberespaço" refere-se à medida em que as ações e comunicações ocorrem em um mundo em rede que transcende as fronteiras geográficas e políticas. Tanto a área intangível de geração e transmissão eletrônica de dados quanto à bases materiais da infraestrutura de telecomunicações e sistemas computacionais formam este espaço. "*Cyber space*" é, portanto, um conceito global que abarca tudo relacionado à *World Wide Web (Internet*), a base desse ambiente, onde a realidade virtual é desenvolvida (Brasília, DF, 2016b, p. 90).

> Esse espaço começou a se desenvolver, no final da década de 1960, com *a Advanced Research Projects Agency Network* (ARPA net), rede experimental financiada pelos militares norte-americanos para integrar computadores de médio e grande porte (*mainframes*) a universidades e centros de pesquisas. Essa foi a fase precursora da internet. A fase seguinte foi a da "internet de pessoas e comunidades", quando indivíduos e máquinas passaram a interagir com grau de diferenciação que separava o humano do artificial. A fase atual, "internet das coisas", caracteriza-se pela computação ubíqua, em que o humano e o artificial se harmonizam. A ubiquidade computacional é manifesta na interligação de objetos e dispositivos inteligentes que interagem entre si e com as pessoas (Brasil, 2016b, p. 91).
>
> A internet vem sendo expandida pela "Nova Tecnologia da Informação e Comunicação" (NICT). As NTIC, que constituem o ciberespaço, servem aos interesses nacionais como elemento estratégico de defesa, segurança e projeção de poder. Eles dizem respeito não apenas à aquisição e proteção de dados e conhecimento, mas também à implementação de decisões voltadas à gestão da burocracia que organiza a infraestrutura nacional e a sociedade (Brasil, 2016b, p. 91).
>
> Os atentados terroristas de 11 de setembro fortaleceram o uso da informação pelo Estado como meio de segurança coletiva e como garantidor. A exploração do ciberespaço levou ao uso de sistemas de monitoramento eletrônico mais sofisticados e abrangentes (Brasil, 2016b, p. 91).
>
> Muitas ameaças tradicionais, como espionagem, terrorismo, atividade extremista, guerra e atividade criminosa, encontram resposta no ciberespaço. Nas últimas duas décadas, a perda de crimes cibernéticos e os desafios de segurança cibernética têm sido objeto de muito debate. Além dos danos causados pelos crimes comuns, destacam-se os que afetam a zona econômica e a segurança nacional (Brasil, 2016b, pág. 92).
>
> Do ponto de vista ciberativista, as ações de grupos visando ataques a sites e bases de dados governamentais, como as do setor de energia no Brasil em 2014, tornaram-se notórias. Houve ataques dessa magnitude na última década. Tem como alvo sistemas de comunicação estatais e privados, como a Estônia em 2007 e a Geórgia em 2008. Outro exemplo de ataque cibernético foi promovido pelo vírus de computador *Stuxnet* contra a instalação nuclear do Irã em 2010. E em 2013, um vazamento foi feito por um funcionário terceirizado da Agência de Segurança Nacional do governo dos EUA e da vigilância global da internet promovida pela Agência de Segurança Nacional do governo dos EUA, conhecida como *Prism*, que monitora governos e empresas. Programa secreto revelado (Brasil, 2016b, pág. 92).

> Os procedimentos tradicionais de inteligência realizados na realidade física se estendem à realidade virtual. A segurança cibernética baseia-se não apenas na prevenção e mitigação de ameaças, mas também na previsão da intenção e do potencial de um invasor. Os ataques cibernéticos significam atividades que vão além da própria rede, pois geralmente fazem parte de uma questão competitiva de natureza política e econômica. Portanto, há um aspecto humano que não pode ser ignorado diante dos dados técnicos. Ao investigar cada situação, é necessário comparar a técnica e a operação (Brasil, 2016b, pág. 93).

> A importância do ciberespaço no trabalho de inteligência reside no fato de que o ciberespaço é tanto um repositório quanto um canal de conhecimento e dados, objeto de análise e ambiente operacional. O ciberespaço atua como um campo onde as informações estratégicas são armazenadas, manipuladas e transmitidas. Além disso, como existem vários atores com motivações diferentes, eles próprios são monitorados e escrutinados para fins de abuso e controle (Brasil, 2016b, p. 94).

Conclui-se parcialmente que o ciberespaço, após sua criação pelo homem, vem sendo explorado de maneira crescente pelos serviços de inteligência do mundo todo como oportunidades de aquisição de dados e exploração de deficiências dos sistemas adversários.

2.2 INTELIGÊNCIA CIBERNÉTICA

A inteligência cibernética (CYBINT) é a inteligência criada a partir de dados provenientes do ciberespaço, protegidos ou não. Isso é chamado de espaço virtual que consiste em dispositivos de computação em rede onde as informações digitais são transmitidas, processadas ou armazenadas (Brasil, 2015b, p. 22).

Este assunto, porém, não pode ser tratado em separado e sem passarmos, preliminarmente, pelo tema da guerra cibernética.

> Em definição simplória, a guerra cibernética se define por uma ação ou conjunto associado de ações com uso de computadores ou rede de computadores para levar a cabo uma guerra no ciberespaço, ou retirando de operação serviços de *internet* e/ou de uso normal da população (energia, água etc.) ou propagando códigos maliciosos pela rede (vírus, *trojans, worms* etc.) (Wendt, 2011, p. 21).

O conceito acima para ser bem compreendido tem de ser, necessariamente, analisado de forma particionada. Então, vejamos:

• Uma ação ou conjunto associado de ações: nos diz que um ataque cibernético pode ser protagonizado por umapessoa, por um grupo de indivíduos, por uma organização ou por um Estado, utilizando apenas uma máquina ou então um conjunto de máquinas, de forma presencial ou não, mas que têm uma finalidade determinada, que pode ser por necessidade de status, pelo desafio próprio ou da coletividade, político-ideológico, financeiro e/ou religioso;

• Uso de computadores ou rede de computadores: significa que os ataques cibernéticos podem ser planejados e executados de um sítio determinado ou por intermédio de uma rede de máquinas, como acontece no caso dos conhecidos "*botnets*", quando uma grande quantidade de computadores pode ser acionadaà distância por criminosos;

• Guerra no ciberespaço: uma definição trazida por Duarte (1999) refere que o ciberespaço é "a trama informacional construída pelo entrelaçamento de meios de telecomunicação e informática, tanto digitais quanto analógicos, em escala global ou regional". Este conceito abrange, portanto, todos os meios onde pode ocorrer a guerra cibernética, qual seja: onde ocorrem as CMCs – comunicações mediadas por computador;

• Retirando de operação serviços de internet: significa que a ação desenvolvida pelos hackers tem por objetivo a retirada de um determinado site e/ou serviço dos provedores de internet;

• Serviços de uso normal da população (energia, água etc.) do Estado: revela que uma ação hacker pode atingir as chamadas infraestruturas críticas de uma região e/ou país e redundar em resultados catastróficos e imensuráveis quando provocar um colapso na rede de transmissão de energia, causando apagão e/ou retardando o retorno do serviço. É claro que esses serviços serão afetados porquanto usem o computador como forma de apoio, execução e controle. Da mesma forma, o ataque pode ocorrer aos órgãos de um país, atingindo sua soberania e segurança.

• Propagando códigos maliciosos pela rede: uma ação no ciberespaço, em grande escala e bem planejada, pode fazer com que cavalos de troia, vírus, *worms*, etc. possam ser espalhados pela rede através de páginas web, de e-mails (*phishing* scam14), de comunicadores instantâneos (*Windows Live Messenger, Pidgin, GTalk* etc.) e de redes sociais (*Orkut, Twitter, Facebook* etc.), dentre outras formas possíveis.

O tema da "guerra cibernética" é, portanto, bastante abrangente. Atinge circunstâncias antes tidas apenas no mundo real, incluindo a ameaça à soberania de um país que, a par da tecnologia e evoluções constantes dos mecanismos de tráfego de dados e voz, tenderia a evoluir e aprimorar mecanismos protetivos (Wendt, 2011, p. 23).

> Em outras palavras, uma vez ocorrendo à ameaça à soberania a tendência lógica é de criação de mecanismos de defesa e reação, caso necessários. No entanto, não é o que se observa! Da mesma forma que os setores públicos, o setor privado também sofre os efeitos dessa guerra e da espionagem industrial, cada vez mais realizada

> através dos meios tecnológicos, pois feita com menor risco e um custo operacional aceitável (Wendt, 2011, p. 23).
>
> Tido como necessário um ou vários mecanismos de defesa, similares aos existentes no mundo real, não se pode vislumbrá-lo(s) sem uma prévia análise e/ou atitude pró-ativa. E é esse o propósito de uma "inteligência cibernética", capaz de propiciar conhecimentos necessários à defesa e otimização da capacidade pró-ativa de resposta(s) em caso de uma ameaça virtual iminente/em curso (Wendt, 2011, p. 23).

No entanto, as ameaças no mundo virtual tendem a ser mais rápidas e sofisticadas que as do mundo real, o que gera um tempo menor de reação por parte do alvo a ser atingido. Por isso, ações de inteligência, baseadas em mecanismos específicos de hardware e software, aliados ao conhecimento humano, podem ser fundamentais à perfeita defesa e à melhor reação, fazendo com que países, organizações públicas e privadas, posicionem-se ou não adequadamente em relação à sua segurança na rede (*cyber security*) (Wendt, 2011, p. 24).

> "Adequadamente ou não" significa dizer que nem sempre os países e/ou empresas dão a real dimensão ao problema e, por consequência, à resposta a ele. Os investimentos são extremamente baixos, o que torna as (re)ações restritas, isso para não dizer minúsculas. Importante referir que não há propriamente distinção entre alvos civis e militares numa eventual "Guerra Cibernética", o que exige um constante acompanhamento e análise dos fatores, pois que as infraestruturas críticas estão expostas às ações, tanto no mundo real quanto no virtual (Wendt, 2011, p. 25).

Com isso, a Inteligência Cibernética nada mais é do que um processo que leva em conta o ciberespaço, objetivando a obtenção, a análise e a capacidade de produção de conhecimentos baseados nas ameaças virtuais e com caráter prospectivo, suficientes para permitir formulações, decisões e ações de defesa e resposta imediatas visando à segurança virtual de uma empresa, organização e/ou Estado (Wendt, 2011, p. 25).

Os conteúdos de abrangência da inteligência cibernética são:

- Os ataques às redes, públicas ou privadas, e às páginas web.

- Análise das vulnerabilidades sobre as redes, sistemas e serviços existentes, enfocando o entrelaçamento à teia regional, nacional e/ou mundial de computadores.

- Constante análise e acompanhamento dos códigos maliciosos distribuídos na web, observando padrões, métodos e formas de disseminação.

- Enfoque na engenharia social virtual e nos efeitos danosos, principalmente nas fraudes eletrônicas.

- Mais especificamente, monitorar as distribuições de *phishingscam* e outros códigos maliciosos (*malwares*), tanto por web sites quanto por e-mail e as demais formas de

disseminação, com atenção especial para as redes sociais e os comunicadores instantâneos de mensagens.

- Observação e catalogação dos casos de espionagem digital, com abordagem dos casos relatados e verificação dos serviços da espécie oferecidos via internet.

- Intenso monitoramento a respeito de *adwares, worms, rootkits, spywares*, vírus e cavalos de Tróia, com observância do comportamento, poliformismo, finalidade e forma de difusão.

- Detectar e monitorar os dados sobre fraudes eletrônicas e o correspondente valor financeiro decorrente das ações dos criminosos virtuais.

- Monitoramento da origem externa e interna dos ataques e da distribuição dos códigos maliciosos, possibilitando a demarcação de estratégias de prevenção e/ou repressão.

- Verificação e catalogação das ações e dos mecanismos de *hardware* e *software* de detecção de ameaças e de respostas imediatas às ameaças virtuais.

- Ao final, proposição de políticas de contingência para os casos de ciberterrorismo, preparando os organismos públicos e privados em relação às ameaças existentes e, em ocorrendo a ação, procurando minimizar os efeitos decorrentes através por meio do retorno quase que imediato das infraestruturas atingidas (Wendt, 2011, p. 27).

Em suma, a guerra cibernética em seu aspecto amplo e, mais especificamente, o ciberterrorrismo, tornam-se uma preocupação constante e que está em nosso meio, o que enseja a adoção de medidas fundamentais e proativas de detecção e reação eficazes (Wendt, 2011, p. 27)

Segundo resultado de entrevistas com especialistas da área, “existem 3 tipos de atividades cibernéticas: ataque cibernético, proteção cibernética e exploração cibernética. Entre as atividades cibernéticas, a exploração cibernética é intimamente ligada à Inteligência, consistindo em "ações de busca ou coleta nos sistemas de tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas"

Seguindo com o resultado da entrevista com os especialistas, “o espaço cibernético é um ambiente complexo que vai além dos limites organizacionais e das fronteiras nacionais. Ele é resultante da interação de pessoas, softwares e serviços disponíveis na Internet, por meio

de dispositivos e redes de telecomunicações conectados a ela. Ainda segundo os especialistas, ele é definido como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas e, também, pela infraestrutura física e lógica por onde transitam e onde são armazenados os dados da fonte cibernética. Isso abrange as redes e os equipamentos de comunicações, além dos sistemas de informação sobre eles estabelecidos e os indivíduos que interagem com todas as camadas do ambiente."

Os especialistas também dizem que, "como ambiente operacional, o espaço cibernético é caracterizado pelas três perspectivas informacionais: física, lógica e cognitiva – cujos fatores a serem analisados interagem entre si, formando o seu caráter único e indivisível."

Por fim, os mesmos especialistas citam que "o espaço cibernético pode ser representado em três camadas (física, lógica e cognitiva) compostas de seis componentes (geografia, rede física, rede lógica, identidade cibernética, identidade e social)".

Já a Doutrina Nacional da Atividade de Inteligência prevê que a "inteligência cibernética" refere-se a duas funções desempenhadas nesse novo âmbito: obtenção de dados e proteção de conhecimentos e dados. Essas funções vinculam-se à produção do conhecimento nesse novo campo de valor estratégico. A importância do domínio do ciberespaço para a Atividade de Inteligência não se esgota no objetivo de garantia de segurança, mas se estende à identificação de oportunidades, isto é, à indicação de tendências e antecipação de cenários para concretizar estratégias (Brasília, DF, 2016b, p. 92).

Desta forma, pode-se concluir parcialmente que o ambiente cibernético trouxe um incremento da gama de dados trabalhados pela inteligência fruto das ferramentas desenvolvidas pela guerra cibernética, por intermédio, principalmente, da exploração cibernética, que é o carro chefe da fonte de inteligência cibernética (*CYBINT*).

3 A TÉCNICA DE AVALIAÇÃO DE DADOS

Para um profissional de inteligência é essencial que os dados utilizados para a produção do conhecimento sejam avaliados a fim de evitar que seja realizado um assessoramento equivocado ao decisor e que haja prejuízo significativo nos esforços na busca da verdade.

Os profissionais de inteligência devem explorar regularmente informações de qualidade incerta para apoiar a tomada de decisões. Se as informações são obtidas de uma fonte humana ou de um sensor automatizado, a falha em avaliar e comunicar suas características pode contribuir para a inteligência falhar. Isso é evidente no caso de c*urveball*, o informante iraquiano que forjou um extenso testemunho sobre as supostas armas de destruição em massa de Saddam Hussein. Submetidas a um escrutínio inadequado, as falsas alegações de c*urveball* sustentaram a estimativa de inteligência nacional de 2002 sobre os programas de armas de destruição em massa (ADM) do Iraque e podem ter influenciado a malfadada decisão de invadir o Iraque em 2003 (Irwin *et al*, 2020).

Reconhecendo a avaliação das informações como uma função fundamental dentro do processo de inteligência, algumas organizações fornecem padrões para avaliar e comunicar características relevantes das informações. Apesar de suas intenções, no entanto, muitas dessas normas são inconsistentes entre as organizações, e podem ser fundamentalmente falhos ou de outra forma inadequados ao contexto da aplicação. Em certas situações, padrões mal formulados podem inibir a colaboração, degradar a qualidade dos julgamentos analíticos e prejudicar a tomada de decisões (Irwin *et al*, 2020).

A fim de desenvolver recomendações baseadas em evidências para práticas futuras na avaliação e comunicação da qualidade da informação, a SAS-114 (Carteira de Intlg da Organização do Tratado do Atlântico Norte - OTAN) coletou padrões em uso em diversas agências e domínios.

Os critérios de avaliação das informações apresentados na doutrina da inteligência da OTAN são conhecidos como código do almirantado ou Sistema da OTAN. Desenvolvido pela Marinha Real britânica na década de 1940, o sistema sofreu poucas mudanças desde a sua criação, e forma a base dos padrões usados por vários membros da Aliança, bem como organizações em outros domínios. De acordo com o código do almirantado, as informações

são avaliadas em duas dimensões: confiabilidade da fonte e credibilidade da informação. Os usuários são instruídos a considerar esses componentes de forma independente e classificá-los em duas escalas separadas. A classificação resultante é expressa usando o código alfanumérico correspondente (por exemplo, *provavelmente* informações verdadeiras de uma fonte*geralmente confiável* é classificada como B2). Ambas as escalas incluem uma opção a ser usada quando há uma incapacidade de avaliar ('F' para confiabilidade de origem e '6' para credibilidade da informação). Assim, as classificações 'F' e '6' não fazem parte das escalas ordinal compostas pelas classificações A-E e 1-5, respectivamente (Irwin *et al*, 2020).

O extinto acordo de padronização da OTAN (STANAG) 2511 fornece uma versão mais detalhada do código do almirantado, e é apresentado abaixo para referência histórica (Quadro 1). De acordo com muitas das normas examinadas, a OTAN STANAG 2511 inclui uma descrição qualitativa para cada classificação de confiabilidade e credibilidade. A confiabilidade da fonte está conceitualmente ligada à "confiança" em uma determinada fonte, com base no desempenho passado, enquanto a credibilidade da informação reflete até que ponto novas informações se conformam com relatórios anteriores. Também vale a pena notar que a OTAN STANAG 2511 usa confirmada por outras fontes como sua maior classificação de credibilidade da informação, onde a doutrina aliada atual substitui completamente crível (Irwin *et al*, 2020).

Quadro 1 - NATO AJP 2.1 2016 valores de confiabilidade e credibilidade da fonte

Confiabilidade da capacidade de coleta		**Credibilidade da informação**	
A	Completamente confiável	**1**	Completamente crível
B	Normalmente confiável	**2**	Provavelmente verdadeiro.
C	Bastante confiável	**3**	Possivelmente verdadeiro
D	Normalmente não é confiável	**4**	Duvidoso
E	Não confiável	**5**	Improvável
F	A confiabilidade não pode ser julgada	**6**	Credibilidade não pode ser julgada

Fonte: Irwin *et al.* (2020).

O exame crítico dessas normas e outras coletadas pelo SAS-114 expõe uma série de fragilidades e inconsistências. Dada a ampla influência do código do almirantado, e os esforços de muitos membros da aliança para se adequarem à doutrina da OTAN, as questões descritas abaixo são comuns na maioria das normas examinadas.

De acordo com o código do almirantado, classificações qualitativas de confiabilidade e credibilidade formam uma progressão comprovadamente intuitiva. No entanto, interpretações subjetivas dos limites entre essas classificações provavelmente variam entre os usuários, assim como interpretações dos critérios de classificação relevantes. Por exemplo, em muitas versões do código do almirantado, diz-se que uma fonte confiável ('A') tem um "histórico de confiabilidade completa", enquanto uma fonte geralmente confiável ('B') tem um "histórico de informações válidas na maioria das vezes" (Irwin *et al*, 2020).

Nenhuma das normas examinadas associa essas descrições com valores numéricos (ou seja, "médias de rebatidas"), potencialmente levando a uma falha de comunicação. Um analista pode atribuir geralmente confiável a fontes que fornecem informações válidas > 70% do tempo. Um analista que recebe essa classificação pode interpretá-lo como uma informação válida > 90% do tempo, e colocar mais confiança na fonte do que é garantido. Por outro lado, um analista pode assumir que geralmente informações confiáveis refletem informações válidas apenas > 50% do tempo, e prematuramente descontar a fonte (Irwin *et al*, 2020).

Solicitados a atribuir valores absolutos de probabilidade a índices de confiabilidade e credibilidade, os oficiais de inteligência dos EUA demonstraram considerável variação em suas interpretações. Por exemplo, interpretações probabilísticas de geralmente confiáveis e provavelmente verdadeiras variaram de 0,55 a .90 e .53 a .90, respectivamente, enquanto interpretações de bastante confiáveis e possivelmente verdadeiras variavam de .40 a .80 (Irwin *et al*, 2020).

3.1 A TÉCNICA DE AVALIAÇÃO DE DADOS NO SIEx

A Técnica de Avaliação de Dados (TAD) tem por finalidade estabelecer os procedimentos para a aferição da credibilidade de dados, matéria-prima para a produção do conhecimento, condição essencial para que possam ser utilizados na elaboração dos diversos tipos de conhecimento de Inteligência (Brasil, 2019, p. 32).

Na aplicação da Metodologia para a Produção do Conhecimento, os dados disponíveis são submetidos à TAD e, dependendo do grau de credibilidade que lhes forem atribuídos, poderão ser utilizados nos diferentes tipos de produção dos conhecimentos de Inteligência

(Brasil, 2019, p. 33).

Na produção de um conhecimento de Inteligência, o analista somente utilizará os dados que foram avaliados quanto à credibilidade. O emprego da TAD depende do perfeito entendimento de como ocorre a comunicação do dado entre a fonte (emissor) e o destinatário.Comunicação é a transmissão de dados entre uma fonte e um destinatário (Brasil, 2019, p. 33).

Fonte de dados é tudo aquilo que contém, produz ou apreende um dado. As fontes podem ser pessoas, grupos, organizações, documentos, fotos, vídeos, instalações, equipamentos e qualquer outro elemento do qual se possa extrair dados de interesse para a Inteligência Militar (Brasil, 2019, p. 33).

Avaliador do dado é todo elemento que, ao receber um dado, está habilitado para determinar a sua credibilidade, por conhecer a TAD (Brasil, 2019, p. 33).

Cabe ressaltar que, entre a fonte e o avaliador, poderá existir um elemento intermediário, que se encarrega, simplesmente, de transmitir o dado. Esse elemento é o Canal de Transmissão, que tem condições de perceber, memorizar e descrever um fato ou uma situação (Brasil, 2019, p. 33).

O avaliador deve sempre considerar como o dado chegou ao seu conhecimento, para constatar se o recebeu diretamente da fonte ou por meio de um canal de transmissão (intermediário) (Brasil, 2019, p. 33).

Quando a transmissão do dado tiver ocorrido por meio de um intermediário, qualquer que seja ele, o avaliador deverá julgar a fonte e, também, julgar o Canal de Transmissão como fonte, conferindo maior credibilidade à sua avaliação (Brasil, 2019, p. 34).

O dado é avaliado quanto aojulgamento da fonte ejulgamento do conteúdo.

O julgamento da fonte tem por finalidade estabelecer o grau de sua idoneidade. Para isso, consideram-se três aspectos: autenticidade, confiança e competência.

Na autenticidade pergunta-se se o dado provém realmente da fonte presumida e, caso afirmativo, se foi nessa fonte que o dado se originou. Além disso verificam-se os canais de transmissão ou meios pelos quais passou o dado e os processos utilizados para identificação e reconhecimento das fontes.

No julgamento de confiança pergunta-se qual o envolvimento da fonte no episódio descrito, qual o interesse da fonte ao fornecer o dado, quais as características pessoais da

fonte e qual a contribuição já prestada anteriormente pela fonte. Verificam-se também os antecedentes (criminal, político, de lealdade, de honestidade etc.), o padrão de vida da fonte, a contribuição já prestada anteriormente e suas motivações.

Por último, ao julgar a fonte analisa-se sua competênciaonde se questiona se a fonte está habilitada a perceber e transmitir o dado e se sua localização permite perceber o fato ou a situação que descreveu. E verifica-se também os atributos pessoais da fonte para perceber, memorizar e descrever o fato ou a situação relatada.

O julgamento desses três aspectos caracteriza a idoneidade da fonte. Estabelecem-se 6 (seis) categorias para avaliar a fonte, representadas por letras do alfabeto:

a) "A" – Inteiramente idônea - É aquela que, ao longo do tempo em que vem sendo utilizada, atendeu sempre, de maneira positiva, aos aspectos dejulgamento;

b) "B" – Normalmente idônea - Em algumas oportunidades, deixou de atender a um ou mais dos aspectos de julgamento;

c) "C" – Regularmente idônea - Coloca-se numa situação intermediária, entre o número de ocasiões em que se conduziu positivamente, ou não, em relação aos aspectos de julgamento;

d) "D" – Normalmente inidônea - Na maioria das oportunidades, deixou de atender aos aspectos de julgamento;

e) "E" – Inidônea - Deixou de atender sempre aos aspectos de julgamento; e

f) "F" – A idoneidade não pôde ser avaliada - A fonte era desconhecida até o momento.

Já o julgamento do conteúdo tem por finalidade estabelecer o grau de veracidade do conteúdo do dado. Consideram-se três aspectos: semelhança, coerência e compatibilidade.

Na semelhança pergunta-se se o dado é confirmado por outras fontes. Além disso verificam-se quais os meios transmissores ou meios pelos quais passou o dado e se procura apurar se há outro dado cujo conteúdo esteja conforme o dado em julgamento.

No julgamento de coerência pergunta-se se o dado em julgamento apresenta contradições em seu conteúdo. Verifica-sea harmonia interna do dado e seu encadeamento lógico.

Por fim, o julgamento do conteúdo quanto àcompatibilidade onde se pergunta se o dado se harmoniza com outros conhecidos anteriormente. Verifica-se,portanto, o relacionamento do dado com o que se sabe sobre o fato ou a situação-objeto e se determina

qual o grau de harmonia do dado.

O julgamento desses três aspectos caracteriza a veracidade do conteúdo do dado. Estabelecem-se 6 (seis) categorias para avaliar a veracidade do conteúdo do dado, representadas por números:

a) "1" – Confirmado por outras fontes – conteúdo do dado difundido por outras fontes apresenta coerência e compatibilidade;

b) "2" – Provavelmente verdadeiro – conteúdo do dado não foi confirmado por outras fontes, entretanto apresentou coerência e compatibilidade;

c) "3" – Possivelmente verdadeiro - É aquele conteúdo do dado que, apesar de não ser confirmado, é coerente e possui compatibilidade parcial;

d) "4" – Duvidoso - Considera-se o conteúdo do dado que, embora coerente, não pôde ser confirmado e é pouco compatível com o que já se conhece sobre o fato ou a situação em julgamento;

e) "5" – Improvável - É o conteúdo do dado que não apresentou compatibilidade, não pôde ser confirmado, sendo coerente; e

f) "6" – Veracidade não avaliada - Esse conteúdo do dado não permite ao avaliador analisar nenhum dos parâmetros de julgamento. Nesse caso, os dados que tratam de assuntos rotineiros não devem ser difundidos até que seja possível atribuir-lhes outro grau de veracidade.

Após integrar os resultados obtidos no julgamento da fonte e do conteúdo, o analista expressa suas conclusões utilizando o código de avaliação de dados, conforme a combinação das duas colunas da tabela a seguir:

Quadro 2 - Resultado da Avaliação do Dado

Julgamento da Fonte	Julgamento do Conteúdo
A - Inteiramente idônea	1 - Confirmado por outras fontes
B - Normalmente idônea	2 - Provavelmente verdadeiro
C - Regularmente idônea	3 - Possivelmente verdadeiro
D - Normalmente inidônea	4 - Duvidoso

E - Inidônea	5 - Improvável
F - A idoneidade não pode ser avaliada	6 - A veracidade não pode ser avaliada

Fonte: Brasil (2019, p. 36).

3.2 A TAD NA FORÇA AÉREA BRASILEIRA

A técnica de avaliação de dados utilizada na Força Aérea Brasileira (FAB), assim como se realiza na OTAN e no SIEx, compreende o julgamento da fonte e de seu conteúdo, finalizando com a determinação do grau de credibilidade do dado.

O julgamento da fonte é realizado com a finalidade de estabelecer o grau de idoneidade dela. No julgamento, a idoneidade da fonte é considerada sob os mesmos três aspectos de julgamento já vistos anteriormente, ou seja, autenticidade, confiança e competência (Brasil, 2021).

Na autenticidade procura-se verificar se o dado provém realmente da fonte presumida. Este trabalho é desenvolvido mediante o estudo das particularidades e dos eventuais indicativos que permitam caracterizar a fonte. Cuidados especiais devem ser observados para distinguir fonte de canal de transmissão, já que muitas vezes surge entre a fonte e o avaliador a figura do intermediário do dado. Este intermediário é considerado canal de transmissão e não deve ser confundido com a fonte do dado. O intermediário também deve ser avaliado.

Na confiançasão considerados indicadores básicos relacionados àsfontes, tais como antecedentes, padrão de vida, contribuição já prestada ao sistemaemotivação.

Por último, no que tange à fonte, a análise da competênciajulga os indicadores habilitação e localização, igualmente como é realizada no SIEx.

Porém, ao final do julgamento da Fonte, chega-se a uma avaliação graduada somente em 4 níveis, diferentemente de como é realizado pelo SIEx. O resultado da avaliação da fonte na FAB chega nos seguintes níveis de credibilidade:

a) A – Idônea: É aquela que, ao longo do tempo em que vem sendo utilizada, atendeu sempre aos parâmetros considerados. Atende positivamente aos três parâmetros:

autenticidade, confiança e competência. Caracteriza–se pela precisão e comprovação posterior dos dados quedisponibiliza.

b) B - Regularmente Idônea: Na maioria das ocasiões, sua avaliação foi positiva em relação aos parâmetros. Atende aos parâmetros autenticidade e competência, mas não plenamente ao parâmetro confiança. Caracteriza-se por disponibilizar dados que normalmente se comprovam.

c) C - Regularmente Inidônea: Na maioria das ocasiões conduziu-se negativamente em relação às avaliações dosparâmetros. Pode atender ou não aos parâmetros autenticidade e competência. Apresenta pouco grau de confiança. Caracteriza–se por disponibilizar dados que normalmente não se comprovam.

d) D - Não Avaliada: A Fonte era desconhecida até o momento. Não há como avaliar o histórico da fonte em atendimento aos parâmetros por ser a sua primeira contribuição ao órgão de inteligência.

O julgamento do conteúdo considera o dado sob os aspectos de semelhança, coerência e compatibilidade, assim como os sistemas já vistos anteriormente.

A análise de semelhança consiste em verificar se há outro dado, oriundo de fonte diferente, cujo conteúdo esteja conforme ao do dado sob avaliação.

A avaliação da coerência consiste em identificar se o dado em questão não apresenta contradições em seu conteúdo. Busca-se, assim, verificar a sua harmonia interna, o seu encadeamento lógico.

E por último, a avaliação de compatibilidade é aferida estabelecendo-se o relacionamento do dado com o que se sabe sobre o mesmo fato ou situação, deste modo, procura-se examinar o grau de harmonia com que o dado se relaciona com outros dados e/ou conhecimentos anteriores.

Assim como no julgamento da fonte, a veracidade do conteúdo desdobra-se em somente 4 níveis e é expressa por meio de um código de avaliação numérico, conforme se segue:

a) 1 – Confirmado: Foi confirmado por outra (s) fontes (s) e apresenta um conteúdo coerente e compatível.

b) 2 – Provavelmente Verdadeiro: Embora não tenha sido confirmado por outra (s) fonte (s), apresenta coerência e compatibilidade.

c) 3 – Duvidoso: Embora coerente, não pôde ser confirmado por outra fonte e é pouco compatível com o que já se conhecesobre o fato ou situações consideradas.

d) 4– Não Avaliado: Não se pôde avaliar o conteúdo com relação aos parâmetros semelhança e compatibilidade.

> Antes de submeter um dado ao processo de avaliação, uma das preocupações do profissional de Inteligência deve ser com a definição do ponto de interesse do dado. Definir o ponto de interesse significa determinar qual o ponto do conteúdo de um dado recebido que interessa efetivamente ao Órgão de Inteligência para o desempenho da sua atividade em um determinado caso (Brasil, 2021).
>
> A importância da definição prévia do ponto de interesse relativo a um dado decorre de que isto auxiliará na identificação da fonte a ser avaliada, bem como determinará o enfoque a ser adotado pelo analista, por ocasião de sua utilização para a elaboração de um Conhecimento de Inteligência (Brasil, 2021).
>
> A questão do ponto de interesse é igualmente importante para a redação dos documentos de Inteligência, pois permite a perfeita definição do "Assunto" que está sendo tratado (Brasil, 2021).

Após observar exemplos de técnicas de avaliação de dados utilizados no Brasil e no exterior, conclui-se parcialmente que as técnicas empregadas atualmente para a avaliação de dados são vocacionadas para a fonte humana (*HUMINT*). Isso se dá pela hereditariedade da atividade de inteligência e pela recente incorporação de fontes tecnológicas que não tiveram ainda suas características estudadas de maneira separada para que se obtivesse uma técnica específica observada suas idiossincrasias.

4 CONCLUSÃO

A inteligência incorporou nos últimos anos capacidades tecnológicas que incrementaram o esforço de busca do dado negado e a coleta de dados disponíveis em fontes abertas. Na atual era da informação o principal trabalho do profissional de inteligência é o de selecionar bons dados a serem utilizados para a confecção de conhecimentos confiáveis para o processo decisório.

Dentro das novas capacidades das fontes tecnológicas incorporadas no Sistema de Inteligência do Exército está a fonte cibernética, ou *CYBINT*. A inteligência cibernética é a Inteligência elaborada a partir de dados, protegidos ou não, obtidos no espaço cibernético. Este, por sua vez, é caracterizado como o espaço virtual composto por dispositivos computacionais conectados em rede, onde informações digitais trafegam, são processadas ou armazenadas (Brasil, 2015b, p.22).

Ou seja, o conhecimento elaborado fruto dos dados provenientes de sistemas computacionais, estando em rede ou não seria uma definição simplificada do que é inteligência cibernética. Por se tratar de uma fonte técnica, muito se questiona sobre a capacidade de avaliar dados provenientes da *CYBINT*. Porém, para se propor uma solução de avaliação desta fonte é necessário entender o processo de extração dos dados e o papel do especialista da fonte na aquisição destes dados.

A aquisição de dados da fonte cibernética passa pelas três atividades desenvolvidas, quais sejam: ataque cibernético, proteção cibernética e exploração cibernética. Dessas três é na exploração cibernética onde encontramos a maior parte dos dados adquiridos. Vale lembrar que as outras duas atividades podem também adquirir dados, porém a formulação de conhecimentos não é alvo principal daqueles tipos de operação.

Além de saber selecionar qual tipo de atividade cibernética é o foco da *CYBINT*, é necessário entender que nos dias de hoje o desafio é selecionar dados de qualidade, pois o mundo que cerca o profissional de inteligência está saturado de toda sorte de dados. Portanto o bom analista descarta aquilo que não possui credibilidade e aproveita o dado mais fidedigno possível.

Nesse mister é necessário realizar uma boa avaliação de dados de forma a utilizar dados bem avaliados para a aumentar a qualidade do conhecimento a ser produzido pelo

profissional de inteligência. A grande maioria das técnicas de avaliação de dados utilizadas nos mais diversos serviços de inteligência do Brasil e do mundo se baseiam nos critérios de idoneidade da fonte e veracidade do conteúdo. Algumas agências graduam os critérios de julgamento do dado em 4 níveis, outros em 6 níveis, porém todos são unânimes em estabelecer um grau de totalmente confiável no que se refere à fonte e de certeza no que se refere ao conteúdo. Assim como todas as técnicas possuem o nível de impossibilidade de avaliação em ambos os aspectos.

A Técnica de Avaliação de Dados (TAD) realizada pelo SIEx tem por finalidade estabelecer os procedimentos para a aferição da credibilidade de dados, matéria-prima para a produção do conhecimento, condição essencial para que possam ser utilizados na elaboraçãodos diversos tipos de conhecimento de Inteligência (Brasil, 2019, p. 32).

Tanto a TAD adotada pelo SIEx quanto a adotada pelos principais serviços de inteligência nacionais e internacionais tem sua origem e principal destinação para avaliação de dados oriundos de Fontes Humanas (*HUMINT*). Quando separamos e analisamos separadamente os critérios de julgamento dos dados da TAD (credibilidade da fonte e veracidade do conteúdo) observamos dois fatos extremamente importantes.

O primeiro fato é que no que tange a análise do conteúdo (semelhança, compatibilidade e coerência) não há muito o que diferir dos dados obtidos por qualquer fonte, seja tecnológica ou não. O dado que se analisa é puro e não sofre influência de pessoas. Portanto, essa avaliação pode ser mantida da maneira e critérios hoje adotados no SIEx, sem ressalvas.

O segundo fato é entender que é na avaliação da Fonte que reside o grande entrave para a TAD das fontes tecnológicas, uma vez que os critérios de avaliação (autenticidade, confiança e competência) são ligados intrinsecamente a dados obtidos de pessoas. Características como antecedentes, motivações, padrão de vida, são aspectos da dimensão humana que não se aplica a máquinas, sistemas e redes.

Portanto, conclui-se que uma nova técnica de avaliação de dados para *CYBINT* manterá a análise da veracidade do conteúdo e terá uma nova forma de se avaliar a credibilidade da fonte.

Para cumprir com esse objetivo é necessário estabelecer a diferença entre sensor, canal de transmissão e equipamento de aquisição.

Sensor, segundo o dicionário da língua portuguesa, é um "dispositivo que permite adquirir, ler ou transmitir uma informação" ("sensor", no Dicionário Priberam da Língua Portuguesa, 2008-2021). Ou seja, sensor é todo aquele que apreende um dado e/ou possui capacidade de transmiti-lo. O homem funcionando como sensor decodifica o que apreendeu de maneira escrita ou verbal (relatórios).

Já o canal de transmissão é definido como um elemento intermediário, que se encarrega, simplesmente, de transmitir o dado proveniente da fonte do dado e o avaliador. Esse elemento tem condições de perceber, memorizar e descrever um fato ou uma situação (Brasil, 2019, p.33).

E finalmente, o equipamento de aquisição é todo material eletrônico, mecânico, óptico ou lógico que tem a capacidade de adquirir um dado, porém não o decodifica, ou seja, não ointerpreta. Sua capacidade de aquisição é fixa pela perenidade de suas características técnicas. Fornece o dado bruto como o adquiriu, não gerando a sua interpretação, dependendo da figura humana para "traduzir" o seu conteúdo.

Com base no exposto, elenca-se 03 (três) soluções viáveis para a avaliação da idoneidade da fonte cibernética: a não utilização da avaliação da fonte, a avaliação do equipamento ou a personificação do sensor.

A solução mais simples é não mais utilizar a avaliação da idoneidade da fonte no que tange à *CYBINT*. Para dados oriundos desta fonte somente seria utilizada a avaliação da veracidade do conteúdo (numérica) apresentando assim a não participação humana na origem do dado. O óbice da adoção dessa solução é o dado ser suscetível a manipulação, imperícia e motivações daquele ativo que originou de alguma forma o dado, contaminando assim a qualidade final do conhecimento.

Outra solução, porém, bem mais complexa, seria adotar a avaliação do equipamento que adquiriu o dado, porém, como foi abordado, suas capacidades já são preestabelecidas e, neste caso, haveria a necessidade de confrontar o conteúdo com essas capacidades, uma vez que nem todo dado pode ser obtido por determinado equipamento. Um exemplo para a *CYBINT* seria avaliarum determinado software de decriptografia, uma rede, um disco rígido ou um determinado computador em relação a determinado dado obtido. Essa linha de ação tem o problema de contaminar a avaliação uma vez que não mais seria feita de maneira estanque. Haveria a necessidade de examinar o conteúdo para determinar se a capacidade do

equipamento teria essa potencialidade, o que se torna subjetivo e de difícil mensuração técnica, pois o resultado da análise também depende da interação humana (*peopleware*).

A última Linha de Ação para a realização da TAD de *CYBINT* é a personificação do sensor. Consiste em encontrar a pessoa que serviu como sensor e realizou a decodificação do dado oriundo do espaço cibernético. Traçando um paralelo com a fonte humana, é como se um agente de operações funcionasse como canal de transmissão ao trazer um dado de um colaborador, porém ele mesmo é o sensor quando traz um dado que ele mesmo apreendeu no AmbOp (observou uma coluna de blindados, por exemplo). No primeiro caso a fonte é o colaborador e no segundo a fonte é ele mesmo.

De igual maneira funcionaria a *CYBINT*. Caso o operador da fonte cibernética consiga extrair por trás do dado buscado a pessoa que produziu o dado (autor) ele avaliará essa pessoa como fonte, porém se ele mesmo for o decodificador do dado oriundo do equipamento de aquisição utilizado, a fonte é ele mesmo (o operador é o sensor). Em outras palavras seria avaliar a pessoa que forneceu o dado.

A busca da personificação do sensor, em qualquer fonte tecnológica, soluciona uma antiga questão no SIEx que é traduzir para a linguagem da inteligência um idioma extremamente técnico e restrito aos especialistas da área.

Por fim, entre as três soluções apresentadas, este autor identifica como sendo a personificação do sensor como a melhor solução para avaliar os dados provenientes da fonte cibernética, que passo a detalhar.

A veracidade do conteúdo se mantém como a prevista atualmente no SIEx, conforme tabela abaixo:

Quadro 3 – Veracidade da informação

Para Determinar	Pergunta-se	Verifica-se
SEMELHANÇA	- O dado é confirmado por outras fontes?	- Quais os meios transmissores ou meios pelos quais passou o dado? - Há outro dado cujo conteúdo esteja conforme o dado em julgamento?
COERÊNCIA	- O dado em julgamento apresenta contradições em seu conteúdo?	- Há harmonia interna do dado? - Há encadeamento lógico?

COMPATIBILIDADE	- O dado harmoniza-se com outros conhecidos anteriormente?	- Há relacionamento do dado com o que se sabe sobre o fato ou a situação que é objeto do mesmo? - Qual o grau de harmonia do dado?

Fonte: O autor.

Esse julgamento desses três aspectos caracteriza a veracidade do conteúdo do dado e se estabelecem as já conhecidas 6 (seis) categorias adotadas pelo SIEx para avaliar a veracidade do conteúdo do dado, representadas por números, de 1 a 6 onde:"1" – dado confirmado, "2" – dado provavelmente verdadeiro, "3" – dado possivelmente verdadeiro, "4" – dado duvidoso, "5" – dado improvável e "6" – veracidade não avaliada.

A grande diferença está na avaliação da idoneidade da fonte, onde se buscaria personificar a pessoa ou especialista que gerou a decodificação do dado. Se analisaria da mesma maneira a autenticidade, confiança e competência, porém com as seguintes características abaixo.

Quadro 4 – Idoneidade da fonte

PARA DETERMINAR	**PERGUNTA-SE**	**VERIFICA-SE**
AUTENTICIDADE	- O dado provém realmente da fonte presumida? - Em caso afirmativo, foi nessa fonte que o dado se originou? - Em caso negativo avalia-se o especialista de *CYBINT* que decodificou o dado	- Canais de transmissão ou meios pelos quais passou o dado. - Processos utilizados para identificação e reconhecimento das fontes. - Em caso de fontes oriundos de redes, IP, domínios e páginas de internet, buscam-se o proprietário intelectual do dado (uma pessoa)
CONFIANÇA	- Uma vez identificada a pessoa que forneceu o dado, qual seu envolvimento no episódio descrito? - Qual o interesse da pessoa ao	- Antecedentes (criminal, político, de lealdade, de honestidade etc.). - Padrão de vida é compatível ou não com o seu poder aquisitivo (cargo,

	fornecer o dado? - Quaisas características pessoais da fonte? - Qual a contribuição já prestada anteriormente pela pessoa que forneceu o dado? - Quantas vezes a decodificação feita pela pessoa teve resultado positivo?	emprego, situação em relação ao OI/AI etc.). - Contribuição já prestada (precisão dos dados etc.). - Motivação (ciúme, vingança, patriotismo, pagamento, interesse pessoal, sentimento do dever etc.).
COMPETÊNCIA	- A pessoa possui habilitação adequada para produzir, perceber e transmitir o dado? - A localização da fonte permite perceber o fato ou a situação que descreve?	- Atributos pessoais da fonte para perceber, memorizar e descrever o fato ou a situação (experiência relativa ao assunto). - Habilitação técnica para produzir o dado.

Fonte: O autor.

Dessa maneira, adotar-se-ia a gradação já em uso pelo SIEx, com 6 (seis) categorias para avaliar a fonte, representadas por letras do alfabeto, de A a F normalmente, porém se atentando que há a necessidade de identificar a pessoa que decodificou tecnicamente o dado oriundo da fonte tecnológica para a produção do conhecimento.

REFERÊNCIAS

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Manual de Campanha Planejamento e Emprego da Inteligência Militar**. EB70-MC-10.307. Estado-Maior do Exército. Brasília, DF, 2016a.

BRASIL. Exército Brasileiro. Estado-Maior. EB70-MT-10.401: **Produção do Conhecimento de Inteligência**. Brasília, DF, 2019.

BRASIL. Exército Brasileiro. Estado-Maior. **Manual de Campanha Inteligência**. EB20-MC-10.207. Estado-Maior do Exército. 2015. Brasília, DF, 2015a.

BRASIL. Exército Brasileiro. Estado-Maior. **Manual de Fundamentos Inteligência Militar Terrestre**. EB20-MF-10.107. 2. ed. Estado-Maior do Exército. Brasília, DF, 2015b.

BRASIL. Exército Brasileiro. Estado-Maior. **Vade-Mécum de Inteligência Militar**. Brasília, DF, 2011.

BRASIL. Força AéreaBrasileira. CIAer. **Metodologia para Produção do Conhecimento**. MCA 200-24. Brasília, DF, 2021.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Doutrina Nacional da Atividade de Inteligência**. Brasília, DF, 2016b. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/Col3v5.pdf. Acesso em: 26 jun 2021.

BRASIL. Ministério da Defesa. **Doutrina de Inteligência de Defesa**. MD52-N-01. Brasília, DF, 2005.

DICIONÁRIO Priberam da Língua Portuguesa (*on-line*). 2008-2021. Disponível em: https://dicionario.priberam.org/sensor. Acesso em: 26 jun 2021.

Heylighen, Francis; JOSLYN, Cliff. Cybernetics and Second Order Cybernetics. In R. A. Meyers (Ed.), **Encyclopedia of Physical Science and Technology**, Eighteen-Volume Set, Third Edition, p. 155-170, 2001. Academia Press. http://pespmc1.vub.ac.be/Papers/Cybernetics-EPST.pdf

IRWIN, Daniel; MANDEL, David R. **STANDARDS FOR EVALUATING SOURCE RELIABILITY AND INFORMATION CREDIBILITY IN INTELLIGENCEPRODUCTION**. DRDC Toronto Research Centre Defence Research and Development Canada. NATO Assessment and Communication of Uncertainty in Intelligence to Support Decision-Making Chapter 7AC/323 (SAS-114) TP/928STO-TR-SAS-114pp. 7-1–7-16, 2020

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. **Manual de Metodologia da Pesquisa Científica**. Centro de Estudos de Pessoal. Escola de Aperfeiçoamento de Oficiais: Rio de Janeiro: 2007.

PORTELA, Lucas Soares. Agenda de Pesquisa sobre o Espaço Cibernético nas Relações Internacionais. **Rev. Bra. Est. Def**. v. 3, nº 1, jan./jun. 2016, p. 91- 113.
SALES, Rodrigo; ALMEIDA, Patrícia Pinheiro. Avaliação de Fontes de Informação na Internet: Avaliando O Site Do Nupill/Ufsc. **Revista Digital de Biblioteconomia e Ciência da Informação,** Campinas, v. 4, n. 2, p. 67-87, jan./jun. 2007.

WENDT, Emerson. **Inteligência cibernética**: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil [recurso eletrônico] / Emerson Wendt. – livro digital. – São Paulo: Editora Delfos, 2011.