Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Artigo de pesquisa

Jomar Barros de Andrade[1]
ORCiD 0009-0000-6136-1289

APLICAÇÃO DOS FUNDAMENTOS DA METODOLOGIA DA PRODUÇÃO DO CONHECIMENTO PARA A INTELIGÊNCIA CIBERNÉTICA

https://doi.org/10.58960/rbi.2025.20.273

De Andrade, Jomar Barros. 2025. "Aplicação dos Fundamentos da Metodologia da Produção do Conhecimento para a Inteligência Cibernética," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.273. https://doi.org/10.58960/rbi.2025.20.273.

Recebido em 31/03/2025
Aprovado em 10/07/2025
Publicado em 07/10/2025

1 General-de-Brigada da Reserva do Exército Brasileiro. Mestre em Ciências Militares (ECEME). Especialista em Inteligência Militar. Foi Chefe do Centro de Estudos Estratégicos do Exército (CEEEx), do Centro de Defesa Cibernética (CDCIBER) e 2º Subchefe (Informação e Comando e Controle) do Estado-Maior de Exército (EME). Desde 2020, concentra sua atuação nas áreas de Inteligência, Comando e Controle e Cibernética. Atualmente, desempenha o cargo de Gerente do Programa Estratégico Defesa Cibernética do Exército, garantindo as entregas de seus diversos projetos e contribuindo com o planejamento desse Setor Estratégico de Defesa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

APLICAÇÃO DOS FUNDAMENTOS DA METODOLOGIA DA PRODUÇÃO DO CONHECIMENTO PARA A INTELIGÊNCIA CIBERNÉTICA

Resumo

A Inteligência e a Defesa Cibernética utilizam dados oriundos do espaço cibernético para atingir seus objetivos. Apesar de a Doutrina da Atividade de Inteligência fornecer os fundamentos gerais, a produção do conhecimento a partir da fonte cibernética demanda o seu aprofundamento. A Técnica de Avaliação de Dados de Cibernética deve ser ampliada para além de seus aspectos originalmente desenvolvidos para as fontes humanas. Para tanto, a lições aprendidas pela Segurança Cibernética são úteis e valiosas. A Metodologia da Produção do Conhecimento empregada para a Inteligência Cibernética, servindo-se de técnicas, procedimentos e ferramentas específicas, é fundamental para que seja possível o desenvolvimento de aplicações de Inteligência Artificial. Por fim, a formação dos recursos humanos deve evoluir, para que mais componentes do Sistema Brasileiro de Inteligência contribuam para a produção de conhecimento cibernético.

Palavras-chave: Inteligência, defesa cibernética, Inteligência Artificial, metodologia.

APPLICATION OF THE FOUNDATIONS OF THE KNOWLEDGE PRODUCTION METHODOLOGY TO CYBER INTELLIGENCE

Abstract

Intelligence and Cyber Defense employ data originating from cyberspace to achieve their objectives. Although the Doctrine of Intelligence Activity provides general foundations, the production of knowledge from cyber sources requires further development. The Cyber Data Evaluation Technique must be expanded beyond its aspects originally developed for human sources. To this end, the lessons learned from Cybersecurity are useful and valuable. The Knowledge Production Methodology employed for Cyber Intelligence, making use of specific techniques, procedures, and tools, is essential for enabling the development of Artificial Intelligence applications. Finally, the training of human resources must evolve, so that more components of the Brazilian Intelligence System may contribute to the production of cyber knowledge.

***Keywords**: Intelligence, cyber defense, Artificial Intelligence, methodology.*

APLICACIÓN DE LOS FUNDAMENTOS DE LA METODOLOGÍA DE PRODUCCIÓN DE CONOCIMIENTO PARA LA INTELIGENCIA CIBERNÉTICA

Resumen

La Ciberinteligencia y la Ciberdefensa utilizan datos del ciberespacio para alcanzar sus objetivos. Si bien la Doctrina de la Actividad de Inteligencia proporciona las bases generales, la producción de conocimiento a partir de fuentes cibernéticas requiere mayor estudio. La Técnica de Evaluación de Datos Cibernéticos debe ampliarse más allá de sus aspectos desarrollados originalmente para fuentes humanas. Para ello, las lecciones aprendidas en Ciberseguridad son útiles y valiosas. La Metodología de Producción de Conocimiento empleada para la Ciberinteligencia, que utiliza técnicas, procedimientos y herramientas específicos, es esencial para el desarrollo de aplicaciones de Inteligencia Artificial. Finalmente, la formación de recursos humanos debe evolucionar para que más componentes del Sistema de Inteligencia Brasileño contribuyan a la producción de conocimiento cibernético.

***Palabras clave**: Inteligencia, ciberdefensa, Inteligencia Artificial, metodología.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Introdução

A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação (TIC) e das oportunidades econômicas e sociais oriundas do ambiente digital (Brasil 2020). A conectividade em tempo integral e a disponibilidade imediata de conteúdo tornaram-se aspectos fundamentais da vida de grande parcela da sociedade.

A Estratégia Nacional de Segurança Cibernética (E-Ciber), já em sua introdução, destaca que tais avanços fazem surgir, na mesma proporção, novas e crescentes ameaças que colocam em risco a administração pública e a sociedade. Além disso, a escala de produção e a disponibilização de informação representam oportunidades e desafios para a Inteligência, o que tem levado, no exterior, a estudos para a criação de estruturas dedicadas à produção do conhecimento especializadas no domínio cibernético (AFCEA 2022).

Sobre esse cenário já altamente complexo, a rápida expansão de aplicações de Inteligência Artificial (IA) tem levado as organizações, ao redor do mundo, a uma corrida para a adoção de ferramentas com essa tecnologia. Reconhecimento de imagens, tradução de idiomas e o uso de ferramentas conversacionais, dentre outras, já são realidade nas áreas de Defesa, Inteligência e Segurança Pública, em diversos países (McMahon 2024, 1).

A Inteligência de Estado e seus profissionais são desafiados por essa conjuntura. Nesse contexto, a Doutrina da Atividade de Inteligência (DAI) estabeleceu o conceito de Inteligência Cibernética como aquela voltada a temas relativos ao Espaço Cibernético (EC), cuja produção busca apoiar a atuação do Brasil frente a vulnerabilidades e ameaças, informando políticas públicas e planos estatais nesse domínio, bem como acompanhar e avaliar capacidades, intenções e atividades de atores externos naquele espaço (Brasil 2023b, 159).

Cabe destacar que o conceito de Fonte é fundamental para a atividade. A expressão Fonte Cibernética, embora não expressamente definida na DAI, passará a ser utilizada para indicar a origem, no espaço cibernético, dos dados utilizados por aquela disciplina.

Pelo seu caráter especializado, a atividade de Inteligência se apoia na Metodologia da Produção do Conhecimento (MPC) (Brasil 2023b, 107) que, com os ajustes necessários às particularidades de cada setor, está consagrada

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

por seu emprego em diversos órgãos de Inteligência brasileiros (Brasil 2023b, 106). No entanto, não há dúvidas que o seu arcabouço teórico, embora consolidado, foi desenvolvido originalmente para trabalhar com fontes humanas (Calaça 2023, 156).

Com o já citado exponencial desenvolvimento das TIC, em especial na área de Cibernética, surgiram novas oportunidades para a Inteligência. No entanto, para que os produtos elaborados a partir de dados oriundos dessas fontes tecnológicas sejam confiáveis, oportunos e possuam a qualidade necessária aos desafios, atuais e futuros, a serem enfrentados pelo Brasil, é necessário que os fundamentos da MPC se desenvolvam e sejam capazes de embasar a atuação nesses domínios.

Destaca-se que, apesar de seus diferentes conceitos e objetivos, a análise de seus respectivos fundamentos evidencia a existência de pontos em comum entre a Segurança Cibernética, a Defesa Cibernética e a Inteligência. Na primeira, o principal ator no que se refere ao Setor Cibernético é o Gabinete de Segurança Institucional da Presidência da República (GSI-PR), preponderando as atividades de proteção, enquanto na segunda, também passa a haver a possiblidade de execução de medidas de exploração e ataque, em cumprimento às demandas das autoridades competentes (Brasil 2023d, 28). A Inteligência se relaciona com ambas, tanto contribuindo para a proteção da informação, quanto se beneficiando dos dados obtidos e dos conhecimentos produzidos (Brasil 2023d, 17).

Porém, ao mesmo tempo que tal convergência indica a possibilidade de compartilhamento de procedimentos e técnicas, também as diferenças de escopo, prioridades e tempos de atuação devem ser bem compreendidas, a fim de permitir uma atuação coordenada dos respectivos órgãos especializados.

Por meio de uma metodologia da pesquisa bibliográfica, o presente artigo irá revisar a literatura existente sobre o tema, aí considerados o marco legal em vigor, os manuais de emprego das Forças Armadas, a produção científica nacional e internacional e, principalmente, a Doutrina da Atividade de Inteligência. Desse modo, o objetivo é aprofundar e expandir uma metodologia oficial.

A análise está estruturada para, ao longo do desenvolvimento, obter o alinhamento dos conceitos na bibliografia, apontando tanto os fundamentos da DAI que são diretamente aplicáveis à Cibernética, quanto aqueles que necessitam de adaptações, para os quais serão apresentadas sugestões

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

baseadas na literatura selecionada. Ao longo do trabalho, serão levantados aspectos relativos ao impacto da IA nas diversas etapas da metodologia.

Por fim, ênfase especial será dada à Técnica de Avaliação de Dados e à execução das fases do ciclo de produção do conhecimento, para o que serão realizados estudos de caso sumários, para contextualizar sua aplicação para a Inteligência Cibernética.

O Espaço Cibernético e os processos de Coleta e Busca de dados

Para a DAI, o Espaço Cibernético é entendido como o conjunto das infraestruturas informáticas e telemáticas interconectadas, que compreende hardware, software, dados, usuários e quaisquer relações lógicas entre eles (Brasil 2023b, 49). Com isso, são de interesse para a Inteligência Cibernética tanto as redes e equipamentos de comunicações quanto os sistemas de informação sobre eles estabelecidos e, não menos importantes, as pessoas que atuam e se relacionam naquele ambiente.

A Doutrina Militar de Defesa Cibernética (DMDC) apresenta definição semelhante, considerando o EC como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (Brasil 2023d, 17). Além disso, divide o espaço cibernético em três camadas: física (dispositivos e infraestrutura de TIC), lógica (aplicações, serviços, protocolos, etc) e ciberpersona (identidades virtuais dos usuários). Tais conceitos serão úteis posteriormente, ao considerarmos a atuação das diferentes disciplinas da Inteligência no EC (Brasil 2015).

Conclui-se que o Espaço Cibernético é transversal às áreas de atuação interna e externa e, embora a Inteligência Cibernética tenha foco nos temas a ele relacionados, não esgota o tema, nem exclui sua importância para as demais áreas. Para fins da MPC, o espaço cibernético em si não é a fonte dos dados, mas o ambiente onde os dados estão. Portanto, para que tais dados sejam obtidos, devem existir os fundamentos técnicos e regulatórios para que sejam realizadas ações especializadas (Brasil 2023b, 145) e ações operacionais (Brasil 2023b, 144) no ciberespaço.

De maneira geral, os conceitos de busca e coleta previstos na DAI são aplicáveis no ambiente cibernético, com as necessárias contextualizações. Coleta é ação especializada que visa à obtenção de dados e informações de livre acesso (Brasil 2023b, 149). Sob o ponto de vista da Inteligência Cibernética,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

enquadram-se na situação de livre acesso os sítios, blogs, serviços de notícias, dentre outros, mesmo aqueles para os quais seja necessário um registro ou assinatura, gratuito ou não, que permita o acesso ao conteúdo oferecido.

Em qualquer circunstância, o acesso a qualquer insumo ou produto do trabalho da Atividade de Inteligência se baseia na necessidade de conhecer (Brasil 2023b, 166). Isso posto, mesmo na coleta de dados já devem ser identificadas e adotadas as medidas de segurança que garantam o sigilo e a discrição, inerentes ao trabalho do profissional de Inteligência (Brasil 2023b, 29).

Busca, por sua vez, é a aplicação combinada de técnicas operacionais para obtenção de dados, informações e conhecimentos indisponíveis (Brasil 2023b, 148). No EC, a busca é realizada sobre redes, sistemas ou qualquer outro componente do ambiente, inclusive pessoas, cujo acesso não seja ostensivamente permitido ou exija o emprego de técnicas especializadas operacionais, para acessar e extrair os dados de interesse.

As técnicas operacionais raramente são empregadas de forma isolada (Brasil 2023b, 137). No caso específico das ações cibernéticas, as características do ambiente naturalmente levam a uma combinação de procedimentos, onde a busca de dados indisponíveis vai exigir o uso especializado de recursos técnicos, o que eventualmente pode ser feito de forma anônima a partir de um ponto de acesso, com outras similares às ações baseadas em recursos humanos, porém adaptadas às características ciberespaço.

Nesse sentido, não há como deixar de identificar a importância, para efeitos do estudo dessa temática, do emprego de modelos conceituais (ou *frameworks*) para conhecer as ameaças e para a normatização das ações proativas (aqui consideradas tanto as operações cibernéticas, quanto as de Inteligência no ciberespaço). A DAI não contempla esse tipo de *framework,* razão pela qual é oportuna a menção ao Modelo Comum de Ameaça Cibernética (*Common Cyber Threat Framework* - CCTF), elaborado pelo Escritório do Diretor Nacional de Inteligência dos Estados Unidos da América (EUA 2018).

Originalmente elaborado para permitir uma melhor compreensão da ameaça cibernética, no âmbito da comunidade de Inteligência norte-americana, nele é visível a incorporação e a simplificação dos conceitos de *Cyber Kill Chain* (Lockheed Martin s.d.), e a estrutura MITRE ATT&CK (Mitre Corporation s.d.), sintetizados em um modelo de quatro etapas: preparação, engajamento, presença e efeito/consequência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Embora a solução dessa lacuna específica esteja fora do escopo deste artigo, entende-se que a incorporação de soluções como o CCTF à DAI pode contribuir tanto para o desenvolvimento de técnicas de busca no espaço cibernético, quanto para a Contrainteligência, com a aplicação dos conceitos da segurança cibernética aplicados na proteção contra ameaças no ciberespaço. Tal situação é mais uma evidência prática da, já mencionada, convergência de fundamentos entre a Inteligência e a Defesa/Segurança Cibernética.

Cabe destacar que dados ou redes mal protegidos não podem ser considerados abertos e, ainda que sua obtenção possa ser feita com o emprego de técnicas simples, ainda assim envolvem procedimentos que só podem ser empregados por pessoal especializado, no contexto de uma Operação de Inteligência. Dessa forma, a penetração em redes externas é um tema sensível, que demanda o estabelecimento de rígidos mecanismos de controle.

A Fonte Cibernética, a Inteligência Cibernética e o Analista de Inteligência

O conceito de Fonte é basilar para a atividade de Inteligência. Definida como a origem de um dado, informação ou conhecimento (Brasil 2023b, 156), as suas características são as discriminadoras dos tipos de Inteligência atualmente contemplados pela DAI, quais sejam, de Fontes Humanas (*Human Intelligence* – HUMINT), Fontes Técnicas (*Technical Intelligence* – TECHINT) ou Fontes Abertas (*Open Source Intelligence* – OSINT). A doutrina considera que os dados oriundos do espaço cibernético estão abarcados pela Inteligência de Sinais (*Signals Intelligence* – SIGINT), que é uma subdivisão da TECHINT.

No entanto, a literatura não dá uma definição de Inteligência Cibernética em função da fonte de seus dados, como nos demais tipos. A DAI, embora adote essa expressão, a define quando trata das áreas de atuação, junto com as inteligências interna, externa e transnacional (Brasil 2023b, 53).

Para fins deste artigo, não será oferecida uma definição diferente da que já está na doutrina, mas será aproveitado o acrônico constante da Inteligência Militar Terrestre, sendo empregada o termo CYBINT (de Cyber Intelligence), para designar a Inteligência Cibernética (Brasil 2015, 3-4), disciplina cujos dados principais têm origem em fontes atuando ou localizadas nas diversas camadas do ciberespaço.

Assim sendo, aplicando-se os conceitos apresentados, até o momento, às peculiaridades do EC, podem ser consideradas como possíveis fontes ciber-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

néticas, dentre outras:

> • Operadores de sistemas próprios (cuja capacidade técnica, perícia ou talento individual sejam fatores determinantes para o resultado alcançado);
>
> • Agentes de Inteligência;
>
> • Sistemas automatizados especializados em obter e processar dados oriundos do ambiente cibernético, cujo produto possa ter sua veracidade acompanhada ao longo do tempo;
>
> • Fontes abertas diversas, gratuitas ou não, especializadas em pesquisa, acompanhamento, análise ou quaisquer outros serviços, voltados para a coleta e processamento de dados oriundos do ambiente cibernético; e
>
> • Operadores de sistemas do alvo, ou outros elementos que tenham acesso ao mesmo, a partir de seu recrutamento como colaboradores.

Nesse ponto, cabe destacar que não se deve confundir a CYBINT com a Inteligência de Ameaças, denominação amplamente consolidada da área da Segurança e Defesa Cibernéticas, que levanta e organiza informação detalhada e acionável sobre ameaças cibernéticas (IBM 2022), de diversos tipos (*malwares, phishings, zero-day exploits,* etc) (IBM 2024a) e atores, em especial as Ameaças Persistentes Avançadas (*Advanced Persistent Threats* – APT) (IBM 2024a). Embora a última produza dados e informações que são utilizados pela primeira, o escopo da CYBINT é bem mais amplo, por não estar limitado ao estudo apenas das ameaças.

Ressalta-se que, atualmente, várias disciplinas de Inteligência, além da CYBINT, atuam no espaço cibernético. A totalidade dos dados de interesse da Inteligência de Mídias Sociais (*Social Media Intelligence* – SOCMINT) (Brasil 2023b, 160) e a maioria dos utilizados pela OSINT, e até pela HUMINT, se encontram no EC.

Aproveitando o conceito de camadas do EC apresentado pela DMDC, SOCMINT e HUMINT atuam fortemente na camada de Ciberpersona, OSINT coleta dados nos sistemas operados na camada Lógica, enquanto categorias de TECHINT têm como foco os sistemas da camada Física. A CYBINT, pela variedade de seus objetivos, atua nas três camadas, de forma coordenada com as demais disciplinas e aproveitando os conhecimentos por elas produzidos.

Longe de ser contraditória, tal situação apenas reforça a característica da Inteligência de se apoiar na integração de diversas fontes para produzir conhecimento. No entanto, aponta também para a necessidade de alinhamento e padronização das técnicas especializadas, empregadas pelos diversos atores.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Os profissionais de inteligência contam com extensa bibliografia sobre a aplicação de Técnicas de Análise Estruturada (TAE) para a produção de conhecimento, sendo crescente o número de profissionais, de diversas áreas, especializados em questões do espaço cibernético. No entanto, não é comum a disponibilidade, em fontes abertas, de material acadêmico ou profissional que faça a convergência das TAE com a cibernética.

O Analista de Inteligência deve possuir, ao mesmo tempo, a competência técnica para trabalhar com os dados das diversas fontes, conforme sua especialidade, e o domínio da MPC.

Em consequência, o arcabouço intelectual de um Analista de CYBINT deve abranger uma base técnica em cibernética, que permita a compreensão do linguajar da área, mas também uma visão abrangente da conjuntura, permitindo a compreensão e a integração de fatos e eventos em todos as expressões do Poder Nacional (político, econômico, psicossocial, militar, científico e tecnológico) (Brasil 2024, 29). Além disso, deve ter conhecimento sobre assuntos de TECHINT e estar familiarizado com técnicas e procedimentos de OSINT e SOCMINT, entre outras, para que possa identificar vulnerabilidades e ameaças, apoiar o processo decisório e acompanhar atores externos no EC.

Ao mesmo tempo, para que os dados obtidos, a partir dos diversos aspectos inerentes a esse ambiente, sejam transformados em conhecimento utilizável, esse profissional deve dominar a MPC, sendo capaz de contemplar as peculiaridades inerentes ao processamento de dados oriundos dos diversos tipos de fonte. Com essas características, o profissional será capaz de ir além dos aspectos puramente técnicos da temática e produzir conhecimentos que, efetivamente, possam contribuir para reduzir a incerteza no processo decisório dos assuntos que se relacionam com a Cibernética.

Inteligência Artificial e CYBINT

O surgimento de programas de computador que simulam a conversa humana com o usuário final, utilizando técnicas de IA conversacional, como processamento de linguagem natural (PLN), conhecidos como chatbots (IBM, 2021), foi um evento disruptivo. Para a Inteligência, essas aplicações representam uma oportunidade de melhoria na rapidez e qualidade no tratamento de grande quantidade de dados, permitindo ao analista mais tempo para a sua interpretação.

A Empresa de Dados Abertos (*Open Source Enterprise* – OSE), subordinada

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

à Diretoria de Inovação Digital (FAS 2015) da Agência Central de Inteligência (Central Intelligence Agency – CIA), lançou uma ferramenta interna, no estilo do ChatGPT, para permitir melhor acesso às fontes abertas por seus analistas (McMahon 2024, 1). No entanto, junto com o entusiasmo por seu potencial, surgem também preocupações com a ética e a integridade da informação contida nos produtos gerados por IA (UNESCO, s.d.).

Em um trabalho produzido para o Centro de Excelência em Defesa Cibernética Cooperativa (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN), Biondi et al. (2021, 12-28) expõem que, embora a definição de CYBINT e seu relacionamento com as demais disciplinas seja uma tarefa em curso, já são inúmeras as oportunidades para a aplicação de técnicas de IA e aprendizado de máquina em seu proveito. Os autores destacam, dentre outras, o contraterrorismo, a identificação de relacionamentos em múltiplos domínios, a descoberta de radares, o ataque contra redes sem fio, a quebra de senhas, a superação de sistemas de proteção, dentre outros.

Apesar dessas possibilidades serem facilmente visualizadas, a efetiva implementação da IA na CYBINT passa por consideráveis desafios. Embora essa análise esteja além do escopo deste trabalho, devem ser destacados alguns aspectos fundamentais, que terão impacto na execução da MPC.

Para tanto, é especialmente interessante o trabalho de Goldfarb et al. (2021, 17) que, ao estudarem as possibilidades da IA e do aprendizado de máquina em apoio ao processo decisório (uma das missões fundamentais da Inteligência), propõem que são duas as variáveis que definem o desempenho de um sistema dessa natureza: a qualidade dos dados e a dificuldade para o julgamento. Dados são de alta qualidade quando a informação de qualidade é abundante e não contaminada por preconceitos, vieses e outras anomalias. A dificuldade para o julgamento é menor, por sua vez, quando os objetivos são claramente definidos e têm a concordância dos diversos envolvidos. Em situações em que os dados são de alta qualidade e o julgamento é claro, sistemas automatizados seriam até mais eficientes que os seres humanos. Na situação oposta, onde os dados são de baixa qualidade e o julgamento é difícil, a automatização não é possível (Quadro 1).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Quadro 1
Implicação dos Dados e do Julgamento para a automação do processo decisório

		Dados	
		Alta qualidade	**Baixa qualidade**
Julgamento	**Claro**	Processo decisório totalmente automatizado é mais eficiente	Automação completa é possível, mas arriscada
	Difícil	Predições automatizadas podem assessorar decisões humanas	Processo decisório automatizado não é possível

Fonte: Goldfarb *et al.* 2021, 18.

O raciocínio de Goldfarb et al. é especialmente apropriado para o emprego do aprendizado de máquina pela Inteligência. Embora as aplicações já estejam em curso e as possibilidades sejam amplas, a IA somente será eficiente caso seus algoritmos sejam desenvolvidos sobre processos muito bem estabelecidos e alimentados com dados de alta qualidade.

Dessa forma, a existência de uma MPC sólida para a Cibernética é fator crítico para o sucesso de iniciativas de Inteligência Artificial na CYBINT. Em síntese, são necessários Analistas de Cibernética, tanto para ensinar as máquinas a realizar a análise, quanto para rotular os dados necessários para seu treinamento.

O emprego de *chatbots* para a resposta de perguntas objetivas, apresentando os resultados em formato definido, já é uma realidade. Para tanto, tais sistemas acessam bancos de dados, selecionam o que é relevante e produzem textos, desempenhando o papel de fonte e de analista. Assim sendo, é fundamental que a credibilidade dessa fonte, a veracidade desses dados e a qualidade desse analista sejam conhecidos.

Não há resposta imediata para essa questão. No entanto, é fundamental que os produtos gerados por IA atendam aos requisitos exigidos pela MPC, para que possam basear a produção de conhecimentos, com impacto em todas as disciplinas que tocam o espaço cibernético, mas principalmente na OSINT e CYBINT.

Como fundamento para uma possível abordagem prática, são interessantes os aspectos estabelecidos na Diretiva para a Comunidade de Inteligência 203 (*Intelligence Community Directive* 203 – ICD 203), do Escritório do Diretor Nacional de Inteligência dos EUA. O trabalho foi a consequência dos estudos realizados para corrigir processos que levaram às falhas de inteligência sobre a existência de armas de destruição em massa, que acabaram fundamentando a invasão do Iraque pelos EUA, em 2003 (McMahon 2024, 2).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

A ICD 203 versa sobre os padrões de análise que devem ser seguidos por todas as disciplinas do sistema de inteligência norte-americano. O documento estabelece cinco Padrões Analíticos (*Analytic Standards* – AS): Objetividade, Independência de Considerações Políticas, Oportunidade, Base em todas as fontes disponíveis de Inteligência e Implementação evidente dos nove Padrões para a Prática de Análise (*Analytic Tradecraft Standards* – ATS) (EUA 2023, 4-6):

> 1. Descrever apropriadamente a qualidade e a credibilidade das fontes, dados e metodologias aplicadas;
>
> 2. Expressar e explicar adequadamente as incertezas associadas com os principais raciocínios analíticos;
>
> 3. Distinguir apropriadamente a diferença entre informação baseada em Inteligência e julgamentos ou deduções do analista;
>
> 4. Incorporar a análise de alternativas;
>
> 5. Demonstrar a relevância para o usuário e considerar as implicações;
>
> 6. Usar argumentação clara e lógica;
>
> 7. Explicar se houve uma mudança de posição em relação a conhecimentos anteriormente produzidos;
>
> 8. Fazer avaliações e julgamentos precisos; e
>
> 9. Incorporar informação visual, quando apropriado.

McMahon (2024, 4-6) analisa quais seriam as condições para uma adesão aos ATS 3 e 4. No que diz respeito à ATS 3 (Distinguir informação de dedução), uma ferramenta de IA generativa, ao ser consultada pelo analista, deveria ser capaz de:

> • Citar a fonte original - para que o analista pudesse verificar e replicar os achados da ferramenta;
>
> • Atestar a fidelidade ao texto original - usando aspas ou outro recurso para diferenciar citações literais de paráfrases;
>
> • Ater-se aos fatos - evitando, a não ser que solicitada, a apresentação de deduções a partir dos fatos existentes;
>
> • Apresentar contexto para as indicações - caso solicitado, apresentar indicações, porém destacando claramente o que é fato e o que é dedução;
>
> • Manter a consistência caso a situação evolua - caso o surgimento de novos dados modifique a resposta, a causa da mudança deve ser rastreável;
>
> • Apresentar o resultado em um formato pré-estabelecido - nos mesmos modelos estabelecidos para a confecção dos diversos tipos de documento de Inteligência;
>
> • Fazer sentido: o julgamento feito pela ferramenta deve ser plausível e apoiado em bases sólidas.

Ao analisar a ATS 4 (Incorporar alternativas), o autor sugere que, sendo de-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

mandada a apresentar diferentes hipóteses para determinado fenômeno, a ferramenta de IA deve ser capaz de apresentar apenas alternativas factíveis, mantendo-se fiel aos padrões anteriormente citados para a ATS 3. Nesse caso, a ferramenta deve, ainda, explicar os pontos fortes e fracos de cada alternativa (McMahon 2024, 11).

Nesse ponto, destaca-se a importância de "fazer a pergunta certa". Os sistemas de IA generativa são projetados para gerar saídas específicas com base na qualidade das perguntas ("prompts") apresentadas. A engenharia de prompts ajuda os modelos a conhecerem e a responder melhor a uma ampla gama de consultas, das mais simples às mais técnicas (IBM 2023). Para a Inteligência, analistas que formulam bons prompts obtém os melhores resultados.

A partir daí, em que pese o elevado potencial do uso de tecnologia no apoio à análise de Inteligência, o ser humano na função de analista continua a ser responsável por suas análises, e responsabilizável perante o tomador de decisão (McMahon 2024, 9).

Dessa forma, pode-se concluir que a aplicação da IA para a Inteligência é factível, permite a aplicação da TAD e tem a OSINT como campo inicial para o aprendizado de valiosas lições. No entanto, seu emprego sem bases sólidas, ao invés de reforçar, irá comprometer o trabalho da Inteligência.

Processos definidos e dados de qualidade são fundamentais para que os algoritmos sejam desenvolvidos e treinados. As técnicas e procedimentos, em especial no campo da engenharia de prompts e ciência de dados, têm potencial para aplicação nas demais disciplinas, particularmente na CYBINT. Por fim, os aspectos éticos e técnicos da aplicação da IA na Inteligência devem ser aprofundados e incorporados à regulamentação da atividade e à MPC.

Aplicação da TAD para a Fonte Cibernética

O objetivo da TAD é a determinação do grau de credibilidade do dado. A DAI apresenta os procedimentos gerais para a sua realização e, em uma das poucas fontes encontradas que aprofunda o tema, Calaça (2023, 155) apresenta um detalhamento dos questionamentos a serem feitos, a fim de proporcionar mais orientações para o analista que a realiza. Porém, a própria autora reconhece que a técnica, originalmente para fontes humanas e, posteriormente, estendida para fontes tecnológicas, depende fortemente da capacidade do analista que a executa (Calaça 2023, 156).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Cabe destacar que a realização da TAD sobre os dados obtidos, a partir de qualquer tipo de fonte, é condição necessária para os trabalhos da MPC. Se um dado não pode ser avaliado de forma estruturada, não possui credibilidade e, dessa forma, não pode ser utilizado para produzir conhecimentos de Inteligência, o que o torna, em última análise, inútil. Em síntese: sem uma TAD para a Fonte Cibernética, não há CYBINT.

Nesse ponto, há distinção importante a fazer: nas situações em que o dado desejado está indisponível, seu detentor deixa de ser uma Fonte e passa a se enquadrar no conceito de Alvo (Brasil 2023b, 146). No entanto, a sua capacidade de originar o dado desejado necessita ser avaliada, durante o processo de seleção dos objetivos da ação cibernética. Ou seja, para a CYBINT, a determinação do valor do alvo cibernético segue uma lógica semelhante ao processo de avaliação da fonte cibernética.

Dessa forma, a definição de uma TAD Cibernética é condição fundamental para o prosseguimento da elaboração doutrinária, necessária para o funcionamento do sistema de Inteligência, em geral, e à especialização de seus recursos humanos, em particular.

Dentro da TAD, o primeiro aspecto a ser tratado é o da avaliação da idoneidade da fonte. Sobre esse aspecto, os aspectos fundamentais a serem avaliados, que determinarão o grau a ser atribuído, são: autenticidade, confiança e competência (Brasil 2023b, 112). A DAI assim define os aspectos a serem avaliados:

> • Autenticidade: avaliar quem produziu, expediu, modificou ou destruiu um determinado conhecimento, informação ou dado sensível (Brasil 2023b, 148). O analista deve identificar se a fonte, de fato, produziu ou obteve o dado (Calaça 2023, 156).
>
> • Confiança: evidenciada pela precisão dos dados obtidos ou fornecidos pela fonte, ao longo do tempo (Calaça 2023, 155).
>
> • Competência: a capacidade pessoal e a localização da fonte.

Embora a busca da redução da subjetividade seja desejável, não é prático nem possível tentar esgotar todas as possibilidades para a Fonte Cibernética. Dessa forma, um primeiro passo seria a padronização de um número de alternativas para cada critério apresentado, a serem avaliados pelo Analista de CYBINT, e integrados de forma a produzir uma classificação geral que, embora ainda subjetiva, apresenta uma metodologia que pode ser ensinada nas escolas e replicada pelos órgãos integrantes do sistema de Inteligência. A seguir, será apresentada uma proposta para essa padronização inicial, semelhante ao

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

que já existe para a HUMINT.

Para a CYBINT, podem ser identificadas duas situações particulares no que diz respeito à avaliação da idoneidade: Fontes Próprias (operadores ou sistemas) e Fontes Externas (indivíduos, sistemas, fontes abertas especializadas etc). Em ambas as situações, quando a fonte for uma pessoa, sua avaliação aproveita os tradicionais conceitos da HUMINT. Nos casos em que a fonte compreender também sistemas de informação, devem ser consideradas suas características técnicas, sintetizadas em uma avaliação de sua qualidade geral para produzir o dado em questão.

Pode-se destacar, no caso da CYBINT:

> • Autenticidade: no caso de fontes próprias, quando o operador ou sistema estiver sendo empregado em situação sob controle ou supervisão do órgão de Inteligência, a autenticidade pode ser considerada como automaticamente configurada. No caso de fontes externas, caso sejam julgadas não autênticas, sua idoneidade não pode ser avaliada.
>
> • Confiança: também avaliada em função da precisão dos resultados obtidos ao longo do tempo.
>
> • Competência: em função da qualidade do sistema (capacidade/atualização dos equipamentos, ferramentas e sistemas utilizados), da capacidade individual (dada pela capacitação técnica/experiência/talento dos operadores) e da localização da fonte (acesso ao alvo).

A qualidade do sistema e a capacidade individual são combinadas no conceito geral de Capacidade da Fonte Cibernética, que pode assumir três valores (Quadro 2):

> Sim: quando sistemas de qualidade são empregados por indivíduos ou equipes capazes;
>
> Parcial: quando falta a qualidade do sistema ou a capacidade individual; e
>
> Não: quando faltam a qualidade e a capacidade.

Quadro 2
Avaliação da Capacidade da Fonte Cibernética

Capacidade	Qualidade do Sistema	Capacidade Individual
Sim	Sim	Sim
Parcial	Sim	Não
	Não	Sim
Não	Não	Não

Fonte: elaborado pelo autor.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Após definida a Capacidade da fonte, deverá ser avaliada sua Localização. É determinado se a fonte tem ou não tem acesso ao alvo, sem gradações admitidas. Dessa forma, a combinação dessas duas variáveis é o que define a situação no quesito da competência que, em conjunto com a autenticidade e confiança, permite a determinação da Idoneidade da Fonte. Aproveitando o código alfabético apresentado por Calaça (2023, 157), temos o Quadro 3.

Quadro 3
Avaliação da Idoneidade de Fontes Cibernéticas

Letra	Grau de Idoneidade	Autenticidade	Confiança	Competência	
			Precisão	Capacidade	Localização
A	Inteiramente Idônea	Sim	Sempre	Sim	Sim
B	Normalmente Idônea	Sim	Sempre	Parcial	Sim
			Maioria	Sim	Sim
C	Regularmente Idônea	Sim	Maioria	Parcial	Sim
			Metade	Sim	Sim
D	Normalmente Inidônea	Sim	Minoria	Parcial	Sim
E	Inidônea	Sim	Minoria	Parcial	Não
F	Não avaliada	Fonte sem autenticidade ou operador/sist. não empregado			

Fonte: elaborado pelo autor.

Em seguida, os fatores básicos para o julgamento do Conteúdo são: Semelhança Externa, Coerência Interna e Compatibilidade (Brasil 2023b, 112). Enquanto a Semelhança pode ser avaliada apenas com a comparação do dado com os já existentes, a Coerência (evidenciada pela ausência de contradições internas do dado) e a Compatibilidade (manifestada pela harmonização do dado com o que já se conhece a respeito do assunto) vão demandar também o emprego de Analistas com domínio funcional do ambiente cibernético.

De forma prática, o julgamento do conteúdo pode ser feito por meio de perguntas simples, feitas pelo Analista de CYBINT:

> Há semelhança com outros dados? Respostas possíveis: sim ou não.
>
> O dado tem coerência interna? Respostas possíveis: sim ou não.
>
> É compatível com o que se sabe? Respostas possíveis: sim, muito, pouco ou não.

Assim como para a idoneidade da fonte, aproveita-se o código numérico apresentado por Calaça (2023, 157) e, após a combinação das repostas, chega-se ao grau de veracidade do conteúdo (Quadro 4).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Quadro 4
Avaliação da Veracidade do Conteúdo

Número	Grau de Veracidade	Conteúdo do Dado		
		Semelhança	**Coerência**	**Compatibilidade**
1	Confirmado por outras fontes	Sim	Sim	Sim
2	Provavelmente verdadeiro	Não	Sim	Sim
3	Possivelmente verdadeiro	Não	Sim	Muito
4	Duvidoso	Não	Sim	Pouco
5	Improvável	Não	Sim	Não
6	Não atribuída	Não apresentou características que permitam avaliar os três parâmetros		

Fonte: elaborado pelo autor.

No entanto, cabe destacar que pode ser obtida uma variedade enorme de dados a partir do EC, tais como conteúdo de bancos de dados, teor das conversas, organização das redes de interesse, tráfego de dados entre os diversos nós das redes, características dos equipamentos e sistemas empregados, medidas de proteção utilizadas e assim por diante.

Tal variedade, que evolui em alta velocidade, representa um desafio para a Inteligência, pois tem como consequência a obtenção de uma enorme quantidade de dados de diversas naturezas que, para serem adequadamente tratados e produzirem conhecimento utilizável, com oportunidade, exigem o emprego de pessoal especializado e que se adote uma metodologia sólida, estabelecida em fundamentos.

Entendendo que as questões da aplicação da TAD sobre produtos de IA ainda merece maior aprofundamento, fora do escopo do presente trabalho, mas a fim de contribuir para a compreensão do que foi apresentado, uma vez que há aspectos originais na abordagem, seguem abaixo exemplos de aplicação sumária da TAD em dados típicos de CYBINT:

> Situação A - ao receber um arquivo, o Analista de Cibernética o submeteu ao seu antivírus instalado e, após receber o resultado negativo, realizou uma verificação adicional no site https://www.virustotal.com/gui/home/upload, onde foi feita uma análise gratuita de presença de malware, comparando as assinaturas encontradas no arquivo com informações do banco de dados do portal. Nesse caso a fonte é o Virustotal e o dado é o resultado da análise.
>
> Situação B - o monitoramento da Dark Web identificou uma mensagem do hacker conhecido como Hell_Knight, que anunciava ter explorado uma

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

vulnerabilidade dos sistemas de controle industrial da Usina Hidrelétrica de Itaipu e informava as condições em que seria realizado o leilão do malware utilizado. O ator é conhecido pela Inteligência, por já ter reivindicado ataques de defacement contra órgãos públicos e colocado à venda arquivos com credenciais de acesso que se revelaram antigas. A fonte é o hacker em questão e o dado é a existência de um exploit capaz de afetar um sistema crítico.

Situação C - um operador de CYBINT, acompanhando a ferramenta de Segurança Cibernética que monitora a honeynet (CERT-BR s.d.), estabelecida pelo seu órgão, identificou sutis alterações no padrão do tráfego da rede, reportando ao Analista que havia indícios da realização de um reconhecimento (primeiro passo da Cyber Kill Chain) por parte de uma ameaça. O operador é capacitado, porém inexperiente e em fase de treinamento com novas ferramentas. Por fim, a fonte é o operador e o dado é o conteúdo de seu relatório.

Os quadros abaixos apresentam, sinteticamente, os passos e o resultado da TAD realizada pelo Analista de CYBINT (Quadros 5, 6 e 7).

Quadro 5
Estudo de Caso de TAD para CYBINT - Integridade

Situação	Integridade				
	Autenticidade	Confiança	Competência		Avaliação
		Precisão	Capacidade	Localização	
A	Sim	Maioria	Sim	Sim	B
B	Sim	Minoria	Não	Não	E
C	Sim	Maioria	Parcial	Sim	C

Fonte: elaborado pelo autor.

Quadro 6
Estudo de Caso de TAD para CYBINT - Veracidade

Situação	Veracidade			
	Semelhança	Coerência	Compatibilidade	Avaliação
A	Sim	Sim	Sim	1
B	Não	Não	Não	6
C	Não	Sim	Sim	3

Fonte: elaborado pelo autor.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Quadro 7
Estudo de Caso de TAD para CYBINT - Síntese

Situação	Integridade	Veracidade	Síntese
	Avaliação	Avaliação	
A	B	1	B1
B	E	6	E6
C	C	3	C3

Fonte: elaborado pelo autor.

MPC para a Fonte Cibernética

O funcionamento do ramo Inteligência pode ser esquematizado em um ciclo composto por cinco fases, caracterizadas por ações: Objetivar, Acompanhar, Informar, Decidir e Agir. As três primeiras fases são realizadas pelos organismos de Inteligência (Brasil 2023b, 55), não havendo especificidades para a CYBINT.

Em seu Capítulo 5, a DAI aprofunda os conceitos relativos ao Elemento de Análise, abordando conceitos fundamentais que não necessitam de contextualização adicional para sua aplicação direta na Inteligência Cibernética:

> As formas racionais de conhecer: ideia, juízo e raciocínio (Brasil 2023b, 93);
>
> Os estados da mente perante a representação da verdade: ignorância, possibilidade, probabilidade e certeza (Brasil 2023b, 96);
>
> Os insumos para a análise: dado, informação e conhecimento (Brasil 2023b, 99); e
>
> Os tipos de conhecimento de Inteligência: informe, apreciação e estimativa (Brasil 2023b, 103).

Dentro do Sistema Brasileiro de Inteligência (SISBIN), organizado pelo Decreto nº 11.693, diversos elementos têm a possibilidade e a responsabilidade de atuar no espaço cibernético, devendo ser capazes de produzir conhecimentos de CYBINT, dentro de suas áreas específicas. É importante destacar que, além dos seus órgãos permanentes, prioritariamente aqueles relacionados com a segurança integrada (Inteligência, Defesa e Segurança Pública) e diplomacia, são previstos órgãos dedicados, como aqueles que possuem unidades de Inteligência, ou atividades similares, e atuem em assuntos estratégicos relacionados à Política Nacional de Inteligência (PNI) (Brasil 2023c).

Considerando que a PNI destaca, entre as principais ameaças, a ocorrência de ataques cibernéticos (Brasil 2023c, item 6-5), conclui-se que outros ór-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

gãos intensivos em tecnologia na administração pública (tais como o Serviço Federal de Processamento de Dados - SERPRO, a Secretaria de Governo Digital - SGD, entre outros) devem ser organizados para atuar como órgãos dedicados, pois têm importante contribuição a fazer para produção do conhecimento de CYBINT.

Tais conhecimentos, evidentemente, serão de interesse tanto do Ramo Inteligência quanto do Ramo Contrainteligência (Brasil 2023b, 53; 74), podendo ser produzidos com a participação de um Elemento de Operações (Brasil 2023b, 132). Para o Analista de CYBINT, esses órgãos dedicados, capazes de obter dados no espaço cibernético, são mais um meio passível de ser acionado por meio de Pedidos de Inteligência (PI) ou qualquer outro documento padronizado.

Assim como já visto para a TAD, as diversas fases da MPC são seguidas sem maiores dificuldades pelo Analista de CYBINT, com as peculiaridades abaixo.

1. Na fase de Planejamento

   Para essa etapa, é importante destacar que a Inteligência não concorre com a Segurança Cibernética. Assim sendo, o foco da CYBINT é claro: apoiar a tomada de decisão e a ação dos entes do estado face às ameaças, oportunidades e atores operando no EC.

   Dessa forma, não é um uso apropriado do tempo do Analista a produção de conhecimentos que se assemelhem a cartilhas, informativos, resenhas ou similares, frequentemente utilizados pela Segurança Cibernética para desenvolver a mentalidade de proteção nos usuários de sistemas de informação.

2. Na fase da Reunião

   A coleta de dados poderá utilizar uma gama variada de técnicas e ferramentas específicas do ambiente cibernético para obter, de forma rápida, sistematizada e objetiva, apenas os dados de interesse para o atendimento dos aspectos essenciais a conhecer.

   Grande quantidade de dados e informações úteis são oriundos de relatórios e publicações em fontes abertas, elaboradas por organizações de Segurança/Defesa Cibernética.

   O uso de ferramentas de IA generativa pode ser particularmente útil nessa fase, considerando os aspectos já apontados.

   Nas ações de busca deverão ser empregados procedimentos específicos para ambiente cibernético, aliadas ou não às técnicas operacionais já existentes. Anonimização, emprego de avatares, monitoramento de conteúdo na deepweb são, dentre outros, tópicos de convergência entre operadores de CYBINT e profissionais de Segurança Cibernética que atuam na defesa proativa dos ativos de interesse.

3. Na fase de Avaliação

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Os dados obtidos por busca ou coleta deverão ser submetidos à TAD, com as particularidades já apontadas para a Fonte Cibernética.

A adaptação das técnicas de Segurança Cibernética é útil para desenvolver procedimentos e técnicas específicas para a Fonte Cibernética. Ferramentas de análise de rede e de incidentes, por exemplo, produzem relatórios e gráficos que podem auxiliar o Analista em seus julgamentos.

4. Na fase de Integração e Interpretação

É quando o Analista de IC deve chegar às suas conclusões, que são a parte do conhecimento que tem efetiva relevância para os tomadores de decisão.

Durante a etapa de Integração, o analista formulará Juízos que poderão ensejar a produção de diversos Informes, em função dos diferentes graus de credibilidade atribuídos às frações obtidas.

Esse conhecimento deve ser visto como um "bloco" básico de informação que mereça ser registrado para uso futuro, no prosseguimento do ciclo de análise. Resultado de um processo simples, não é comum que um informe seja apresentado a uma autoridade para apoio à tomada de decisão.

A grande quantidade de dados associados ao espaço cibernético provavelmente irá demandar algum tipo de síntese ou agregação. Por exemplo: considerando que diariamente as redes dos órgãos do Estado recebem milhares de tentativas de invasão, feitas automaticamente a partir de todo o mundo, cada tentativa isolada não tem significado particular. No entanto, a totalização do número de tentativas, associada à sua autoria e local de origem, acompanhada ao longo do tempo, pode apresentar dados de interesse para a Inteligência, justificando a produção de informes.

Na etapa da Interpretação, o Analista irá elaborar Raciocínios para concluir sobre o significado dos dados obtidos e sobre os conhecimentos produzidos. Em função da situação, serão elaboradas Apreciações, expressando a opinião ou certeza do Analista sobre fatos passados, presentes ou seus desdobramentos no futuro imediato, ou Estimativas, projetando as opiniões para cenários futuros.

Como exemplos de Apreciações de CYBINT podem ser citadas análises sobre comportamentos de ameaças cibernéticas durante períodos determinados, avaliações do poder cibernético de atores estatais ou não estatais, resultados de análises de resiliência de sistemas próprios, dentre outros. Embora tais conhecimentos possam se valer de produtos de Segurança e Defesa Cibernética como insumos (tais como análises, relatórios, etc), deles se diferenciam não só por empregarem a Linguagem de Inteligência, mas por terem objetivos específicos, levantados durante a fase de planejamento da MPC.

As Estimativas de CYBINT, por sua vez, buscam identificar as principais forças presentes no cenário cibernético e antecipar seus comportamentos no futuro, na forma de cenários. Da mesma forma que nas Apreciações, existe ampla disponibilidade de trabalhos acadêmicos e profissionais sobre o futuro da Cibernética, que podem subsidiar o trabalho do Analista.

Destaca-se a importância das Estimativas de CYBINT para a atividade crucial de alerta estratégico para os mais altos níveis de decisão. As temáticas da ciberspionagem, invasão de sistemas, extração de dados, ataques a infraestruturas críticas, operações de informação e atuação do cibercrime são todas atuais, relevantes e frequentemente motivado-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

ras de crises. Todas elas são adequadas para a produção de cenários e elaboração de indicadores, a cargo da CYBINT (Gentry 2022, 739-744).

Para elaborar tais raciocínios, o Analista deverá se valer das Técnicas de Apoio à Análise constantes da doutrina (Brasil 2023b, 116), enriquecidas pelos recursos, ferramentas e processos da Segurança Cibernética, como já mencionado.

Considerando que a produção de conhecimento é mais eficiente quando feita em grupos multidisciplinares, é altamente vantajosa a organização de equipes compostas por especialistas em Inteligência, que dominem a MPC e as TAE, e técnicos em cibernética, preferencialmente incluindo aqueles com perfil ofensivo - hacking ético (IBM 2023b). O SISBIN, pela variedade de seus integrantes, está em posição única para organizar esse tipo de grupo, pois conta com todas as capacidades em seus diferentes órgãos.

5. Na fase de Formalização e Validação:

   Não há diferenças nessa fase da CYBINT em relação às demais disciplinas, devendo ser seguida a padronização adotada pelos órgãos do SISBIN para a formalização dos documentos. No entanto, é importante destacar que a Linguagem de Inteligência (Brasil 2023b, 123) é fundamental para a correta compreensão do conhecimento, por seus usuários.

   Considerando que o linguajar especializado dos profissionais de cibernética não é de amplo conhecimento, além de ser carregado de imagens e termos técnicos, o analista de CYBINT deve dar objetividade e simplicidade para o produto final, apresentando a informação de acordo com o perfil do usuário e está sendo apoiado.

6. Na fase de Difusão e Resultados, não há diferenças para a CYBINT.

Por fim, destaca-se que, tendo sido evidenciada a aderência da Inteligência Cibernética à MPC, incluídas as suas peculiaridades, é necessária a formalização e a padronização de seus fundamentos que, a partir de então, podem e devem ser objeto de especialização dos recursos humanos do SISBIN. Dessa forma, o papel dos estabelecimentos de ensino de Inteligência é fundamental, como polo irradiador desse conhecimento para todo o sistema.

Conclusão

As ideias expostas não têm o objetivo de esgotar o assunto, mas esperam contribuir para o debate, ainda incipiente, sobre a necessária convergência de esforços para a sistematização da produção do conhecimento pela Inteligência Cibernética, nova e importante disciplina da atividade.

Cabe destacar que a adequação da metodologia para as peculiaridades da Fonte Cibernética, embora não seja suficiente, é condição necessária para a Produção do Conhecimento. Além disso, é absolutamente essencial na construção do arcabouço doutrinário para a atuação dos diversos atores

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

estatais atuantes no ambiente cibernético, com evidentes reflexos para a especialização dos recursos humanos empregados.

Como foi dito, os aspectos de Inteligência são apenas uma parcela do amplo e complexo ecossistema do Espaço Cibernético. No entanto, a experiência mostra que essa parte é fundamental para que o SISBIN cumpra sua missão de contribuir para a proteção dos interesses do Brasil. A visão da Inteligência, que combina a produção do conhecimento com a proteção dos ativos de informação, é especialmente capaz de produzir uma metodologia integrada e objetiva para a CYBINT. Os fundamentos técnicos da Segurança Cibernética, por sua vez, representam uma valiosa fonte de dados e a oportunidade para aprendizado de lições.

Por fim, para que a Inteligência não desperdice a oportunidade representada pelo rápido desenvolvimento das aplicações de IA, é fundamental que a MPC seja aprofundada para contemplar as peculiaridades das fontes tecnológicas, em especial da CYBINT, definindo seus processos e desenvolvendo a capacidade de trabalhar com a enorme massa de dados, de diversas naturezas.

Dessa forma, a maturidade do SISBIN e de sua MPC, aliados à qualidade dos estabelecimentos de ensino do sistema, são importantes instrumentos para a organização e a integração dessa nova e importante área de atuação do Estado brasileiro.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

Referências

Armed Forces Communications & Electronics Association International. 2022. "U.S. Cyber Command Means To Magnify Cyber Intelligence". The Cyber Edge Newsletter. Acessado em 24 de março de 2025. https://www.afcea.org/signal-media/cyber-edge/us-cyber-command-means-magnify-cyber-intelligence.

Biondi, Fabio, Giuseppe Buonocore e Richard Matthews. 2021. "Generative Adversarial Networks from a Cyber Intelligence perspective".

Brasil. 2015. EB20-MF-10.107 - Inteligência Militar Terrestre (2ª Ed). Exército Brasileiro. https://bdex.eb.mil.br/jspui/bitstream/123456789/95/1/EB20-MF-10.107.pdf.

Brasil. 2016. Decreto Nº 8.793, de 29 de junho de 2016 – Fixa a Política Nacional de Inteligência. Secretaria Geral. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

Brasil. 2020. Estratégia Nacional de Segurança Cibernética. Secretaria Geral da Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

Brasil. 2023a. Política Nacional de Cibersegurança. Casa Civil. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

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

Brasil. 2023c. Decreto Nº 11.693, de 6 de setembro de 2023 - Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. Casa Civil. https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm.

Brasil. 2023d. MD31-M-07 - Doutrina Militar de Defesa Cibernética. Ministério da Defesa. https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf.

Brasil. 2024. Fundamentos do Poder Nacional. Escola Superior de Guerra. https://www.gov.br/esg/pt-br/centrais-de-conteudo/publicacoes/fundamentos-do-poder-nacional/fundamentos-do-poder-nacional-rev-2024-mac2-1.pdf.

Calaça, Irene. 2023. "Técnica de Avaliação de Dados (TAD) e Fonte em Inteligência". *Revista Brasileira de Inteligência* 18: 149-165. https://doi.org/10.58960/rbi.2023.18.232.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Rede no Brasil). s.d. "Honeypots e Honeynets: Definições e Aplicações". Acessado a 28 de junho de 2025. https://www.cert.br/docs/whitepapers/honeypots-honeynets/.

EUA (Estados Unidos da América). 2018. A Common Cyber Threat Framework: A Foundation for Communication. Escritório do Diretor Nacional de Inteligência. Acessado a 25 de setembro de 2025. https://info.publicintelligence.net/ODNI-CyberThreatFramework.pdf.

EUA (Estados Unidos da América). 2023. Intelligence Community Directive 203, Analytic Standards. Escritório do Diretor Nacional de Inteligência. Acessado a 28 de junho de 2025. https://www.dni.gov/files/documents/ICD/ICD-203.pdf.

FAS (Federation of American Scientists. 2015. "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)". Acessado em 27 de março de 2025. https://fas.org/publication/osc-ose/.

Gentry, John A. 2022. "Cyber Intelligence: Strategic Warning Is Possible," *International Journal of Intelligence and CounterIntelligence* 36 (3): 729–754. https://doi.org/10.1080/08850607.2022.2095544.

Goldfarb, Avi e Jon R. Lindsay. 2021. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security* 46 (3): 7–50. https://doi.org/10.1162/isec_a_00425.

IBM. 2021. "O que é um chatbot?". Acessado em 27 de março de 2025. https://www.ibm.com/br-pt/topics/chatbots.

IBM. 2022. "O que é Inteligência de Ameaças?". Acessado em 27 de março de 2025. https://www.ibm.com/br-pt/topics/threat-intelligence.

IBM. 2023. "O que é Engenharia de Prompt?". Acessado em 27 de março de 2025. https://www.ibm.com/br-pt/think/topics/prompt-engineering.

IBM. 2023b. "O que é hacking ético?". Acessado em 28 de março de 2025. https://www.ibm.com/br-pt/topics/ethical-hacking.

IBM. 2024a. "Types of cyberthreats". Acessado em 27 de março de 2025. https://www.ibm.com/think/topics/cyberthreats-types.

IBM. 2024b. "O que são ameaças persistentes avançadas?". Acessado em 31 de março de 2025. https://www.ibm.com/br-pt/topics/advanced--persistent-threats.

Lockheed Martin. s.d. "The Cyber Kill Chain". Acessado em 25 de março de 2025. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.273
ISSN 2595-4717

McMahon, Gerald. 2024. "Analytic Tradecraft Standards in an Age of AI". https://www.belfercenter.org/research-analysis/analytic-tradecraft--standards-age-ai.

Mitre Corporation. s.d. Acessado a 27 de junho de 2025. https://attack.mitre.org/.

UNESCO (United Nations Educational, Scientific and Cultural Organization). s.d. "Ética da IA e integridade da informação". Acessado em 27 de março de 2025. https://www.unesco.org/pt/g20/digital-economy.