Produção do conhecimento de Inteligência Cibernética:
padronizar para integrar

Data de submissão: 2 de abril de 2025 **Data de aprovação**: 7 de maio de 2025

Jomar Barros de Andrade*
Guilherme Otávio Godinho de Carvalho**

Resumo Executivo

O espaço cibernético é fonte valiosa de dados para a Inteligência. No entanto, suas características dificultam o emprego da Metodologia da Produção do Conhecimento, desenvolvida originalmente para as fontes humanas. Dessa forma, a falta de uma metodologia para a Inteligência Cibernética prejudica a obtenção de resultados e a integração sistêmica. Em que pese o papel da Agência Brasileira de Inteligência, como Órgão Central do SISBIN, o Ministério da Defesa tem papel fundamental no aprofundamento dessa temática, por sua presença em todos os níveis de decisão, pela maturidade de seu sistema de Inteligência e pela capacidade das Forças Singulares. Do exposto, o presente *policy paper* pretende discutir os desafios relacionados à gestão do tema, apresentando recomendações para o desenvolvimento de fundamentos que permitam à Defesa um melhor suporte de Inteligência às suas operações para, posteriormente, ficar em condições de bem assessorar os trabalhos sobre o tema no âmbito do SISBIN. As escolas de Inteligência e os Comandos Operacionais de Cibernética possuem um papel fundamental nesse processo, que se desenvolve em ciclos e se materializa no Plano de Inteligência de Defesa.

Palavras-chave: inteligência; cibernética; metodologia; integração; padronização.

* 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). Atualmente é o Gerente do Programa Estratégico do Exército Defesa Cibernética.

**Coronel da Reserva do Exército Brasileiro. Doutorando e mestre em Relações Internacionais (UnB) e mestre em Ciências Militares (ECEME). Especialista em Inteligência Militar (EsIMEx). Atualmente professor da Escola Superior de Defesa.

1 ANÁLISE DO PROBLEMA E SUAS IMPLICAÇÕES PARA DEFESA

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. A conectividade em tempo integral e a disponibilidade imediata de conteúdo tornaram-se aspectos fundamentais da vida de grande parcela da sociedade.

A Inteligência de Estado e seus profissionais são desafiados por essa conjuntura. Nesse contexto, os diplomas fundamentais da atividade destacam a importância da cibernética, como segue:

- a Política Nacional de Inteligência (PNI), em sua Diretriz 8.4 (Expandir a capacidade operacional da Inteligência no espaço cibernético), estabelece que "o comprometimento da capacidade operacional do Estado e de sistemas computacionais essenciais ao provimento das necessidades básicas da sociedade deve ser preocupação permanente, exigindo constante aperfeiçoamento técnico dos entes públicos responsáveis pela integridade desses sistemas" (Brasil, 2016);

- a Estratégia Nacional de Inteligência (ENI) aborda o tema sob diversos aspectos. Ataques Cibernéticos são elencados dentre as ameaças presentes no ambiente estratégico (Brasil, 2017, p. 17), ao mesmo tempo que o desenvolvimento da Inteligência Cibernética, tanto nas atitudes defensivas quanto proativas, é uma oportunidade para a consecução dos objetivos nacionais (Brasil, 2017, p. 20), a maior utilização de tecnologia de ponta, especialmente no campo cibernético, é reconhecida como um desafio (Brasil, 2017, p. 22). Em consequência, estabelece dois objetivos estratégicos relacionados com a temática: "Ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência Cibernética" e "Promover a qualificação técnica para proteção e exploração do campo cibernético" (Brasil, 2017, p. 26 - 27); e

- a Doutrina da Atividade de Inteligência (DAI) apresenta o conceito de Inteligência Cibernética (*Cyber Intelligence* – CYBINT[1]) como aquela voltada a temas relativos ao espaço cibernético (EC)[2], cuja produção busca apoiar a atuação do Brasil frente a vulnerabilidades e

[1] A DAI não apresenta uma abreviatura para Inteligência Cibernética. Dessa forma, será utilizada a constante na publicação EB20-MF-10.107 - Inteligência Militar Terrestre (2ª Ed). Brasília, DF: EB, 2015.

[2] Para a DAI, o espaço cibernético é entendido como o conjunto das infraestruturas informáticas e telemáticas interconectadas que compreende hardware e software, dados e usuários, e quaisquer relações lógicas entre eles. A Doutrina Militar de Defesa Cibernética apresenta definição semelhante, dividindo o espaço cibernético em três camadas: física (dispositivos e infraestrutura de TIC), lógica (aplicações, serviços, protocolos etc) e ciberpersona (identidades virtuais dos usuários).

ameaças, informar políticas públicas e planos estatais nesse domínio, bem como acompanhar e avaliar capacidades, intenções e atividades de atores externos naquele espaço (Brasil, 2023, p. 159). A doutrina discorre amplamente sobre a Metodologia da Produção do Conhecimento (MPC) que, em síntese, é composta de seis fases: planejamento; reunião; avaliação; integração e interpretação; formalização e validação; difusão e resultados. Embora as fases da MPC sejam apresentadas em sequência cronológica, na prática elas não implicam procedimentos rigorosamente ordenados e não têm limites precisos. São fases que se interpenetram, inter-relacionam e interdependem. Tais procedimentos podem ocorrer em sequência, em paralelo ou de forma sobreposta, a depender de fatores como a composição e a organização da equipe, os prazos e as circunstâncias de produção (Brasil, 2023a, *passim*).

No entanto, ao mesmo tempo que reconhece sua importância para a padronização e a integração, no âmbito do Sistema Brasileiro de Inteligência (SISBIN), a DAI não aprofunda as orientações específicas para a sua aplicação pela CYBINT.

O Sistema de Inteligência de Defesa (SINDE), por sua vez, internaliza e desenvolve esses conceitos em seus documentos de mais alto nível, como segue:

- a Política de Inteligência de Defesa (PID), em sua análise do Ambiente Internacional e Nacional, reconhece a importância do domínio no campo cibernético para impedir a ação adversa e difundir a mentalidade de proteção em todos os setores (Brasil, 2023c, p. 15) e lista os ataques cibernéticos dentre as ameaças levantadas (Brasil, 2023c, p. 17). Em consequência, emite a Diretriz no âmbito do SINDE nº 6.1.9 Expandir a capacidade da Inteligência no espaço cibernético; e

- a Estratégia de Inteligência de Defesa (EID) aponta as entregas do Setor Cibernético de Defesa como uma oportunidade (Brasil, 2023d, p. 15); também elenca a utilização de tecnologia de ponta dentre os desafios e define duas ações estratégicas relacionadas com o tema: a "b) Atualizar a Doutrina de Inteligência de Defesa" e a "e) Promover o aperfeiçoamento dos integrantes do SINDE e a interoperabilidade com órgãos e agências nacionais de Inteligência" (Brasil, 2023d, p. 17).

O desafio enfrentado pela Defesa, em relação ao tema da padronização da MPC para a CYBINT, faz parte de uma questão mais ampla, que não é exclusiva do Brasil, qual seja, a necessidade da adoção de padrões de análise mais rígidos pela Inteligência, aí incluída a de Defesa e, consequentemente, a Militar. A falta desses fundamentos representa óbices e riscos significativos para a atividade de Inteligência, tais como:

- diferenças de interpretação quanto às definições norteadoras da produção do conhecimento entre os diversos integrantes do sistema;

- baixo rigor na avaliação dos insumos para a produção de Inteligência, comprometendo o resultado dos trabalhos de análise;

- desconhecimento ou baixa utilização de melhores práticas para o tratamento de grandes volumes de dados;

- falhas de segurança quando da obtenção de dados no espaço cibernético, dentre outros.

Dessa forma, o problema pode receber o seguinte enunciado: "Aprofundar os fundamentos metodológicos da Inteligência para contemplar as particularidades da atuação no espaço cibernético, a fim de intensificar a produção de conhecimentos a partir desse domínio, aperfeiçoar os recursos humanos do SINDE, apoiar o processo decisório no âmbito da Defesa e fortalecer a integração no âmbito do SISBIN".

A responsabilidade pelo estabelecimento de padrões para o SISBIN recai sobre a Agência Brasileira de Inteligência, órgão central do sistema (Brasil, 2023b, passim), sendo a Defesa e as Forças Singulares (FS) atores fundamentais na temática — tanto por suas condições de órgãos permanentes do sistema quanto pela seleção da Cibernética como um dos Setores Estratégicos para a Defesa.

Sob o tema, são interessantes as lições aprendidas pelos Estados Unidos da América (EUA) que, após as falhas de inteligência sobre a existência de armas de destruição em massa, que acabaram fundamentando a invasão do Iraque, em 2003 (McMahon, 2025, p. 2), desenvolveram um trabalho de correção de processos internos, que culminou na emissão da Diretiva para a Comunidade de Inteligência 203 (*United States, 2015*), do Escritório do Diretor Nacional de Inteligência. O documento estabelece os Padrões de Análise de Inteligência adotados naquele país, devendo ser adotados por todos os órgãos, respeitadas suas peculiaridades.

Porém, essa adoção não é livre de desafios. Schmor e Kwoun (2020) discorrem sobre as dificuldades enfrentadas pelos analistas de Inteligência Militar para apresentar produtos que efetivamente suportem o processo de tomada de decisão (viés cognitivo, falta de padronização, dificuldade de interoperabilidade com outros órgãos do sistema de Inteligência), identificam os benefícios de uma internalização da ICD 203 no âmbito do Exército dos EUA e apontam que as diretivas, no âmbito da Defesa, eram ainda mais rígidas se comparadas às orientações gerais. Por fim, apresentam recomendações que, com a devida contextualização, servem de referência para o enfrentamento de problemas similares (Schmor; Kwoun, 2020, *passim*).

As três dificuldades apontadas acima também existem no âmbito do SISBIN e do SINDE. No entanto, considerando que a MPC em geral, e sua Técnica de Avaliação de Dados (TAD), em particular, foram desenvolvidas para a Inteligência de Fontes Humanas (*Human Intelligence* - HUMINT), a sua aplicação no âmbito da CYBINT representa um desafio ainda mais complexo.

É oportuno destacar que diversos elementos do SISBIN, listados no Decreto Nº 11.693, têm a possibilidade e a responsabilidade de atuar no espaço cibernético, devendo ser capazes de produzir conhecimentos de CYBINT, dentro de suas áreas específicas. Além dos seus órgãos permanentes prioritariamente relacionados com Segurança Integrada (Inteligência, Defesa e Segurança Pública) e diplomacia, são previstos órgãos dedicados, como aqueles que possuem unidades dedicadas à Inteligência, ou atividades similares, e atuem em assuntos estratégicos relacionados à PNI (Brasil, 2023b).

Considerando que, como já dito, a PNI destaca, em seu item 6.5, a ocorrência de ataques cibernéticos dentre as principais ameaças, é evidente que outros órgãos intensivos em tecnologia na administração pública – tais como o Serviço Federal de Processamento de Dados (SERPRO), a Secretaria de Governo Digital (SGD), dentre outros – devem ser organizados para atuar como órgãos dedicados, pois têm importante contribuição a fazer, tanto para a garantia da segurança da Informação, quanto para a produção do conhecimento de Inteligência Cibernética.

De forma semelhante, a análise de seus fundamentos evidencia a existência de pontos em comum entre a Inteligência e a Defesa Cibernética (Brasil, 2023e, p. 17), uma vez que a última tem, dentre suas finalidades, obter dados para a produção de conhecimentos. Porém, ainda que essa convergência indique a vantajosa possibilidade de compartilhamento de procedimentos, ferramentas e técnicas, também as diferenças de escopo, prioridades e horizontes temporais devem ser bem compreendidas, a fim de permitir uma atuação coordenada dos seus respectivos órgãos.

Por isso, não se deve confundir a CYBINT com a Inteligência de Ameaças, denominação essa amplamente consolidada da área da Segurança e Defesa Cibernéticas que levanta e organiza informação detalhada e acionável sobre ameaças cibernéticas (IBM, 2025a), de diversos tipos (*malwares*, *phishing*s, *zero-day exploits* etc) (IBM, 2025b) e atores, em especial as Ameaças Persistentes Avançadas (*Advanced Persistent Threats* – APT) (IBM, 2025c). 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.

Aspecto fundamental do problema é a obtenção dos dados no espaço cibernético. Em síntese, a DAI estabelece que os dados podem ser obtidos por meio de Coleta (ação especializada que visa à obtenção de dados e informações de livre acesso) ou Busca (aplicação combinada de técnicas operacionais para obtenção de dados, informações e conhecimentos indisponíveis) (Brasil, 2023, p. 148 - 149).

Sob o ponto de vista da Inteligência Cibernética, 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. Cabe destacar que, em qualquer circunstância, o acesso a qualquer insumo ou produto do trabalho da Atividade de Inteligência se baseia na necessidade de conhecer (Brasil, 2023, p. 166). Isso posto, na coleta de dados devem ser identificadas e adotadas as medidas de segurança que garantam o sigilo e a discrição inerentes ao trabalho do profissional de Inteligência (Brasil, 2023, p. 29).

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. Dessa forma, a penetração em redes externas, ainda que no contexto de uma defesa proativa e com o objetivo de proteger os sistemas de interesse para o Estado, é um tema sensível que demanda o aprofundamento de sua regulamentação, dentro da temática das ações operacionais.

Tais considerações são especialmente relevantes, pois 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, 2023, p. 160) e a maioria dos utilizados pela Inteligência de Fontes Abertas (*Open Source Intelligence* – OSINT) e 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, a OSINT coleta seus dados nos sistemas operados na camada lógica, enquanto categorias de TECHINT têm como foco os sistemas da camada física. A CYBINT, devido à variedade de seus objetivos, atua nas três camadas de forma coordenada com as demais disciplinas, 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, tanto para a obtenção quanto para a análise.

A Defesa Cibernética representa relevante fonte de lições aprendidas e técnicas, táticas e procedimentos para a CYBINT. A própria Doutrina Militar de Defesa Cibernética, em seu item 5.3 A Capacidade Cibernética em proveito da Inteligência, destaca o compartilhamento de técnicas, táticas e procedimentos, a integração de fontes, a produção do conhecimento por organizações de cibernética e o papel da Exploração Cibernética para o mapeamento do ECI (Brasil, 2023e, p. 39).

Amplamente justificada a necessidade de aprofundamento da MPC para a CYBINT, aproveitando as melhores práticas da Defesa Cibernética e de forma integrada com as demais disciplinas da Inteligência, o passo seguinte é a identificação dos atores mais apropriados para a tarefa e, em seguida, qual a estratégia para sua difusão no âmbito do SISBIN, destacando o papel da Defesa nesse processo.

Entendendo que a questão não pode ser solucionada por um único ente, e consolidado o entendimento das responsabilidades do seu Órgão Central, o caráter sistêmico do SISBIN representa uma excepcional oportunidade para a solução de problemas de interesse comum. Dessa forma, destacando o papel dos estabelecimentos de ensino na formulação doutrinária, naturalmente caberia à Escola de Inteligência (EsInt) da ABIN o papel de relator de um grupo de trabalho estabelecido para aprofundar e padronizar a produção do conhecimento pela CYBINT, o que, necessariamente, envolveria atores de outros ministérios.

Reconhecendo que o espírito do Decreto nº 11.693 é o de reduzir o colegiado do SISBIN, direcionando seu escopo para os especialistas dos diversos órgãos, também participariam do trabalho representantes das áreas de Segurança e Defesa Cibernética, TIC, infraestruturas críticas e outras, conforme análise oportuna. Assim, organizações do Ministério da Defesa (MD), tais como o Comando de Defesa Cibernética (ComDCiber); do Ministério da Gestão e da Inovação em Serviços Públicos, como a Secretaria de Governo Digital; do Gabinete de Segurança Institucional (GSI), em especial o (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov); das Agências Reguladoras, dentre outros, seriam indicações naturais para participar dos trabalhos técnicos.

Dentre esses atores, é possível que existam órgãos que não possuem seus elementos de Inteligência organizados. Dessa forma, além da padronização de procedimentos, os resultados esperados podem incluir indicações sobre quais instituições devem ser órgãos dedicados do SISBIN, especificamente para a atuação em CYBINT.

Considerando as peculiaridades do SISBIN, a importação pura e simples de documentos como a ICD 203 é algo fora de questão. No entanto, a objetividade e a simplicidade daquele documento são características positivas, que devem inspirar os produtos a serem desenvolvidos.

A Defesa, em face do papel desempenhado por seu Setor Cibernético, da maturidade do SINDE, da existência de estabelecimentos de ensino de Inteligência e de comandos conjuntos de cibernética, está em uma posição privilegiada para apoiar e, consequentemente, orientar e se beneficiar desse processo. Cabe destacar que uma das maiores prioridades, tanto para o SINDE quanto para o Sistema Militar de Defesa Cibernética (SMDC), é a proteção de infraestruturas críticas, aspecto fortemente relacionado com tópicos avançados de CYBINT, tais como a atuação das APT e a proteção de sistemas SCADA (*Supervisory Control And Data Acquisition*).

Considerando que a CYBINT já atua fortemente nos níveis operacional e tático, é de interesse da Defesa também a tradução de uma base doutrinária mais profunda para esses segmentos. Dessa forma, a necessária integração entre as operações militares, sejam elas conjuntas, singulares ou interagências, se beneficiaria diretamente da atuação do MD junto ao processo de formulação mencionado.

Destaca-se que o planejamento estratégico, no âmbito do MD, é feito de forma sincronizada nos níveis Defesa (conforme o método previsto no Sistema de Planejamento Estratégico de Defesa – SISPED) (Brasil, 2015) e Militar (seguindo a publicação M51-M-01 - Sistemática de Planejamento Estratégico Militar - SPEM) . Sua execução ocorre em ciclos quadrienais e tem, já na primeira fase da SPEM, a determinação das Prioridades de Defesa (Brasil, 2018, *passim*). Para que sejam efetivas, quaisquer ações relacionadas ao desenvolvimento da CYBINT devem, necessariamente, ter tido sua necessidade levantada durante o planejamento estratégico e suas implementações previstas nos diversos planos de ação, dele decorrentes.

Assim sendo, iniciar proativamente tais estudos no âmbito da Defesa, para posteriormente provocar a discussão do assunto no âmbito do SISBIN, é a forma mais prática de colocar em movimento a discussão desse tema. A capilarização dos achados do grupo de trabalho por todo o sistema, em especial no âmbito dos órgãos não permanentes, é um desafio. No entanto, a existência de cursos de Inteligência Cibernética, no âmbito da Defesa, é um bom ponto de partida para promover a difusão.

A partir dos fundamentos comuns elaborados, as atividades de ensino das diversas escolas de Inteligência devem se adequar às particularidades das atividades de cada órgão. No caso daqueles que não possuem estabelecimentos de ensino, a EsInt, a Escola Superior de Defesa

(ESD) e a Escola Superior de Guerra (ESG) são pontos focais naturais para a realização de cursos específicos.

Por fim, o problema não se encerra nesse primeiro ciclo de trabalho. São indispensáveis a aplicação e a validação das técnicas e procedimentos eventualmente desenvolvidos, tendo em vista a natureza dinâmica da Cibernética e seus impactos na Inteligência. Dessa forma, impõe-se uma sistemática de acompanhamento de lições aprendidas, envolvendo os diversos atores de interesse.

2 RECOMENDAÇÕES

– Inserir o tema da CYBINT na agenda do SISBIN: a conjuntura atual justifica que o tema seja imediatamente incluído no âmbito do SISBIN, a fim de sensibilizar seus integrantes permanentes e provocar o acionamento de órgãos, relacionados com a Cibernética, que devam se tornar dedicados.

– Estabelecer Grupo de Trabalho no âmbito da Defesa para propor uma MPC para a Inteligência Cibernética, contemplando aspectos de obtenção e análise de dados. Tendo em vista sua capacidade de operar em diferentes níveis (estratégico, operacional e tático) e utilizando-se das potencialidades de estruturas consolidadas — como o SINDE, o Comando de Operações Conjuntas de Cibernética e o Sistema de Inteligência estabelecido nas Forças Singulares, com seus respectivos Centros de Inteligência — o Ministério da Defesa possui as melhores condições para desenvolver uma proposta inicial de fundamentos para a CYBINT. Essa proposta poderá, posteriormente, apoiar eventuais trabalhos realizados no âmbito do SISBIN.

– Priorizar a CYBINT no planejamento estratégico no âmbito da Defesa: aumentar e sincronizar a prioridade dada ao tema nos planejamentos estratégicos de defesa e militar, de modo a promover o alinhamento das ações no âmbito do MD e das Forças.

– Revisar os aspectos de Cibernética do Plano de Inteligência de Defesa (PINDE): tendo em vista seu caráter orientador , o aprofundamento dos aspectos relacionados com o espaço cibernético, destacadamente os envolvidos em mais de uma disciplina, potencializará o desenvolvimento da CYBINT.

REFERÊNCIAS

BRASIL. Casa Civil. Agência Brasileira de Inteligência. **Doutrina da Atividade de Inteligência.** Aprovada pela Portaria GAB/DG/ABIN/CC/PR nº 1.205, de 27 de novembro de 2023. Brasília, DF: Abin, 2023a.

BRASIL. Casa Civil. Secretaria Especial para Assuntos Jurídicos. **Decreto nº 11.693, de 6 de setembro de 2023 – Dispõem sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência.** Brasília, DF: SEAJ, 2023b.

BRASIL. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto de 15 de dezembro de 2017 – Aprova a Estratégia Nacional de Inteligência.** Brasília, DF: SAAJ, 2017.

BRASIL. Exército Brasileiro. **EB20-MF-10.107 - Inteligência Militar Terrestre (2ª Ed).** Brasília, DF: EB, 2015.

BRASIL. Ministério da Defesa. **MD60-P-01 – Política de Inteligência de Defesa.** Brasília, DF: MD, 2023c.

BRASIL. Ministério da Defesa. **MD60-E-01 – Estratégia de Inteligência de Defesa.** Brasília, DF: MD, 2023d.

BRASIL. Ministério da Defesa. **MD31-M-07 - Doutrina Militar de Defesa Cibernética.** Brasília, DF: MD, 2023e.

BRASIL. Ministério da Defesa. **Sistema de Planejamento Estratégico de Defesa (SISPED) - Método.** Brasília, DF: MD, 2015.

BRASIL. Ministério da Defesa. **MD51-M-01 – Sistema de Planejamento Estratégico Militar (SPEM).** Brasília, DF: MD, 2018.

BRASIL. Secretaria Geral. Subchefia para Assuntos Jurídicos. **Decreto Nº 8.793, de 29 de junho de 2016 – Fixa a Política Nacional de Inteligência.** Brasília, DF: SAAJ, 2016.

IBM. **O que é Inteligência de Ameaças?.** Disponível em https://www.ibm.com/br-pt/topics/threat-intelligence. Acesso em: 27 mar. 2025a.

IBM. **Types of cyberthreats.** Disponível em https://www.ibm.com/think/topics/cyberthreats-types. Acesso em: 27 mar. 2025b.

IBM. **O que são ameaças persistentes avançadas?.** Disponível em https://www.ibm.com/br-pt/topics/advanced-persistent-threats. Acesso em: 31 mar. 2025c.

McMAHON, Gerald M. **Analytic Tradecraft Standards in an Age of AI**. Disponível em: https://www.belfercenter.org/research-analysis/analytic-tradecraft-standards-age-ai. Acesso em: 24 mar. 2025.

SCHMOR, Robert W. e KWOUN, James S. Normas Técnicas para a Análise de Informações Uma oportunidade de proporcionar aos comandantes no Exército uma vantagem no processo decisório**.** Military Review, 3º Trim, p. 12-25. EUA: The Army University, 2020.

United States. Office of the Director of National Intelligence. **Intelligence Community Directive 203, Analytic Standards**. Washington, DC: 2 jan. 2015.
Disponível em: https://www.dni.gov/files/documents/ICD/ICD-203.pdf. Acesso em: 24 mar. 2025.