Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artigo de investigação

A INTELIGÊNCIA EM FOCO: DA TEORIA CLÁSSICA A UMA NOVA ABORDAGEM DE IMPLEMENTAÇÃO NA ERA DIGITAL

Tradução para o português com ajuda de IA (DeepL)

Paula Castro Castañer
Perito em segurança na Telefónica S.A.
Doutorando em Ciências Forenses na Universidade de Alcalá
Mestrado em Cibersegurança e Privacidade pela Universitat Oberta de Catalunya (UOC)
paula.castroc@edu.uah.es
ORCID: 0009-0008-0315-8387

Recebido a 14/02/2025
Aceite em 16/06/2025
Publicado em 27/06/2025

Citação recomendada: Castro P. (2025). A inteligência em foco: Da teoria clássica a uma nova abordagem de implementação na era digital. *Revista Logos Guardia Civil*, 3(2), p.p. 71-100.

Depósito legal: M-3619-2023
NIPO em linha: 126-23-019-8
ISSN em linha: 2952-394X

ORCID: **0009-0008-0315-8387**

DEDICAÇÃO

Ao meu tutor, Hilário, por ter confiado em mim e me ter apoiado em todos os meus projectos.

ORCID: **0009-0008-0315-8387**

A INTELIGÊNCIA EM FOCO: DA TEORIA CLÁSSICA A UMA NOVA ABORDAGEM DE IMPLEMENTAÇÃO NA ERA DIGITAL

Resumo: Este artigo aborda a evolução da intelligence no domínio da Defesa e Segurança, desde as abordagens tradicionais até à sua adaptação à era digital, estabelecendo uma proposta que responde a algumas das limitações apontadas na literatura sobre o ciclo clássico de intelligence. Para o efeito, são explorados conceitos-chave, como a definição do conceito de intelligence, os diferentes tipos de intelligence e ainda o ciclo tradicional de intelligence e as suas fases. Além disso, é apresentada uma revisão da evolução e das diferentes abordagens que foram adoptadas ao longo da história no domínio da inteligência. Por fim, propõe um modelo de inteligência, denominado IDEM, com fases flexíveis e que combina o talento do analista humano e o processamento automatizado de big data para garantir uma inteligência proactiva, adaptativa e de qualidade face às complexas ciberameaças transnacionais.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Palavras-chave: ciberameaças, ciberinteligência, ciclo de inteligência, modelo IDEM, abordagem em rede

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red **.**

ORCID: **0009-0008-0315-8387**

ABREVIATURAS

ABI: *Inteligência baseada em actividades*

CCN-CERT: Centro Nacional de Criptologia - Equipa *de Resposta a Emergências Informáticas*

CESID: Centro Superior de Informação da Defesa (Centro de Informação da Defesa)

CIA: *Agência Central de Inteligência, Agência* Central *de Inteligência*

CIFAS: Centro de Inteligência das Forças Armadas

CNI: Centro Nacional de Informações

COMINT: *Informações sobre comunicações*

COP*: Policiamento comunitário*, policiamento *orientado para a comunidade*

CTI: *Informação sobre ameaças cibernéticas, Informação sobre* ameaças cibernéticas

CYBINT: Ciberespionagem, Ciberespionagem

ELINT: *Inteligência eletrónica*

FISINT: *Informações de sinais de* instrumentação *estrangeira*

GEOINT: *Inteligência Geoespacial, Inteligência* Geoespacial

HUMINT: *Inteligência Humana*

IDEM: Enhanced Dynamic Intelligence Enrichment and Enhancement (enriquecimento e melhoramento da inteligência dinâmica)

IDS: *Sistema de Deteção de Intrusão,* Sistema de *Deteção de Intrusão*

ILP*: Intelligence-Led Policing, Policiamento liderado por informações*

IMINT: *Inteligência imagiológica*

ISR: *Intelligence Surveillance and Reconnnaissance), Informações,* vigilância e reconhecimento

JISR: *Joint Intelligence Surveillance and Reconnnaissance (Informações,* Vigilância e Reconhecimento Conjuntos*),* Informações, Vigilância e *Reconhecimento* Conjuntos

MASINT: *Inteligência de* Medição e *Assinatura*

ML: *Aprendizagem automática*, Aprendizagem automática

NLP: *Processamento de linguagem natural*

OSCE: *Organização para a Segurança e a Cooperação na Europa*, Organização *para a Segurança e a Cooperação* na Europa

OSINT: *Informações de fonte aberta*

SCADA: *Controlo de Supervisão* e *Aquisição de Dados*

SECED: Serviço Central de Documentação

SIEM: *Gestão de Informações* e *Eventos de Segurança*

SIGINT: *Inteligência* de sinais

SOCMINT: *Inteligência* em matéria de redes sociais, Inteligência em matéria de redes sociais

TCPED: Atribuição, *recolha, processamento, exploração, difusão*, abordagem, recolha, processamento, exploração, *difusão*

TTPs: *Ameaças, Técnicas e Procedimentos*

ORCID: **0009-0008-0315-8387**

1. INTRODUÇÃO

Num mundo em que a Inteligência Artificial parece dominar grande parte das atenções e preocupações públicas, onde é que a inteligência, em todas as suas outras formas, fica em segundo plano? A omnipresença da Inteligência Artificial nos debates contemporâneos ofusca frequentemente a importância de outros tipos de inteligência que são fundamentais para o progresso e o desenvolvimento humanos.

A inteligência humana, nas suas múltiplas manifestações, continua a ser um pilar insubstituível para a prosperidade da sociedade, ainda mais nos contextos complexos e mutáveis desta Era Digital. Uma dessas manifestações é a inteligência competitiva, que permite obter recomendações acionáveis através do processamento de informações sobre o ambiente externo em busca de oportunidades ou desenvolvimentos que possam ter impacto na posição competitiva de uma empresa ou país (Lee, 2023). Ou a inteligência prospetiva, que, com base em informações passadas e presentes, bem como em especulações futuras, tenta "desenhar" um mapa cognitivo para determinar diferentes opções e reduzir o nível de incerteza que acompanha qualquer decisão (Montero Gómez, 2006).

É verdade que o crescimento exponencial da digitalização, da exposição e da globalização está a impulsionar a origem e a evolução de novas formas de inteligência em resposta a novas tecnologias e métodos de recolha de dados, dando origem a inteligências como a inteligência de fonte aberta (OSINT) ou a inteligência geoespacial (GEOINT), entre outras. Estas disciplinas tiram partido da vasta quantidade de informação disponível para fornecer uma visão global, integrada e detalhada de vários fenómenos. No entanto, a inteligência não se deve limitar à recolha e análise de dados, mas deve também integrar considerações éticas e avaliar as potenciais consequências a longo prazo das decisões.

Atualmente, a informação e a tecnologia são vitais para quase todos os aspectos da vida, e a inteligência desempenha um papel crucial, especialmente no domínio da cibersegurança, uma vez que a capacidade de antecipar, identificar e atenuar as ameaças é essencial para preservar a integridade, a confidencialidade e a disponibilidade dos sistemas.

No entanto, coloca-se a questão: será esta capacidade uma realidade nas agências governamentais e privadas actuais, será a intelligence eficaz na antecipação e mitigação dos riscos crescentes no ciberespaço e estará o ciclo de intelligence atualizado para responder às exigências da Era Digital? O presente documento tem como objetivo realizar uma análise teórica para responder a estas questões e avaliar a eficácia da inteligência no contexto atual.

1.1. NOTA METODOLÓGICA

Para o desenvolvimento deste trabalho, foi realizada uma revisão narrativa da literatura académica e técnica relacionada com a inteligência nos domínios da defesa e segurança, bem como a sua adaptação ao ambiente digital. Esta revisão serviu de base para contextualizar a evolução do conceito, analisar criticamente o ciclo clássico de inteligência e fundamentar a proposta do modelo IDEM.

A pesquisa foi efectuada em bases de dados académicas como Scopus, Google Scholar e Dialnet, bem como em fontes institucionais nacionais e internacionais. Foram utilizadas palavras-chave em espanhol e inglês, tais como "ciclo de inteligência", "ciberinteligência", "inteligência de ciberameaças" ou "ciberameaças". Foi dada prioridade a publicações recentes (2000-2024) que oferecessem abordagens teóricas, modelos metodológicos ou análises críticas do processo de inteligência. Ocasionalmente, devido à falta de literatura de fonte aberta, foram consultados sítios Web de renome ou sítios Web escritos por especialistas técnicos na matéria.

Foram excluídos os documentos sem suporte académico ou institucional, bem como os textos que não abordavam especificamente a dimensão estrutural ou processual da inteligência. A literatura selecionada foi organizada em torno de cinco eixos temáticos: (1) definição do conceito de inteligência, (2) classificação dos tipos de inteligência, (3) evolução histórica e organizacional dos serviços de inteligência, (4) revisão crítica do ciclo tradicional e (5) propostas contemporâneas para sua adaptação à era digital.

Esta abordagem metodológica permitiu detetar lacunas teóricas relevantes e servir de base para o desenvolvimento de um modelo atualizado que integra tanto a dimensão humana como as capacidades tecnológicas da inteligência atual.

2. CONCEITO E EVOLUÇÃO DA INTELIGÊNCIA

O termo inteligência é um conceito abstrato e complexo de delimitar devido à multiplicidade de abordagens sob as quais pode ser estudado. Esta dificuldade não responde apenas à diversidade de domínios que a analisam, mas também aos desafios que se colocam num mesmo contexto para estabelecer uma definição única.

No domínio da defesa e da segurança, a maioria dos autores associa o nascimento da inteligência à emergência dos Estados e das relações interestatais. No entanto, não existe consenso sobre a definição de intelligence, em grande parte devido às diferentes abordagens adoptadas na prática por diferentes países (Andric & Terzic, 2023). Esta disparidade dificulta tanto o avanço teórico do seu estudo como a compreensão aprofundada das várias dimensões e factores que afectam a sua prática (Payá-Santos, 2023).

Neste contexto, uma das primeiras classificações fundamentais, a trindade, foi estabelecida por Sherman Kent, definindo três realidades para este conceito: a inteligência como organização, como processo e como resultado (Díaz Fernández, 2013).

- **Inteligência como organização:** refere-se aos serviços de inteligência principalmente sob a égide da administração pública, como é o caso do Centro Nacional de Inteligência (CNI) e do Centro de Inteligência das Forças Armadas (CIFAS) em Espanha. As funções destas instituições incluem a obtenção, avaliação, interpretação e difusão de informações para proteger e promover os interesses de Espanha, tanto dentro como fora do país; prevenir, detetar e neutralizar ameaças à Constituição, aos direitos e liberdades, à soberania, à segurança do Estado, à estabilidade institucional e ao bem-estar da população; promover a cooperação com serviços de informações estrangeiros e organizações internacionais; interpretar o tráfego de sinais estratégicos; coordenar a utilização de meios de encriptação; garantir a segurança da informação classificada; e

proteger as suas próprias instalações, informações e recursos (Jefatura del Estado, 2002).

- **Inteligência como processo**: compreende todas as atividades, geralmente englobadas no chamado ciclo de inteligência (discutido em maior profundidade em secções posteriores), que são necessárias para atender às demandas dos líderes e que interpretam um ambiente, contexto ou problema. Estas actividades são consideradas um processo cíclico contínuo e vão desde a recolha de informação de várias fontes, continuando com a sua posterior análise e processamento, até à disseminação dos dados de interesse para os utilizadores finais (Chainey & Chapman, 2013).
- **Inteligência como produto:** refere-se ao resultado e/ou conhecimento obtido, em qualquer formato, após o ciclo de inteligência. Esse produto deve influenciar a tomada de decisão e impactar o contexto interpretado (Chainey & Chapman, 2013).

Recentemente, foi também proposta uma quarta dimensão: **a inteligência como cultura,** definida por Navarro como "o conjunto de iniciativas e recursos que promovem a consciencialização da sua necessidade e proporcionam uma compreensão cívica da sua realidade" (Payá-Santos, 2023).

Independentemente da interpretação adoptada, a inteligência visa reduzir a incerteza intrínseca à condição humana e a complexidade do mundo contemporâneo na tomada de decisões para prevenir e evitar qualquer perigo ou ameaça (Jordan, 2015).

Para o conseguir, a inteligência baseia-se em conhecimentos teóricos relacionados com a política, a economia, as relações internacionais, a segurança, a sociologia, a tecnologia, a psicologia, etc. Por conseguinte, é essencial apresentar equipas de peritos de elevada qualidade nas diferentes áreas temáticas, a fim de abordar os problemas de múltiplas perspectivas e encontrar soluções mais eficazes com uma abordagem transversal.

O recente aspeto multidisciplinar da inteligência é uma consequência do alargamento do conceito de segurança e da crescente complexidade do contexto societal, onde as ameaças assimétricas e a ciberguerra são cada vez mais comuns.

Em contrapartida, uma das qualidades mais antigas dos serviços secretos é o secretismo das suas actividades e das informações obtidas. No entanto, a utilização crescente de fontes abertas (OSINT) está a mudar esta perspetiva. Além disso, a globalização e a expansão da utilização da Internet também afectam os conflitos, que são cada vez mais transnacionais e exigem uma cooperação internacional em matéria de informações. No entanto, a proteção das fontes, especialmente das fontes humanas (HUMINT), continua a ser um princípio fundamental, assim como a necessidade de preservar a discrição no tratamento das informações para evitar contramedidas, desinformação ou violação de operações sensíveis.

Em suma, pode-se estabelecer que a inteligência engloba o processo, o produto e a instituição que realiza a coleta, a avaliação e o processamento de informações (Knight, 2024) como ferramenta de tomada de decisão, a fim de identificar, alertar e prevenir riscos e ameaças, reduzindo a incerteza (Francisco & Barrilao, 2019). Para tal, estas tarefas

devem ser realizadas de forma intencional, atempada, planeada, "secreta" e organizada (Andric & Terzic, 2023).

2.1. TIPOS DE INTELIGÊNCIA

Existem várias classificações de inteligência, mas uma das mais comuns é de acordo com o meio em que a informação é encontrada, estabelecendo os seguintes tipos (Kamiński, 2019):

- **SIGINT** (*Signal Intelligence*): é derivada da interceção de sinais, independentemente da forma como são transmitidos. Existem três subcategorias: inteligência de comunicações (COMINT), inteligência eletrónica (ELINT) e inteligência de sinais de instrumentação estrangeira (FISINT). É particularmente importante no controlo das ameaças digitais e dos conflitos híbridos.
- **MASINT** *(Measurement and Signature Intelligence)*: baseia-se na medição de atributos físicos, como as emissões electromagnéticas, as propriedades químicas ou as caraterísticas acústicas. É utilizada em operações militares avançadas e na deteção de armas com o objetivo de caraterizar, localizar e identificar alvos.
- **HUMINT** (*Human Intelligence)*: é o método mais antigo de recolha de informações a partir de fontes humanas, seja através de entrevistas, observação direta, infiltração ou colaboração com actores locais. É essencial em contextos em que as tecnologias não podem aceder-lhe.
- **GEOINT** *(Geospatial Intelligence)* e **IMINT** *(Imagery Intelligence):* inteligência geoespacial e imagética. A primeira combina mapas, dados geográficos e informações de teledeteção, enquanto a segunda se centra na análise visual de imagens de satélite, aéreas ou de drones.
- **OSINT** *(Open-Source Intelligence)*: inteligência derivada de informações do domínio público em formato físico, analógico ou digital em diferentes suportes, como a rádio, a televisão, os jornais, as revistas, a Internet, as bases de dados comerciais, os vídeos, os gráficos, os desenhos, as redes sociais, etc. relatórios abertos ou públicos. O seu volume, acessibilidade e utilidade aumentaram exponencialmente com a Internet (Stewart Bertram, 2015).
- **SOCMINT** *(Social Media Intelligence*): por vezes também referida como uma subcategoria da OSINT, centrada nos media sociais. É utilizada para monitorizar tendências, detetar ameaças emergentes, analisar perceções e seguir atores específicos (Mahood, 2015).

No entanto, outra tipificação comum é de acordo com a sua finalidade: estratégica, tática e operacional (Gruszczak, 2018).

- **Informação estratégica:** centra-se na identificação de riscos, ameaças e oportunidades para apoiar a definição de objectivos e a tomada de decisões, tendo em conta o ambiente, os intervenientes relevantes e as possíveis evoluções.
- **Informações tácticas**: centram-se no planeamento e na execução de operações específicas para atingir um objetivo de âmbito limitado, derivado dos objectivos gerais das informações estratégicas.
- **Inteligência** operacional: também conhecida como inteligência operacional no âmbito militar, tem como objetivo permitir a organização e a execução de actividades para cumprir uma missão específica (Jiménez Villalonga, 2018).

A coexistência e a complementaridade entre estas categorias permitem construir uma inteligência global, adaptada aos diferentes níveis de decisão.

2.2. EVOLUÇÃO DAS ABORDAGENS E ESTRATÉGIAS DE INFORMAÇÃO

Muitos autores defendem que a inteligência é tão antiga quanto a história da humanidade, uma vez que esconder informações confidenciais e descobrir as dos adversários sempre foi uma ferramenta para alcançar e manter o poder. Assim o demonstram civilizações como a China antiga com a sabedoria milenar do mestre Sun Tzu (Navarro Bonilla, 2005) ou a Grécia clássica com os procedimentos secretos de transmissão de informação de Eneias, o Tático (Vela Tejada, 1993).

Na sua origem, a Intelligence era um instrumento ao serviço do poder político, com uma orientação eminentemente militar: conhecer a força, a localização e as capacidades do inimigo para facilitar a tomada de decisões do dirigente. No entanto, à medida que as sociedades se tornaram mais complexas, o mesmo aconteceu com as suas ameaças, o que levou à progressiva expansão da inteligência para aspectos sociais, económicos ou políticos. Assim, as actividades de Intelligence assumiram um papel crucial com o nascimento dos Estados e das relações entre eles, com o objetivo de defender e proteger os interesses nacionais (Andric & Terzic, 2023).

No entanto, só em meados do século XX, nomeadamente após as duas guerras mundiais e a Guerra Fria, é que as potências mundiais começaram a organizar formalmente os seus serviços de informações (os Estados Unidos com a CIA, o Reino Unido com o MI6 e Israel com a Mossad).

A Espanha, embora menos proeminente internacionalmente neste domínio, também fez a primeira tentativa de criar um serviço de informações por volta desta altura. Em 1972 foi criado o Serviço Central de Documentação (SECED) e em 1977 o Centro Superior de Informação de Defesa (CESID), mas só em 2002 foi fundado o atual CNI (Centro Nacional de Informações, 2023).

A partir de então, a revolução tecnológica e a explosão do volume de informação disponível marcaram uma mudança radical: a intelligence deixou de ser um domínio fechado e exclusivamente centrado no Estado para se tornar uma atividade transversal e dinâmica com implicações para além da esfera político-militar. Embora a essência das informações continue a ser a mesma, os métodos, o calendário e os objectivos sofreram profundas transformações. O acesso massivo a dados através de fontes abertas, a aceleração dos fluxos de informação e a globalização das ameaças reduziram o ciclo de vida da informação e puseram em causa o papel central anteriormente ocupado pelo secretismo (Payá-Santos, 2023).

A este novo contexto juntaram-se os atentados de 11 de setembro, que marcaram um ponto de viragem, evidenciando a necessidade de identificar e prevenir ameaças assimétricas e transnacionais, esbatendo a distinção clássica entre inteligência interna e externa, e empurrando as instituições policiais para a adoção de modelos mais analíticos, preventivos e colaborativos (Knight, 2024).

Com o progressivo alargamento da inteligência a outras áreas estratégicas, como o policiamento, que historicamente funcionava numa lógica reactiva, as funções policiais

começaram a evoluir significativamente. A sua abordagem clássica, centrada na resposta a crimes consumados ou na resposta a pedidos de serviço, foi posta em causa à medida que as mudanças sociais e a crescente complexidade da criminalidade exigiam novas formas de intervenção (Organização para a Segurança e Cooperação na Europa, 2017). Posteriormente, várias correntes filosóficas influenciaram o policiamento, tais como (Gkougkoudis et al., 2022):

- ***Policiamento comunitário* ou *policiamento orientado para a comunidade* (COP):** dá prioridade à cooperação entre os cidadãos e as agências de aplicação da lei, promovendo a confiança e a prevenção (Carter & Fox, 2019).
- **Policiamento *para a resolução de problemas***: visa identificar e analisar os problemas subjacentes à criminalidade numa perspetiva mais ampla e transversal e procurar soluções estruturais e sustentáveis (Organização para a Segurança e Cooperação na Europa, 2017).
- ***Policiamento de tolerância zero*:** resposta rigorosa mesmo para delitos menores, baseada em ideias desenvolvidas por dois criminologistas americanos, James Q. Wilson e George Kelling, que em 1982 publicaram um artigo intitulado "Broken Windows" (Grabosky, 1999).

No entanto, nas últimas décadas, devido à complexidade das ameaças e dos riscos, muitos académicos e profissionais salientaram que a abordagem holística mais bem sucedida para combater a globalização da criminalidade é o *Intelligence-Led Policing* (ILP), que se traduz por policiamento baseado em informações. Esta abordagem surgiu na década de 1990 no Reino Unido como uma estratégia para melhorar a eficiência fiscal dos serviços policiais, ou seja, para otimizar a afetação de recursos, a produtividade operacional e a qualidade dos resultados do policiamento. Inicialmente implementada sobretudo para combater a criminalidade grave e organizada, evoluiu desde então a nível mundial como um modelo proactivo, impulsionado pela análise de dados e centrado na prevenção, redução e perturbação de todos os tipos de criminalidade. Nos Estados Unidos, foram os acontecimentos de 11 de setembro de 2001 que levaram finalmente à sua adoção, centrando a sua abordagem em formas mais complexas de criminalidade (Summers & Rossmo, 2019).

A ILP é uma filosofia proativa para identificar e prevenir problemas criminais usando dados brutos e análises mistas (quantitativas e qualitativas), mas não é uma tática pontual, mas uma estrutura flexível, adaptável e sustentável baseada em dados objetivos (Carter & Fox, 2019). No entanto, sua implementação enfrenta desafios em termos de clareza terminológica e integração de dados, bem como a necessidade de garantir o respeito aos direitos humanos na gestão da inteligência.

Paralelamente, o modelo de inteligência baseada em actividades (ABI) expandiu as capacidades analíticas, especialmente face a ameaças emergentes. Com antecedentes na Guerra Fria, o seu desenvolvimento foi impulsionado pela necessidade de gerir e analisar enormes volumes de dados gerados pelas tecnologias modernas, como os drones e as redes sociais, especialmente no contexto da luta contra o terrorismo. Os métodos tradicionais de análise revelaram-se inadequados neste novo ambiente, uma vez que os analistas passam demasiado tempo à procura de informações e a monitorizar alvos conhecidos, limitando a sua capacidade de descobrir o desconhecido. A ABI melhora este processo ao permitir a correlação em tempo real de dados provenientes de uma variedade

de fontes, ultrapassando as limitações dos métodos tradicionais de informação, vigilância e reconhecimento (ISR) (Atwood, 2015).

Outra abordagem relevante é o modelo 3i proposto por Ratcliffe em 2006, baseado em três pilares fundamentais: "interpretar", "influenciar" e "ter impacto" no ambiente criminal. Os analistas devem interpretar ativamente o ambiente, influenciar os decisores que, por sua vez, utilizam essa informação para conceber estratégias que afectam o ambiente criminal (Budhram, 2015). Em 2016, acrescentou mais um i, o da intenção, como se pode ver na Figura 1, destacando a necessidade de clareza e compreensão dos objectivos estabelecidos (Organização para a Segurança e Cooperação na Europa, 2017).

Figura 1
O modelo 4-i de Ratcliffe: intenção, interpretação, influência e impacto

Nota: Adaptado de *OSCE Guidance on Intelligence-led Policing (p. 24)*, por *OSCE, 2017, OSCE. Intelligence-led Policing* (p. 24), pela OSCE, 2017, OSCE

Em suma, as informações evoluíram de uma atividade altamente secreta e centralizada para um processo transversal, interdisciplinar, distribuído e tecnologicamente apoiado. Esta evolução justifica a necessidade de novos modelos como o IDEM, que integram a análise humana com o processamento automatizado para fazer face às ameaças modernas, nomeadamente no ciberespaço. Além disso, esta trajetória permite-nos observar uma crescente convergência entre as lógicas de segurança, defesa e tecnologia, posicionando a inteligência como uma componente chave da soberania digital e da resiliência institucional.

3. O CICLO DA INTELIGÊNCIA

Embora Sherman Kent seja frequentemente creditado com a formulação científica do método de inteligência, pesquisas posteriores mostraram que uma metodologia rigorosa e um conjunto abrangente de operações (o que mais tarde ficou conhecido como o ciclo de inteligência) já foram delineados, por exemplo, durante a Guerra Civil Espanhola (Navarro Bonilla, 2004).

O ciclo de inteligência reúne todas as actividades que permitem a transformação da informação bruta em inteligência e, como o seu nome indica, tem um carácter cíclico. O ciclo de inteligência clássico tem quatro fases, mas em alguns países são acrescentadas

fases diferentes ou subfases diferenciadas. Por exemplo, em Espanha, o CCN-CERT estabelece seis fases para o ciclo de inteligência: direção e planeamento; recolha; transformação; análise e produção; disseminação e, finalmente, avaliação (Centro Criptológico Nacional, 2015).

- A primeira fase, designada por **direção e planeamento**, estabelece o quê e o como, ou seja, os requisitos do produto de informações a produzir e as acções a desenvolver para o obter. O objeto do estudo, o âmbito, os objectivos, o prazo e o tipo de relatório devem ser claros para que o trabalho nas restantes fases seja eficiente e resulte em maior qualidade e em conformidade com as normas legais nacionais e internacionais (Organização para a Segurança e Cooperação na Europa, 2017).
- Na fase seguinte, **a recolha,** são recolhidos dados brutos, por exemplo, das fontes acima mencionadas (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). Este processo é complexo, uma vez que os analistas devem encontrar o equilíbrio certo entre a recolha de todos os dados necessários e suficientes sem cair numa sobrecarga de informação redundante. Para tal, devem estar conscientes da existência, relevância, acessibilidade e fiabilidade das fontes selecionadas, bem como das restrições legais e dos requisitos de autorização (Organização para a Segurança e a Cooperação na Europa, 2017). Além disso, a validade e a exatidão das informações devem ser avaliadas antes de prosseguir com as restantes etapas do ciclo de informações.
- Na fase de **transformação**, os dados brutos recolhidos na fase anterior são convertidos em conjuntos estruturados, como bases de dados, referências bibliográficas, etc., transformando a informação nos formatos necessários para continuar o ciclo e obter inteligência. Esta fase consiste em catalogar, hierarquizar e referenciar a informação recolhida.
- A quarta fase, **análise e produção**, é composta pelas actividades através das quais a informação transformada é integrada, avaliada, analisada e preparada de modo a obter o produto final. Dentro desta fase, podem ser estabelecidas duas subfases: a primeira envolve a integração de dados obtidos de diferentes fontes para estabelecer hipóteses e identificar um padrão de inteligência; a segunda envolve a interpretação dos dados, ou seja, ir além das informações obtidas, refutando ou apoiando as hipóteses pré-estabelecidas (Organização para a Segurança e Cooperação na Europa, 2017). Geralmente, esta fase resulta naquilo a que se chama *inteligência acionável*, *um* produto de inteligência que responde aos requisitos definidos na fase de direção e planeamento e, portanto, às necessidades do consumidor. Este produto, por sua vez, pode ser de vários tipos, como uma análise de tendências, uma avaliação a longo prazo, uma informação atual, uma informação de estimativa ou de alerta, etc. (National Cryptologic Centre, 2015).
- Na fase de **divulgação**, o produto final é entregue ao consumidor que o solicitou e, se necessário e legalmente admissível, será também partilhado com outras partes interessadas.
- A última fase corresponde à **avaliação**, que permite o feedback contínuo de todas as fases anteriores do ciclo de inteligência com os resultados obtidos, permitindo o ajuste e o aperfeiçoamento das actividades individuais e do ciclo como um todo. Isto é particularmente útil para responder de forma optimizada às necessidades de informação em constante evolução.

No entanto, muitos especialistas põem em causa este modelo tradicional de inteligência e uma das críticas é a simplificação excessiva deste modelo em relação à grande complexidade do processo real de aquisição de inteligência. Robert Clark salienta que este termo "se tornou um conceito teológico: ninguém questiona a sua validade", apesar de não definir as etapas exactas a seguir (Phythian et al., 2013).

Além disso, Arthur Hulnick salienta que a noção de que os clientes dos serviços de informações orientam os produtores no início do ciclo é incorrecta, uma vez que os clientes esperam frequentemente ser alertados pelo sistema de informações, pelo que o processo de recolha é principalmente orientado pela necessidade de preencher lacunas de dados e não por orientações políticas (Pothoven et al., 2023).

Por outro lado, nem sempre os organismos de recolha de dados são abordados; muitas vezes, as bases de dados existentes que foram alimentadas durante anos são consultadas diretamente para preparar um relatório. Ou podem ser solicitados novos dados brutos às equipas que os recolhem, mas um novo pedido de informações não é normalmente feito ao nível do cliente (Jordán, 2011).

Quanto à fase de análise, a sua definição dentro do ciclo de inteligência não é criticada em si mesma, mas afirma-se que é a fase em que se cometem mais erros, não por falta de informação, mas pelo contrário, devido à sobrecarga de dados que leva a que a informação relevante seja ignorada ou interpretada de forma inadequada pelos analistas (Jordán, 2016). Os analistas precisam de estar conscientes dos seus próprios processos mentais e de potenciais erros, evitando simplificações cognitivas não intencionais e, claro, enviesamentos. Além disso, em alguns casos, como em situações de crise, os dados brutos chegam diretamente sem passar por esta fase.

No que se refere à fase de divulgação, esta também não é por vezes ultrapassada, uma vez que nem todas as análises produzidas chegam aos consumidores. Muitas não são lidas pelos destinatários e são armazenadas diretamente na base de dados interna. Noutros casos, é frequente os clientes já terem tomado as suas decisões e ignorarem as informações que não as apoiam.

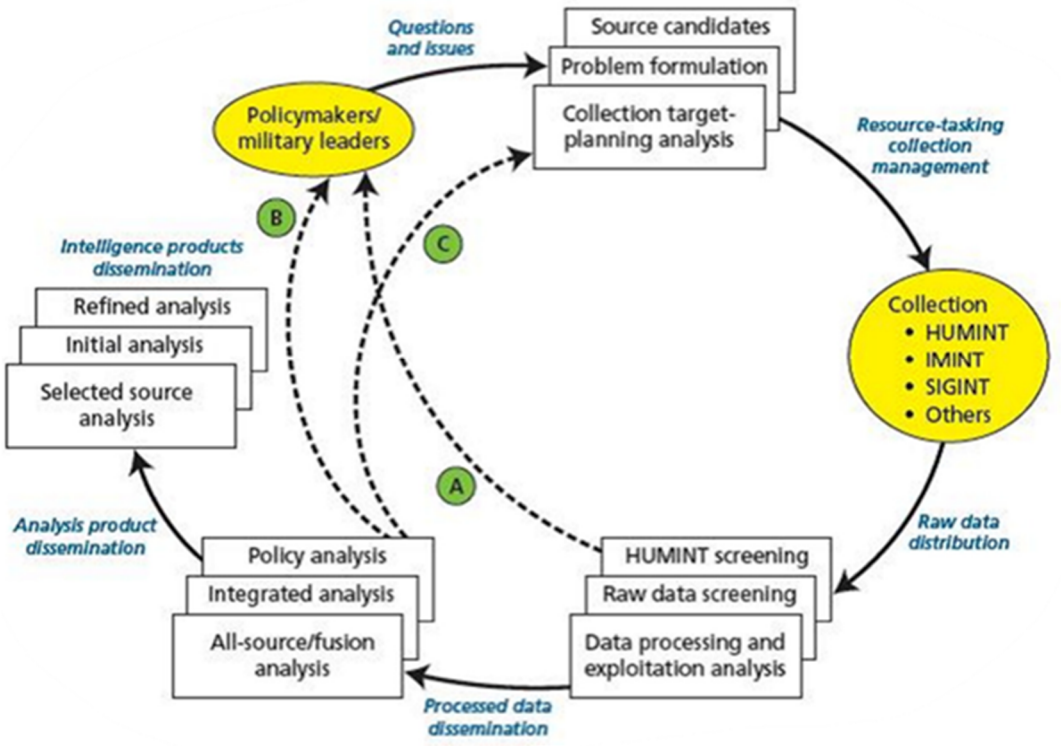
Além disso, em relação ao ciclo de inteligência em geral, critica-se a sua definição como uma sequência de fases que é finalmente organizada de forma circular, quando se trata de um processo mais dinâmico, onde todas as fases se retroalimentam, podendo avançar e retroceder em qualquer direção dentro do ciclo. Aponta também para problemas organizacionais, de comando e de fluxo de informação que conduzem a uma falta de flexibilidade na ação e na comunicação, atrasando os processos de tomada de decisão (Organização para a Segurança e Cooperação na Europa, 2017).

Comentadores como Peter Gill e Mark Phythian argumentam que o conceito de ciclo de informações se tornou obsoleto devido aos avanços tecnológicos, à revolução da informação e às mudanças nas ameaças e nos alvos. Propõem a sua substituição por uma "rede de informações" que reflicta melhor as interações complexas entre a definição de alvos, a recolha e a análise, e realça os factores contextuais que influenciam o processo e podem ser afectados pelos seus resultados (Pothoven et al., 2023).

Por outro lado, vários autores tentaram captar a complexidade do ciclo de inteligência em esquemas alternativos ao tradicional. Como se pode ver emFigura2 ,

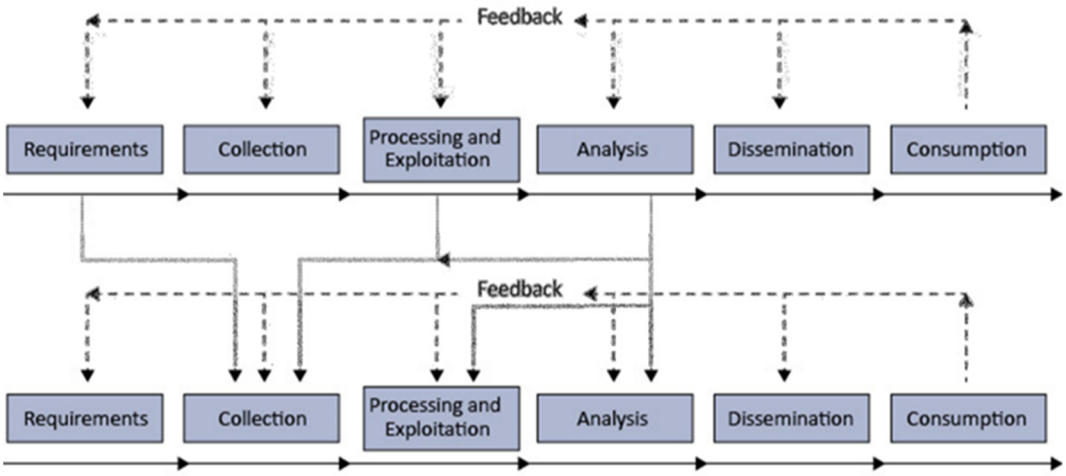
Treverton e Gabbard propõem uma abordagem mais realista que inclui atalhos entre fases, mostrando que há passos que por vezes são perdidos, por exemplo, que a informação não analisada pode chegar diretamente aos decisores. Mark Lowenthal apresenta um ciclo composto por feedbacks constantes, em que novas necessidades e ambiguidades reactivam o processo, tornando-o mais dinâmico e multifacetado, como se pode ver emFigura3 . E Robert M. Clark apresenta o conceito de *Target-Centric Intelligence*, um modelo colaborativo e orientado para o alvo, onde todos os participantes constroem juntos uma imagem partilhada da questão de inteligência de interesse, representada naFigura 4 (Jordan, 2016).

Figura2
Abordagem de Treverton e Gabbard



Nota: Extraído de *A Review of the Intelligence Cycle* (p. 4) de J. Jordán, 2016, *Análise GESI (Grupo de Estudos em Segurança Internacional)*, 2.

Figura3
Processo multi-estratos Mark Lowenthal



Nota: Extraído de *A Review of the Intelligence Cycle* (p. 5) de J. Jordán, 2016, *Análise GESI (Grupo de Estudos em Segurança Internacional),* 2.

Figura 4
Inteligência centrada no alvo por Robert M. Clark

Nota: Extraído de *A Review of the Intelligence Cycle* (p. 6) de J. Jordán, 2016, *Análise GESI (Grupo de Estudos em Segurança Internacional),* 2.

Por último, surgiram também propostas como o conceito JISR (Joint Intelligence, Surveillance and Reconnaissance) da NATO. Este termo refere-se ao conjunto integrado de capacidades de informações e operações que sincroniza e integra o planeamento e a execução de todas as capacidades de recolha de informações com o seu processamento, exploração e divulgação. Este conceito surge da necessidade de melhorar a partilha de informações e de informações para prevenir crises, ameaças terroristas, actividades criminosas transnacionais e ciberameaças (Gruszczak, 2018). A inteligência, a vigilância

e o reconhecimento (ISR) sempre foram actividades essenciais das operações militares, mas foram divididas de acordo com os níveis de comando (estratégico, operacional e tático), ou de acordo com as várias disciplinas de inteligência, dependendo do tipo e complexidade das fontes de informação envolvidas. No contexto atual, esta divisão limita a utilização óptima dos especialistas, agências, fontes e actividades de informações. Por conseguinte, é proposto o modelo JISR, em que as actividades de informações, vigilância e reconhecimento funcionam como uma unidade única, integrando todos os níveis e domínios (Ministério da Defesa, 2023).

No entanto, o modelo JISR apresenta o mesmo processo que o ISR, que é composto por 5 fases: planeamento, recolha, processamento, exploração e disseminação (TCPED). A principal diferença em relação ao ciclo tradicional de intelligence é que este processo não é linear nem circular, mas as diferentes fases são executadas de forma dinâmica, sequencial, simultânea ou independente, consoante o resultado pretendido. No entanto, neste modelo, o processo ISR está normalmente alinhado com a fase de recolha do ciclo de informações, e os resultados desta recolha são incorporados na fase de processamento, bem como apoiam o ciclo de decisão.

No entanto, esta abordagem também enfrenta várias limitações. Em primeiro lugar, pode haver uma falta de recursos suficientes para satisfazer todos os requisitos, especialmente devido à elevada procura e à baixa disponibilidade de certas capacidades de recolha. Há também problemas técnicos, como limitações na capacidade de computação e na largura de banda, que afectam a capacidade de processar e divulgar resultados. Os adversários podem interferir através de ataques às capacidades ISR, camuflagem, ocultação e desinformação. Além disso, o acesso à ISR pode ser limitado por barreiras físicas, cognitivas, virtuais, jurídicas e políticas (Ministério da Defesa, 2023).

A inteligência como processo atual deve, portanto, afastar-se dos modelos tradicionais lineares e cíclicos para estruturas mais fluidas e em rede, capazes de responder com agilidade às ameaças emergentes e tirar partido do vasto volume de dados disponíveis (Jiménez Villalonga, 2018).

4. PROPOSTA DE ACTUALIZAÇÃO DO CICLO DE INTELIGÊNCIA NA ERA DIGITAL: O MODELO IDEM

O ciclo clássico dos serviços de informações foi durante décadas a espinha dorsal dos serviços de informações enquanto processo. Na altura, esta representação sequencial fazia sentido, pois facilitava a normalização, a formação dos analistas e a gestão das operações. No entanto, o modelo tem limitações significativas quando transposto para os actuais contextos de complexidade, incerteza e ritmo acelerado de mudança, especialmente em domínios como o ciberespaço.

Neste ambiente altamente dinâmico, a inteligência tornou-se extremamente importante como ferramenta para compreender e antecipar ameaças, particularmente no domínio digital. À medida que as organizações expandem a sua presença no ciberespaço para maximizar a sua visibilidade e alcance, também aumentam a sua exposição a potenciais ataques. Esta transformação exige que se repense o papel da inteligência para além da sua formulação clássica, adaptando-a às particularidades de um ambiente descentralizado, interligado e em constante evolução.

No entanto, esta adaptação não é simples. A proliferação de termos e abordagens reflecte tanto a juventude do campo como a sua rápida expansão. Em alguns quadros conceptuais, o termo ciberinteligência ou CYBINT é utilizado como um subtipo de COMINT (Jiménez Villalonga, 2018), mas também pode ser considerado como um tipo de inteligência superior que engloba e coordena as actividades OSINT, SIGMINT, SOCMINT e até HUMINT (Portillo, 2019).

No contexto europeu, é mais comum falar-se de inteligência contra ciberameaças (CTI), que se refere à aplicação sistemática da inteligência para identificar, analisar e mitigar as ameaças que afectam o ciberespaço. Segundo a Gartner (Lee, 2023), a CTI assenta em conhecimentos baseados em provas que fornecem contexto, mecanismos, indicadores e conselhos práticos sobre ameaças emergentes ou existentes.

É por isso que a CTI desempenha um papel crucial ao ajudar as organizações a desenvolver uma estratégia de segurança proactiva que lhes permite compreender e antecipar as tácticas, técnicas *e* procedimentos (TTP) dos adversários. Também facilita a identificação de ameaças na sua origem e a resposta efectiva a incidentes antes que estes possam causar danos significativos.

No entanto, quando se trata de implementar sistemas de investigação ou de trabalho neste domínio, continua a não haver ciclos metodológicos específicos e amplamente aceites para estruturar o processo de recolha e análise de ciberinteligência. Por conseguinte, existe uma tendência para recorrer ao ciclo tradicional de recolha de informações ou a uma das abordagens alternativas existentes. Mas, como já foi referido, todas elas apresentam limitações significativas para a sua aplicação efectiva em ambientes digitais.

O modelo clássico é rígido e sequencial; o **modelo proposto por Treverton e Gabbard** permite alguma flexibilidade, mas carece de um feedback claro; o **modelo centrado no objetivo** propõe um ciclo contínuo mais próximo do objetivo, mas sem uma estrutura verdadeiramente flexível entre fases; e **a abordagem multinível de Lowenthal** introduz dinamismo, mas mantém uma certa linearidade e as ligações bidireccionais entre fases não são totalmente compreendidas.

Tabela 1
Quadro comparativo dos diferentes modelos de representação da inteligência como processo

	Modelo clássico	Modelo Treverton e Gabbard	Modelo por Mark Lowenthal	Modelo centrado no alvo
Estrutura	Linear ou cíclico (fases sucessivas num círculo)	Semi-linear (com possíveis "atalhos")	Multinível (com camadas activas conforme necessário)	Cíclico (centrado no objetivo)
Início do processo	A pedido do consumidor	Semelhante ao clássico, mas permite reiniciar a partir de fases intermédias.	De novas necessidades para reativar fases anteriores	Da análise do objetivo (de análises anteriores ou de novas necessidades e informações)
Fases principais	Direção e planificação, recolha, tratamento, análise e produção, difusão, avaliação	Semelhante ao modelo clássico, mas sem ordem estrita ou menção de feedback.	O mesmo que o clássico, com ciclos internos e *feedback* contínuo.	Os requisitos e *as lacunas*, a recolha, a análise e a divulgação estão interligados em torno do objetivo de
Interação entre fases	Limitado (feedback no final)	Médio (linear com atalhos)	Descarga (contínua e simultânea)	Média (ciclos ligados pelo objetivo)
Flexibilidade e adaptabilidade	Baixo (modelo rígido e sequencial)	Médio (alguma fluidez, mas mantém fases definidas)	Elevada (orientada para a reformulação contínua do processo)	Médio: (dinamismo em torno do objetivo)
Divulgação de informações	No final do processo	Pode ser omitido ou antecipado se o produto o exigir.	Pode ocorrer em diferentes níveis e momentos, dependendo do ciclo interno ativado.	Fim do processo, após a fase de produção
Feedback	No final do processo	Não explicitamente referenciado	Em todas as fases	Não explicitamente referenciado

É por isso que este trabalho propõe o modelo de inteligência IDEM (Enhanced Dynamic Enriched Intelligence) com uma abordagem em rede, não linear e altamente adaptativa, em que as fases do processo de inteligência não se seguem sequencialmente, mas interagem de forma dinâmica, flexível e contínua, permitindo um feedback constante entre fases e equipas de trabalho.

Enquanto o modelo tradicional começa com a **direção e o planeamento,** onde os requisitos de informação são estabelecidos de acordo com as necessidades do decisor, o modelo IDEM propõe começar com uma fase **de identificação e priorização das ameaças** em tempo real. Uma das críticas mais repetidas ao ciclo tradicional é a sua falta de flexibilidade, pois uma vez definidos os objectivos, o processo tende a seguir uma trajetória fixa, o que é ineficaz no contexto atual, em que as ameaças evoluem rapidamente e nem sempre estão alinhadas com as necessidades previamente estabelecidas. Por conseguinte, o objetivo desta fase deve ser detetar e dar prioridade às ameaças emergentes de forma proactiva, sem depender apenas das orientações iniciais dos consumidores, que muitas vezes não chegam a tempo ou nem sequer são formuladas.

Esta fase tornar-se-ia um processo dinâmico e contínuo, alimentado por uma monitorização constante, pelo reconhecimento em tempo real de padrões de ameaças emergentes e pela capacidade de redirecionar rapidamente os esforços de informação à medida que surgem novas ameaças ou mudanças nas condições (Dahj, 2022).

A fase seguinte, a **recolha**, continua a ser fundamental para os serviços de informações enquanto processo, uma vez que sem dados e informações não é possível obter conhecimentos acionáveis. No modelo clássico, um dos maiores desafios tem sido o de filtrar eficazmente grandes volumes de dados para evitar tanto a saturação da informação como a perda de informação crítica. Na Era Digital, esta tarefa tornou-se ainda mais complexa devido ao aumento exponencial da quantidade de fontes e dados disponíveis, impulsionado pelas novas tecnologias, pela globalização e pelo curto prazo de validade da informação. A IDEM aborda esta complexidade através da utilização de tecnologias avançadas, como a *aprendizagem automática* (ML) e a inteligência artificial, que permitem uma recolha automatizada, contínua e abrangente. Apesar de tratarem volumes significativamente maiores, estas ferramentas permitem filtrar, hierarquizar e enriquecer a informação em tempo real, garantindo a sua relevância e utilidade.

Nesta abordagem, não faz sentido estabelecer uma fase específica para a **transformação** de dados, como no modelo clássico. Graças a tecnologias avançadas, como o processamento de linguagem natural (PNL*)* e as ferramentas de análise *de grandes volumes de dados*, a conversão de dados brutos em informações relevantes e contextualizadas pode ocorrer em várias fases do processo em simultâneo. Isto permite que os dados sejam processados, estruturados e analisados em paralelo, facilitando uma resposta ágil a novas informações ou alterações no ambiente.

Além disso, a separação entre **transformação** e **análise** pode levar a uma falta de integração e a uma perda de contexto durante a transição. Por esta razão, o IDEM substitui estas duas fases do modelo clássico por uma única fase de **contextualização e enriquecimento** que se concentra em colocar os dados no contexto, interpretar a sua relevância e compreender a ligação a outros eventos e padrões. Desta forma, a análise pode ser continuamente actualizada e ajustada à medida que surgem novos dados e novas questões, desenvolvendo uma capacidade de adaptação contínua. É também essencial processar e integrar informações de múltiplas fontes de dados, uma vez que estas facilitam uma interpretação mais profunda e eficiente, especialmente no atual contexto de ameaças híbridas. Ao contrário da abordagem tradicional, e também dos sistemas ISR clássicos, que estabelece um processo individual para cada tipo de fonte (OSINT, HUMINT, SIGINT, COMINT, etc.) (Ministério da Defesa, 2023), a IDEM propõe um modelo interconectado, multi-sensor, mais eficaz na deteção e análise de fenómenos complexos, tal como sugerido pela doutrina JISR do Departamento de Defesa dos EUA, discutida na secção 2.2

Em contrapartida, o modelo IDEM mantém uma etapa específica para a **produção de** inteligência acionável. Enquanto, no ciclo tradicional, a análise e a produção se concentram na geração de relatórios e recomendações que auxiliam a tomada de decisão, o IDEM defende produtos não apenas reativos, mas também preditivos, permitindo a antecipação de eventos e tendências ou a avaliação de impactos que facilitem o ajuste de estratégias e decisões em tempo real. A tónica é colocada aqui na inteligência como apoio dinâmico à decisão e não como um produto fechado.

Paralelamente ao desenvolvimento de todas estas fases, a fase de **feedback** definida no ciclo de inteligência tradicional é indispensável, mas reinterpretada como um processo transversal. Para garantir uma melhoria contínua e um processo mais eficaz, é fundamental que os pontos de melhoria ou os pontos fracos sejam evidenciados ao longo de cada uma das fases. Isto permitirá que estas observações sejam tidas em conta não só nas etapas seguintes, mas também em futuras investigações, em vez de se esperar pela obtenção do produto final de intelligence, como acontece no modelo tradicional.

Finalmente, no ciclo tradicional, **a disseminação** é reservada para o final do processo, uma vez produzido o relatório de intelligence. O IDEM rompe com esta lógica, propondo uma divulgação modular e progressiva, não só partilhando a inteligência enquanto tal, mas também as ameaças reconhecidas e classificadas na fase de identificação e priorização, ou os dados recolhidos das diferentes fontes disponíveis ou ainda os dados contextualizados e enriquecidos em diferentes formatos. Obviamente, esta difusão precoce deve ser cuidadosamente gerida, assegurando a proteção das fontes para evitar contramedidas e desinformação por parte dos alvos e para proteger as fontes humanas (HUMINT). No entanto, a natureza transnacional dos crimes actuais exige a cooperação internacional de diferentes serviços de informações e, por conseguinte, a partilha atempada e não retardada de informações entre eles para obter resultados mais eficazes.

No entanto, apesar das capacidades técnicas oferecidas pela automatização, o papel do analista humano continua a ser essencial em cada uma das fases acima descritas. As ferramentas automatizadas funcionam com parâmetros e algoritmos definidos pelos seus programadores, que são verdadeiramente capazes de interpretar a informação num contexto mais amplo, tendo em conta factores culturais, políticos e situacionais. Além disso, os modelos preditivos não têm a flexibilidade cognitiva necessária para lidar com ambiguidades, contradições ou excepções e podem falhar face a entradas erradas, dados tendenciosos ou situações imprevistas.

Os analistas, por outro lado, são capazes de se adaptar, inovar e reajustar as suas abordagens em resposta a novos paradigmas, enquanto os modelos de inteligência artificial necessitam de uma grande quantidade de dados de treino para poderem desenvolver novas metodologias de análise e não são capazes de aplicar abordagens criativas se surgirem novas questões. Esta capacidade dos humanos de colaborar entre equipas, de discutir interpretações, de reestruturar estratégias com base no *feedback* recebido é essencial para o sucesso da implementação de estratégias de inteligência (Jordan, 2011).

Tabela 2
Quadro comparativo entre o modelo clássico e o modelo IDEM proposto

	Modelo clássico	Modelo IDEM (proposta própria)
Estrutura	Linear ou cíclico (fases sucessivas num círculo)	Modular, dinâmico e em rede (círculos concêntricos e interligados)
Início do processo	A pedido do consumidor	Proactivo, sem pedido prévio
Fases principais	Direção e planificação, recolha, tratamento, análise e produção, difusão, avaliação	Identificação e definição de prioridades, recolha, contextualização e enriquecimento, produção de informações, feedback e divulgação
Interação entre fases	Limitado (feedback no final)	Descarga: fases interactiva e bidirecional
Flexibilidade e adaptabilidade	Baixo (modelo rígido e sequencial)	Muito elevado (fases simultâneas e reiniciáveis)
Divulgação de informações	No final do processo	Transversal e contínuo desde as fases iniciais do processo
Feedback	No final do processo	Constante: em todas as fases
Tecnologia aplicada	Não explicitamente abrangido	Integração de tecnologias avançadas (IA, ML, PNL, *grandes volumes de dados*)
Participação humana	Central, mas hierárquico	Combinação sinérgica de analistas humanos e ferramentas automatizadas
Aplicabilidade em ambientes digitais	Limitada	Elevada (orientada para as ciberameaças e cenários complexos)

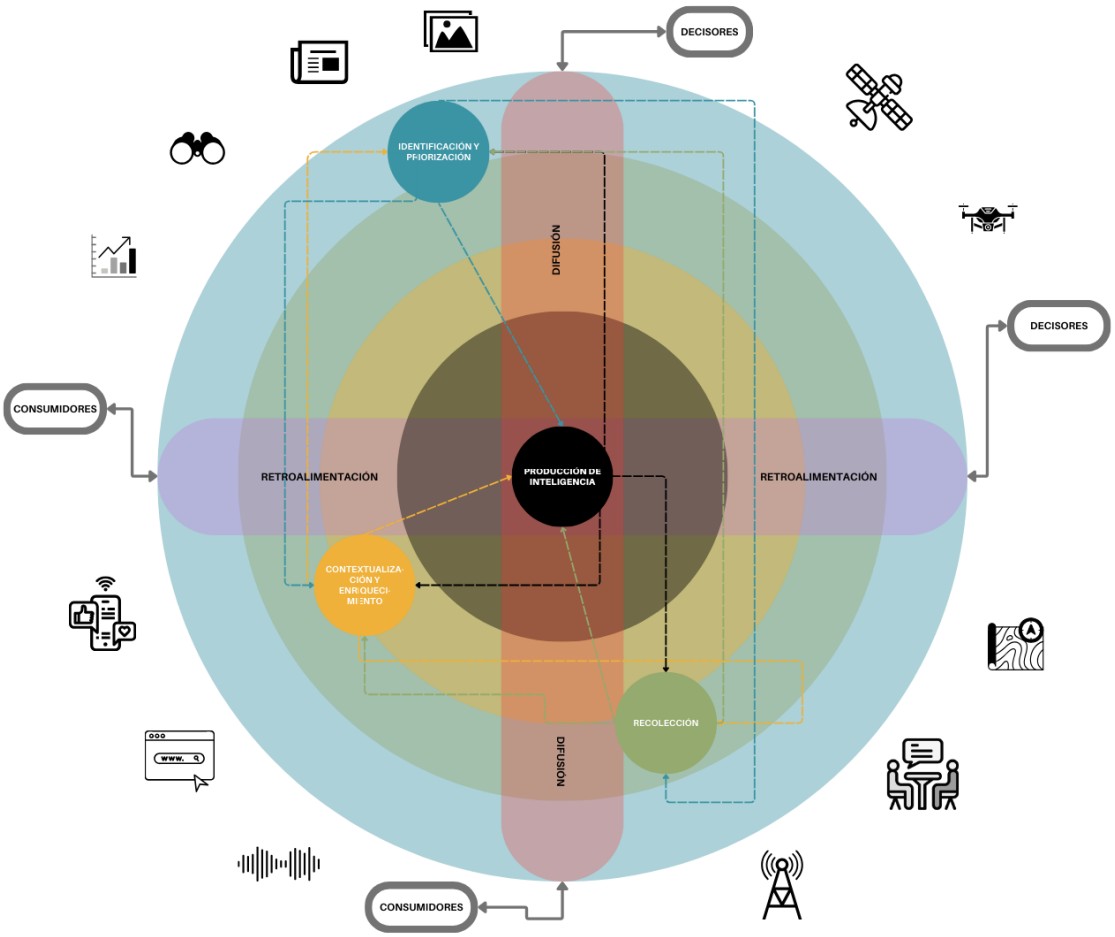
A seguir é apresentado um esquema representativo do modelo IDEM, no qual as diferentes fases estão dispostas em círculos concêntricos. Esta disposição reflecte, por um lado, a proximidade crescente do produto final da inteligência à medida que nos aproximamos do centro e, por outro lado, a natureza constante de todas as fases, uma vez que as fases mais internas estão contidas nas mais externas. No entanto, o modelo não estabelece um percurso linear, não é necessário passar por todas as fases para chegar ao centro. Este carácter dinâmico é representado por setas que indicam os possíveis fluxos de entrada e saída entre as diferentes fases, permitindo transições diretas e bidireccionais de acordo com as necessidades do contexto.

Perpendicularmente a estes círculos e perpendicularmente entre si, integram-se dois elementos-chave, representados como rectângulos transversais. O primeiro representa a fase de feedback, transversal a todas as fases e oportuna para a melhoria contínua de todo o ciclo. O segundo simboliza a fase de disseminação, também colateral a todas as fases e essencial para obter produtos mais completos e resultados mais eficazes.

No exterior do sistema encontram-se os consumidores e os decisores. O seu número e relevância dependerão tanto das necessidades de informação requeridas como do impacto esperado da análise efectuada. Estas figuras são representadas por setas bidireccionais, que indicam a sua dupla função de estabelecer o objetivo e os critérios das informações, ao mesmo tempo que recebem feedback ou produtos de informações para facilitar a sua tomada de decisão.

São também incorporados ícones de diferentes fontes de informação, apoiando assim a estratégia de recolha, contextualização e enriquecimento de dados de diferentes fontes para um processo de informação mais abrangente, transversal e eficaz.

Figura 5
Modelo de inteligência IDEM



Nota: Elaboração própria, Paula Castro Castañer, 2024.

A combinação da adaptabilidade, da experiência, do juízo crítico e do talento humano com a capacidade das máquinas para processar grandes volumes de dados cria uma sinergia que garante uma tomada de decisões mais eficaz, multidisciplinar, informada e flexível, assegurando uma maior qualidade e relevância da inteligência gerada.

4.1. EXEMPLO PRÁTICO DA APLICAÇÃO DO MODELO IDEM

Um exemplo prático que ilustra a utilidade da aplicação deste modelo de inteligência é o caso de um fornecedor nacional de energia detetar uma anomalia nos seus sistemas de controlo SCADA. Nesta situação, não existe ainda um incidente confirmado ou um pedido explícito dos decisores (uma vez que estes provavelmente ainda não têm conhecimento desta situação), o que implica que a ativação do processo de inteligência tenha origem de forma proactiva e autónoma, com base em sinais identificados no

ambiente operacional. No entanto, a equipa de informações internas ativa o modelo IDEM para antecipar se se trata de uma ameaça real ou de um falso alarme.

Um alerta automático de tráfego anómalo para os servidores de backup provém do IDS, que inicia a fase de identificação e priorização. Este alerta, embora preliminar, é suficiente para que a equipa de inteligência interna classifique a ameaça como prioritária, tendo em conta o potencial impacto que um compromisso desta natureza pode ter nas infra-estruturas críticas do país. Em consequência, decide-se despriorizar temporariamente as investigações abertas sobre campanhas hacktivistas e a vigilância geopolítica de baixo impacto, bem como outras tarefas de monitorização de rotina em fóruns e canais obscuros. Esta reorientação permite concentrar os esforços humanos e tecnológicos numa única hipótese de trabalho: uma possível intrusão avançada direcionada.

A recolha é desencadeada simultaneamente a partir de múltiplas fontes internas (logs, SIEM, registos de autenticação) e externas (feeds de ciberinteligência, bases de dados de indicadores de comprometimento, alertas de entidades cooperantes ou fornecedores de informações). Durante esta fase, quando surgem indícios que sugerem motivações económicas por detrás do possível ataque, como, por exemplo, a extração de dados de mercado em vez de informação operacional, o processo regressa brevemente à fase de identificação para reformular a hipótese inicial. Este regresso permite que a análise se centre agora na possibilidade de um caso de espionagem económica industrial em desenvolvimento, mudando consequentemente o foco do resto das actividades do processo de informações.

Na fase de contextualização e enriquecimento, os dados recolhidos são integrados com informações históricas de incidentes anteriores e análises de tendências no sector da energia. São utilizadas técnicas de análise comportamental, de atribuição de TTP e de extração de dados históricos. Estas metodologias facilitam a deteção de padrões e coincidências com campanhas previamente atribuídas a actores estatais ou a grupos intermediários, ou seja, entidades que operam como proxies ou agentes indirectos de outros actores com interesses geopolíticos ou económicos.

Os resultados das informações são distribuídos em diferentes formatos, adaptados às necessidades específicas de cada tipo de destinatário. Entre eles contam-se os alertas tácticos dirigidos às equipas de cibersegurança responsáveis pela resposta imediata, os relatórios estratégicos dirigidos aos gestores de topo dos sistemas de energia e as recomendações preventivas dirigidas a outros operadores do sector para que reforcem a sua postura de defesa.

É importante notar que esta produção e divulgação de informações é feita de forma contínua e em paralelo com o desenvolvimento da investigação, sem esperar por uma "conclusão definitiva". Esta abordagem permite uma resposta precoce e dinâmica a ameaças emergentes, uma vez que outros actores relevantes no sector da energia poderiam reportar incidentes semelhantes nas suas redes após a receção destes produtos, o que permitiria reabrir ciclos de análise e reajustar a priorização de ameaças à escala nacional.

Para além do feedback externo dos intervenientes relevantes para ajustar os pressupostos e as prioridades com base nos sinais do ambiente, há também uma fase de feedback interno contínuo destinada a melhorar o próprio processo de informações. Por

exemplo, durante a fase de contextualização, a equipa de informações detecta que certos indicadores-chave de comprometimento (IoCs) não foram inicialmente priorizados pelos sistemas de alerta automatizados. Esta observação é documentada e canalizada para a equipa responsável pelo ajuste dos limiares de sensibilidade do SIEM, o que permite aperfeiçoar os critérios de deteção para futuros casos semelhantes. Finalmente, no final do ciclo, é efectuada uma revisão interna do desempenho do modelo IDEM neste caso específico, avaliando métricas como o tempo de resposta, a precisão das hipóteses iniciais e a utilidade dos produtos gerados. Esta avaliação alimenta uma base de conhecimento interna que permite o ajuste de metodologias, ferramentas e fluxos de trabalho, garantindo que o modelo evolui de forma adaptativa e com base na experiência acumulada.

Esta dinâmica de retrocesso, reformulação e ação simultânea permitida pelo modelo IDEM seria impraticável no modelo clássico do ciclo de inteligência, nem em muitos dos modelos propostos na literatura revista, onde os processos são mais rígidos, lineares e dependentes da iniciativa dos decisores.

5. CONCLUSÕES

A inteligência, entendida como organização, processo, produto e mesmo cultura, desempenha um papel fundamental na gestão da incerteza em ambientes de ameaça voláteis, interligados e cada vez mais híbridos. A sua natureza multidisciplinar e a diversidade de abordagens utilizadas por diferentes países e disciplinas dificultam uma definição única e uma classificação fechada dos seus tipos, mas reflectem também a sua riqueza concetual e a necessidade de cooperação e adaptação constante.

O ciclo clássico da informação, embora valioso na altura por fornecer estrutura e normalização, tem limitações significativas para responder aos desafios contemporâneos, especialmente no domínio digital. A natureza dinâmica e descentralizada do ciberespaço, bem como o volume e a velocidade dos dados, exigem modelos mais flexíveis e adaptáveis. O modelo IDEM proposto neste documento responde a esta necessidade através de uma estrutura modular, não linear e em rede, em que as fases interagem simultaneamente e se retroalimentam constantemente umas às outras.

Esta nova abordagem reorganiza as fases do ciclo tradicional e acrescenta elementos-chave como a identificação proactiva de ameaças, a contextualização integrada com a análise, a divulgação precoce e transversal de informações e a incorporação sistemática de feedback. Integra também tecnologias avançadas, como a inteligência artificial e a aprendizagem automática, para otimizar a gestão de grandes volumes de dados e melhorar as capacidades de previsão.

No entanto, a tecnologia, por si só, não é suficiente. O discernimento humano, a capacidade crítica, a criatividade analítica e o conhecimento contextual continuam a ser essenciais. A sinergia entre os analistas e os sistemas automatizados garante uma informação mais eficiente, exacta e útil para a tomada de decisões.

Em suma, a inteligência do século XXI deve ser ágil, multidisciplinar e colaborativa. Só através de abordagens híbridas, abertas à aprendizagem e à melhoria contínua, será possível antecipar e mitigar eficazmente as ameaças emergentes. O modelo IDEM é um passo nessa direção: uma proposta adaptativa e realista para responder aos desafios que a era digital impõe aos sistemas de intelligence contemporâneos.

A realidade do contexto atual continua a apresentar desafios e dificuldades significativas para antecipar e mitigar eficazmente as ameaças contemporâneas, sobretudo as que se manifestam no ciberespaço, pois é difícil acompanhar e antecipar-se aos cibercriminosos. É, pois, necessário que a comunidade de informações continue a investigar e a desenvolver estratégias que diminuam as actuais fragilidades, promovam a sensibilização para a cultura de informações, a divulgação de informações e a cooperação internacional.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Andric, J., & Terzic, M. (2023). Ciclo de inteligência na luta contra o terrorismo com o uso de dados OSINT. Jornal de Sistemas de Informação e Gestão de Operações, 17(1). https://doi.org/10.1080/2158379X.2021.1879572

Atwood, C. P. (2015). Inteligência baseada em atividades revolucionando a análise de inteligência militar. Joint Force Quarterly, 77. https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/

Budhram, T. (2015). Policiamento baseado em informações: uma abordagem proactiva para combater a corrupção. South African Crime Quarterly, 52. https://doi.org/10.17159/2413-3108/2015/i52a30

Carter, J. G., & Fox, B. (2019). Policiamento comunitário e policiamento liderado por inteligência: um exame da validade convergente ou discriminante. Policing: An International Journal, 42(1), 43-58. https://doi.org/10.1108/PIJPSM-07-2018-0105

Centro Nacional de Criptologia (2015). CCN-STIC-425 Ciclo de Inteligência e Análise de Intrusão.

Centro Nacional de Informações (2023). Origens dos Serviços de Informações. https://www.cni.es/sobre-el-cni/nuestra-historia

Chainey, S., & Chapman, J. (2013). Uma abordagem orientada para o problema para a produção de avaliações de inteligência estratégica. Policing: An International Journal of Police Strategies & Management, 36(3), 474-490. https://doi.org/10.1108/PIJPSM-02-2012-0012

Dahj, J. N. M. (2022). Dominando a inteligência cibernética. Packt Publishing Ltd.

Díaz Fernández, A. M. (2013). O papel da inteligência estratégica no mundo atual. Cuadernos de Estrategia, 162, 35-66. https://dialnet.unirioja.es/servlet/articulo?codigo=4275959

Francisco, J., & Barrilao, S. (2019). Serviços de inteligência, sigilo e garantia judicial de direitos. Teoría y Realidad Constitucional, 309-340.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. Digital, 2, 143-163. https://doi.org/10.3390/digital2020009

Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).

Gruszczak, A. (2018). O desafio da adaptação das informações da NATO. https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge

Jefatura del Estado (2002). Lei 11/2002, de 6 de maio, que regula o Centro Nacional de Informações.

Jiménez Villalonga, R. (2018, 26 de novembro). Tipos de inteligência. https://global-strategy.org/tipos-de-inteligencia/

Jordán, J. (2011). Introdução à análise de inteligência. 2340-8421, 2, Art. 2. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2016). Uma revisão do Ciclo de Inteligência. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. https://www.seguridadinternacional.es/resi/index.php/revista

Kamiński, M. A. (2019). Fontes de Inteligência no Processo de Coleta de Informações pela Comunidade de Inteligência dos EUA. Security Dimensions, 32(32), 82-105. https://doi.org/10.5604/01.3001.0014.0988

Knight, T. C. (2024). Five Thousand Candles: Optimizing Information Sharing Policies for Homeland Security Uma dissertação. Sistema Universitário Público Americano.

Lee, M. (2023). Cyber Threat Intelligence (1ª ed.), John Wiley & Sons, Inc.

Mahood, L. M. E. K. (2015). SOCMINT: seguindo e gostando de inteligência de mídia social [Canadian Forces College]. https://www.cfc.forces.gc.ca/254-eng.html

Ministério da Defesa (2023). Informações, vigilância e reconhecimento.

Montero Gómez, A. (2006). Inteligencia Prospetiva de Seguridad (24; Área: Segurança e Defesa). https://www.realinstitutoelcano.org/publicaciones/

Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51-66. https://dialnet.unirioja.es/servlet/articulo?codigo=2270935

Navarro Bonilla, D. (2005). Informação, espionagem e inteligência na monarquia hispânica (séculos XVI-XVII). Revista de Historia Militar, Extraordinario, 13-40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075

Organização para a Segurança e a Cooperação na Europa (2017). Guia da OSCE sobre policiamento baseado em informações (Unidade de Assuntos de Polícia Estratégica do Departamento de Ameaças Transnacionais, Ed.; Vol. 13).

Payá-Santos, C. A. (2023). O desempenho da inteligência em Espanha nos âmbitos público, empresarial e académico. Revista Científica General José María Córdova, 21(44), 1029-1047. https://doi.org/10.21830/19006586.1222

Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). Compreendendo o Ciclo da Inteligência (M. Phythian, Ed.).

Portillo, I. (2019). Saber o que é Cyber Intelligence e Cyber Threat Intelligence. https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

Pothoven, S., Rietjens, S., & de Werd, P. (2023). Paradigmas produtor-cliente para inteligência de defesa. Estudos de Defesa, 23(1), 68-85. https://doi.org/10.1080/14702436.2022.2089658

Stewart Bertram (2015). O Tao da Inteligência de Código Aberto. IT Governance Publishing.

Summers, L., & Rossmo, D. K. (2019). Entrevistas de infractores: implicações para o policiamento baseado em informações. Policing, 42(1), 31-42. https://doi.org/10.1108/PIJPSM-07-2018-0096

Vela Tejada, J. (1993). Tradição e originalidade na obra de Eneias, o Tático: A génese da historiografia militar. Minerva. Revista de Filología Clásica, 7, 79-92. https://doi.org/https://doi.org/10.24197/mrfc.7.1993