

## Artigos Dossiê

# A intelligence como fator de prevenção da guerra híbrida

Intelligence as a factor in the prevention of hybrid warfare

Ricardo Caiado<sup>1</sup> 

<sup>1</sup>Instituto Universitário de Lisboa , Lisboa, Portugal

## Resumo

A transformação tecnológica dos conflitos contemporâneos tornou mais difícil distinguir paz, crise, coerção e guerra. A guerra híbrida combina instrumentos militares e não militares, explícitos e encobertos, convencionais e não convencionais, explorando vulnerabilidades políticas, sociais, económicas, tecnológicas e informacionais. Neste contexto, este artigo analisa a intelligence como capacidade preventiva, procurando responder à questão: em que medida a produção e a disseminação oportuna de conhecimento podem reduzir a probabilidade de êxito de uma campanha híbrida e contribuir para impedir a sua escalada? Defende-se que a intelligence não constitui apenas um instrumento de deteção de ameaças, mas uma capacidade estratégica de antecipação, diagnóstico de vulnerabilidades, construção de alerta precoce, apoio à decisão e coordenação de respostas. A investigação adota uma abordagem qualitativa, baseada em revisão de literatura especializada, análise documental e estudo comparativo de orientações recentes da NATO, União Europeia e organizações internacionais, complementada pela análise das implicações para Estados do Sul Global. Sustenta-se que, em ambientes híbridos, a prevenção depende menos da existência de informação em abundância do que da capacidade de transformar sinais dispersos em conhecimento acionável, partilhá-lo entre instituições e convertê-lo em resiliência. O artigo conclui que a intelligence pode funcionar como fator de prevenção da guerra híbrida quando integrada numa arquitetura de segurança de toda a sociedade, tecnologicamente capacitada, juridicamente controlada e adaptada às especificidades políticas e institucionais do Sul Global.

**Palavras-chave:** *Intelligence*; Guerra híbrida; Alerta precoce; Prevenção; Sul Global

## Abstract

---

The technological transformation of contemporary conflicts has made it increasingly difficult to distinguish peace, crisis, coercion and war. Hybrid warfare combines military and non-military, overt and covert, conventional and unconventional means, while exploiting political, social, economic, technological and informational vulnerabilities. This article examines intelligence as a preventive capability and asks to what extent timely intelligence production and dissemination can reduce the likelihood of success of a hybrid campaign and contribute to preventing escalation. It argues that intelligence is not merely a tool for threat detection, but a strategic capability for anticipation, vulnerability assessment, early warning, decision support and response coordination. The research adopts a qualitative approach based on a review of specialized literature, documentary analysis and a comparative assessment of recent NATO, European Union and international policy documents, complemented by an analysis of implications for Global South states. The article argues that prevention in hybrid environments depends less on the availability of information than on the ability to transform dispersed signals into actionable knowledge, share it across institutions and convert it into resilience. It concludes that intelligence can become a factor of hybrid warfare prevention when embedded in a whole-of-society security architecture that is technologically enabled, legally constrained and adapted to the political and institutional specificities of the Global South.

**Keywords:** Intelligence; Hybrid warfare; Early warning; Prevention; Global South

## 1 INTRODUÇÃO

A guerra deixou de ser compreendida adequadamente através de uma oposição rígida entre guerra e paz, ou entre meios militares e não militares. A competição estratégica contemporânea desenvolve-se num espaço intermédio em que operações de influência, ciberataques, sabotagem, coerção económica, manipulação informacional, pressão política e instrumentos militares podem ser utilizados de forma articulada, muitas vezes sem que o Estado-alvo consiga determinar imediatamente a natureza, a autoria ou a finalidade da ação. A União Europeia descreve as ameaças híbridas como atividades coordenadas e maliciosas que podem combinar manipulação da informação, ciberataques, coerção económica, manobras políticas encobertas, diplomacia coerciva e ameaça de força militar, frequentemente procurando permanecer abaixo do limiar percebido de guerra (CONSELHO DA UNIÃO EUROPEIA, 2026).

O fenómeno é particularmente relevante para o Sul Global. Estados com capacidades institucionais, tecnológicas e financeiras limitadas podem apresentar

maior exposição a vulnerabilidades que atravessam simultaneamente o espaço político, económico, social, informacional e digital. A expansão da conectividade, a dependência de infraestruturas digitais e a crescente centralidade das plataformas informacionais criam oportunidades de desenvolvimento, mas também novas superfícies de exploração. Estudos recentes sobre África mostram que ameaças híbridas podem explorar fragilidades de governação, desigualdades socioeconómicas, défices de segurança e polarização social, combinando desinformação, ciberoperações, coerção económica e violência armada (ACCORD, 2026).

Neste ambiente, a intelligence adquire uma função que ultrapassa a recolha de informação sobre um adversário. A sua finalidade estratégica consiste em reduzir a incerteza relevante para a decisão, identificar padrões, avaliar intenções e capacidades, antecipar cenários e fornecer aos decisores conhecimento suficientemente oportuno para permitir ação preventiva. A formulação clássica de KENT (1951) permanece particularmente útil: intelligence é uma forma especializada de conhecimento destinada a apoiar as decisões de mais alto nível.

Este artigo pergunta: em que medida a intelligence pode funcionar como fator de prevenção da guerra híbrida? Defende-se que a intelligence constitui uma capacidade preventiva decisiva quando consegue converter sinais dispersos em conhecimento acionável, antecipar a combinação de instrumentos empregues pelo adversário, identificar vulnerabilidades críticas e fornecer alerta precoce que permita ativar mecanismos diplomáticos, políticos, económicos, cibernéticos, policiais e militares antes que a campanha híbrida alcance efeitos estratégicos irreversíveis.

Metodologicamente, o estudo adota uma abordagem qualitativa, de natureza analítico-documental. Parte da literatura clássica sobre intelligence e guerra híbrida e atualiza-a através de documentos institucionais recentes da NATO, União Europeia e outras organizações, bem como de literatura académica contemporânea sobre a relação entre intelligence, alerta precoce e ameaças híbridas. A análise é projetada para o contexto do Sul Global, onde a prevenção deve ser pensada em articulação com autonomia tecnológica, cooperação regional, resiliência social e redução de dependências externas.

## **2 INTELLIGENCE E GUERRA HÍBRIDA: DA INFORMAÇÃO AO CONHECIMENTO ESTRATÉGICO**

A distinção entre informação e intelligence é fundamental. Informação corresponde a dados, factos ou sinais suscetíveis de utilização; intelligence resulta do processo de seleção, validação, contextualização, análise e interpretação orientado para uma necessidade de decisão. Esta distinção, presente em KENT (1951) e desenvolvida por HERMAN (2001) e LOWENTHAL (2022), impede que a acumulação de dados seja confundida com conhecimento estratégico.

A inteligência contemporânea pode ser compreendida simultaneamente como produto, processo e organização. Como produto, é conhecimento destinado a um utilizador; como processo, compreende direção, recolha, processamento, análise, disseminação e retroalimentação; como organização, envolve estruturas especializadas que produzem e protegem esse conhecimento. A tradição analítica de KENT (1951) permanece relevante porque integra estas três dimensões.

No contexto híbrido, esta arquitetura torna-se mais complexa. O adversário pode produzir sinais deliberadamente contraditórios, utilizar intermediários, explorar atores legítimos, recorrer a campanhas de influência e combinar ações com diferentes ritmos temporais. Uma campanha pode começar com manipulação informacional, evoluir para ciberespionagem, passar para sabotagem de infraestrutura e culminar em coerção política ou militar. A análise isolada de cada incidente tende, por isso, a subestimar a natureza estratégica do conjunto.

NILSSON, WEISSMANN e PALMERTZ (2025) sublinham que as ameaças híbridas exigem compreender a interação entre os atores de intelligence e os atores sociais responsáveis por formular respostas e construir resiliência. A intelligence deixa, assim, de ser atividade exclusivamente interna dos serviços de informações e passa a integrar uma arquitetura de conhecimento estratégico que envolve instituições públicas, forças armadas, polícia, entidades reguladoras, operadores de infraestruturas críticas, academia e setor privado.

---

## 2.1 Estado da arte: intelligence, alerta precoce e ameaças híbridas

A literatura contemporânea converge em três ideias que são particularmente relevantes para este estudo. Primeiro, as ameaças híbridas são caracterizadas pela combinação de instrumentos e pela exploração deliberada das zonas cinzentas entre competição, coerção e conflito. Segundo, a intelligence enfrenta um ambiente em que a velocidade de circulação da informação é superior à capacidade institucional de a validar e interpretar. Terceiro, a prevenção depende da ligação entre análise e resposta: produzir conhecimento sem mecanismos capazes de o transformar em decisão, preparação e resiliência reduz significativamente o seu valor estratégico.

A abordagem clássica de KENT (1951) permanece útil ao compreender a intelligence como conhecimento necessário para formular e executar políticas de segurança. HERMAN (2001) acrescenta a dimensão organizacional e informacional, enquanto LOWENTHAL (2022) evidencia a relação entre produção de intelligence e decisão política. No contexto contemporâneo, contudo, o problema já não é apenas obter informação secreta. A expansão de fontes abertas, plataformas digitais, sensores, imagens, dados económicos e comunicações produz um ambiente de abundância informacional no qual a capacidade de seleção, validação e contextualização passa a ser tão importante quanto a capacidade de recolha.

No domínio das ameaças híbridas, NILSSON, WEISSMANN e PALMERTZ (2025) demonstram a necessidade de uma interação mais estreita entre comunidades de intelligence e atores sociais responsáveis por construir respostas e resiliência. Esta perspetiva permite ultrapassar uma conceção excessivamente fechada da intelligence. A prevenção de uma campanha híbrida exige conhecimento partilhado entre estruturas de defesa, segurança, diplomacia, proteção civil, cibersegurança, operadores de infraestruturas críticas e, em determinadas circunstâncias, setor privado e sociedade civil.

O estado da arte revela, portanto, uma lacuna analítica que este artigo procura explorar: a intelligence é frequentemente estudada como função de apoio à decisão

ou como instrumento de segurança nacional, enquanto a prevenção da guerra híbrida exige analisá-la como uma capacidade sistêmica que liga detecção, interpretação, alerta, decisão, resposta e aprendizagem. A contribuição deste estudo consiste precisamente em deslocar o centro da análise do produto de intelligence para a cadeia institucional que transforma conhecimento em prevenção.

### **3 OS MECANISMOS PREVENTIVOS DA INTELLIGENCE**

#### **3.1 Delimitação analítica e critérios de análise**

A análise foi organizada segundo quatro dimensões. A primeira é epistemológica e procura determinar como a intelligence reduz incerteza num ambiente caracterizado por informação incompleta, engano e ambiguidade. A segunda é institucional e examina a articulação entre serviços, decisores e organizações responsáveis pela resposta. A terceira é tecnológica e considera o impacto da inteligência artificial, da análise de dados e das fontes digitais sobre a produção de conhecimento. A quarta é político-estratégica e avalia as implicações da prevenção para soberania, resiliência, autonomia e controlo democrático.

Durante a investigação foram privilegiadas fontes académicas e institucionais que permitem articular fundamentos clássicos da intelligence com desenvolvimentos recentes sobre ameaças híbridas. A análise documental de documentos da NATO e da União Europeia é utilizada como evidência da evolução das políticas de prevenção e resiliência, enquanto a literatura especializada permite problematizar os pressupostos e limites dessas abordagens. Não se pretende medir estatisticamente a eficácia de um serviço de intelligence específico, mas construir um modelo concetual suscetível de orientar investigação empírica futura.

#### **3.2 Alerta precoce e antecipação estratégica**

O primeiro mecanismo preventivo é o alerta precoce. A sua função consiste em identificar mudanças relevantes no ambiente estratégico antes de estas se

transformarem em crise. Não se trata de prever o futuro de forma determinista, mas de construir indicadores, cenários e hipóteses que permitam ao decisor reconhecer trajetórias de risco.

A NATO inclui atualmente sistemas de alerta precoce, indicadores e strategic foresight entre as prioridades relacionadas com segurança, ao lado de ferramentas para monitorizar e analisar atividades maliciosas no espaço informacional (NATO, 2026). Esta orientação confirma uma transformação importante: o alerta deixa de depender exclusivamente de fontes secretas e passa a resultar da integração de OSINT, SIGINT, HUMINT, IMINT, dados cibernéticos, indicadores económicos e análise de redes.

Em termos preventivos, o alerta deve responder a cinco perguntas: o que está a mudar; por que está a mudar; quem beneficia da mudança; quais as vulnerabilidades exploradas; e que evolução é plausível se não houver intervenção. A resposta permite transformar o ciclo de intelligence num ciclo de prevenção.

### 3.3 Identificação de vulnerabilidades e preparação do Estado

A segunda função consiste em identificar as vulnerabilidades que tornam um Estado suscetível a campanhas híbridas. O adversário não necessita necessariamente de possuir superioridade militar; pode explorar dependências e fragilidades preexistentes. Entre elas encontram-se dependências tecnológicas externas, concentração de cadeias de abastecimento, fragilidade de infraestruturas críticas, polarização social, baixa confiança institucional, insuficiente literacia mediática e digital e reduzida capacidade de coordenação.

A intelligence contribui para a prevenção quando deixa de olhar apenas para as capacidades do adversário e passa a analisar a relação entre capacidade, intenção, oportunidade e vulnerabilidade do alvo. A análise deve ser dinâmica: aquilo que hoje constitui fragilidade pode amanhã deixar de existir, enquanto uma nova dependência pode surgir em consequência da transformação tecnológica.

### **3.4 Atribuição, avaliação e decisão**

A atribuição é uma das maiores dificuldades das ameaças híbridas. A utilização de proxies, infraestruturas comprometidas, empresas de fachada, plataformas digitais e operações de influência dificulta a determinação de autoria. A intelligence deve trabalhar com graus de confiança e não apenas com afirmações binárias. Uma avaliação profissional distingue facto observado, inferência analítica, hipótese concorrente e juízo de confiança.

Uma atribuição errada pode desencadear escalada desnecessária. Em sentido inverso, excessiva prudência pode impedir medidas preventivas. A qualidade da intelligence reside, portanto, na capacidade de explicitar a incerteza sem paralisar a decisão.

### **3.5 Intelligence e decisão política: proximidade sem instrumentalização**

A intelligence tem relação estruturalmente próxima com o poder político, porque é produzida para apoiar decisões. Essa proximidade constitui condição de utilidade e risco. Se se afastar demasiado do decisor, pode produzir conhecimento irrelevante; se se aproximar excessivamente, pode adaptar a análise às preferências políticas.

A prevenção torna este problema sensível porque os juízos de intelligence podem ser utilizados para justificar medidas extraordinárias, restrições de direitos ou respostas coercivas. A independência analítica, a separação entre avaliação e decisão e o controlo democrático são, portanto, componentes da própria eficácia preventiva.

## **4 O CICLO DE INTELLIGENCE COMO CICLO DE PREVENÇÃO**

O ciclo clássico de intelligence é normalmente apresentado através de cinco etapas: direção e planeamento, recolha, processamento, análise e produção, e disseminação. Esta representação é útil, mas insuficiente para explicar a prevenção de ameaças híbridas. Em ambientes complexos, a produção deve ser concebida como processo interativo, em que a utilização do produto e o feedback geram novos requisitos.

Nestes termos, propõe-se interpretar o ciclo de intelligence como um ciclo de prevenção composto por seis momentos: (1) definição de necessidades estratégicas; (2) recolha multidomínio; (3) fusão e validação; (4) análise de indicadores e cenários; (5) alerta e decisão; e (6) avaliação da resposta e aprendizagem.

No primeiro momento, o decisor define o que necessita de saber. No segundo, a recolha combina disciplinas e fontes. No terceiro, informação proveniente de diferentes comunidades é integrada e confrontada. No quarto, os analistas produzem hipóteses, indicadores e cenários. No quinto, o produto chega aos responsáveis por decisões políticas, diplomáticas, económicas, policiais, militares e tecnológicas. No sexto, avalia-se se a resposta reduziu a vulnerabilidade e se novos indicadores exigem alteração do diagnóstico.

Esta última etapa é essencial. Uma intelligence orientada para a prevenção não termina na disseminação do relatório. O sucesso mede-se pela capacidade de gerar aprendizagem institucional e melhorar a preparação futura. O ciclo deixa de ser linear e transforma-se num sistema adaptativo.

Por sua vez, a inteligência artificial, a aprendizagem automática e o processamento de linguagem natural podem acelerar a identificação de padrões, detetar anomalias e apoiar a monitorização de redes. Todavia, a tecnologia não substitui o julgamento analítico. Os sistemas automatizados podem reproduzir vieses, gerar falsos positivos e ser manipulados. A inteligência artificial deve ser tratada como multiplicador de capacidade, não como substituto da análise humana.

#### **4.1 Intelligence tecnológica, ia e fusão de dados**

A transformação tecnológica altera não apenas a quantidade de informação disponível, mas também a natureza do trabalho analítico. Os sistemas de inteligência artificial podem apoiar a classificação de grandes volumes de documentos, a identificação de relações entre entidades, a deteção de anomalias e o acompanhamento de tendências. A aprendizagem automática pode contribuir para identificar alterações

de comportamento em redes digitais ou infraestruturas, enquanto técnicas de processamento de linguagem natural permitem analisar grandes conjuntos de textos, mensagens públicas e fontes abertas. O ganho potencial está na capacidade de reduzir o tempo entre recolha e interpretação.

Todavia, a aceleração tecnológica introduz uma distinção essencial entre deteção e conhecimento. Um sistema pode detetar uma anomalia sem conseguir explicar a sua causa; pode identificar uma alteração estatística sem saber se ela resulta de uma campanha hostil, de um acontecimento normal ou de uma mudança no comportamento dos utilizadores. Por isso, a automação deve ser integrada numa cadeia de validação humana. A tecnologia amplia a capacidade sensorial e computacional da intelligence, mas não elimina a necessidade de contextualização, formulação de hipóteses concorrentes e avaliação de incerteza.

Por outro lado, existe ainda uma dimensão adversarial. As mesmas tecnologias que fortalecem a capacidade defensiva podem ser utilizadas pelo adversário para produzir deepfakes, perfis sintéticos, operações de influência automatizadas, ataques cibernéticos adaptativos e grandes volumes de informação enganosa. A vantagem tecnológica, portanto, é relativa e dinâmica. A intelligence preventiva deve avaliar não apenas a capacidade própria, mas também a possibilidade de o adversário utilizar tecnologia para degradar a qualidade dos dados, manipular indicadores ou induzir os analistas a conclusões erradas.

## **5 INTELLIGENCE, GUERRA HÍBRIDA E RESILIÊNCIA NO SUL GLOBAL**

O enquadramento do Sul Global exige evitar a simples transferência de modelos institucionais concebidos para Estados com capacidades materiais muito diferentes. A questão central não é reproduzir integralmente as arquiteturas de intelligence de grandes potências, mas construir capacidades proporcionais às vulnerabilidades nacionais e regionais.

Em África, as ameaças híbridas podem explorar fragilidades de governação,

conflitos locais, desigualdades, dependência económica e insuficiência de capacidades digitais. A análise do ACCORD (2026) destaca a combinação entre ciberoperações, desinformação, coerção económica e insurgência, bem como limitações de coordenação e partilha de intelligence entre mecanismos regionais. O problema é, portanto, institucional e político, além de tecnológico.

O European Union Institute for Security Studies alertou para o crescimento de ameaças híbridas em África e para a dificuldade de deteção quando diferentes instrumentos são utilizados simultaneamente e os seus efeitos apenas se tornam claros numa fase posterior. Uma resposta consiste em monitorizar sistematicamente atividades híbridas noutras regiões, permitindo reconhecer padrões e antecipar a sua adaptação a novos contextos (EUISS, 2022).

Para o Sul Global, a cooperação regional pode funcionar como multiplicador de intelligence. Nenhum Estado necessita dominar todas as disciplinas; pode construir capacidades complementares através de redes de partilha, centros regionais de análise, mecanismos conjuntos de alerta e protocolos de proteção de infraestruturas críticas.

A autonomia tecnológica deve integrar esta estratégia. A dependência excessiva de fornecedores externos pode criar novas vulnerabilidades, nomeadamente quando sistemas críticos, serviços de cloud, sensores, plataformas de comunicação ou ferramentas de análise são controlados fora da jurisdição nacional. A prevenção exige combinar cooperação internacional com capacidade nacional mínima para compreender, validar e proteger os próprios sistemas.

O caso brasileiro oferece uma ilustração da necessidade de estudar a guerra híbrida a partir das especificidades do Sul Global. Trabalho recente da Escola de Guerra Naval identifica a interação entre tecnologias de informação, desinformação, polarização, ciberoperações e disputas geopolíticas no Brasil (SOARES, 2025). O valor deste tipo de estudo está em desenvolver capacidades nacionais de análise crítica das vulnerabilidades e dos padrões de influência.

No plano africano, a intelligence regional enfrenta ainda a coexistência de ameaças híbridas com terrorismo, criminalidade transnacional, insurgência, fragilidade institucional e conflitos por recursos. A separação rígida entre intelligence militar, policial, económica e política pode reduzir a eficácia preventiva. A arquitetura deve favorecer a fusão de conhecimento, respeitando as competências legais de cada entidade.

## **6 OS LIMITES DA INTELLIGENCE COMO INSTRUMENTO PREVENTIVO**

A primeira limitação é epistemológica. A intelligence trabalha com informação incompleta e adversários que procuram negar, manipular ou enganar. Não existe garantia de previsão. A prevenção deve, portanto, ser concebida em termos probabilísticos e de gestão de riscos.

A segunda limitação é organizacional. Os serviços podem sofrer de compartimentação, competição burocrática, excesso de informação e insuficiente partilha. A existência de várias fontes não garante melhor intelligence se os sistemas não conseguirem integrar e interpretar os dados.

A terceira limitação é tecnológica. A inteligência artificial aumenta a capacidade de processamento, mas também permite gerar conteúdos sintéticos, falsos perfis, deepfakes e campanhas personalizadas em grande escala.

A quarta limitação é política. A intelligence pode ser politizada quando a análise é pressionada para confirmar uma decisão já tomada. A prevenção perde eficácia quando o decisor seleciona apenas informações que sustentam a sua preferência.

A quinta limitação é jurídica e democrática. A recolha preventiva pode interferir com privacidade, proteção de dados, liberdade de expressão e outros direitos fundamentais. A prevenção não pode ser concebida como suspensão da legalidade; quanto maior o poder intrusivo das capacidades de intelligence, maior deve ser a exigência de controlo judicial, parlamentar e institucional.

A sexta limitação é a dependência externa. Estados do Sul Global podem depender de parceiros para sensores, satélites, plataformas digitais, software de

análise e informação estratégica. A cooperação deve ser acompanhada de transferência de conhecimento, formação e desenvolvimento de capacidades endógenas. Nesta perspectiva, atente-se para o Quadro 1.

Quadro 1 - Funções preventivas da *intelligence*: perguntas centrais, produtos esperados e riscos de falha

| Função preventiva | Pergunta central                        | Produto esperado                   | Risco de falha                             |
|-------------------|-----------------------------------------|------------------------------------|--------------------------------------------|
| Deteção           | Que sinais relevantes estão a surgir?   | Indicadores e sinais priorizados   | Ruído e excesso de informação              |
| Interpretação     | O que significam os sinais em contexto? | Hipóteses e avaliação de cenários  | Viés analítico ou leitura isolada          |
| Antecipação       | Que evolução é plausível?               | Alerta precoce e cenários          | Falsa certeza ou atraso                    |
| Ativação          | Que decisão preventiva é necessária?    | Opções para o decisor              | Desligamento entre intelligence e política |
| Resiliência       | Como reduzir a vulnerabilidade?         | Preparação e proteção              | Conhecimento sem capacidade de resposta    |
| Aprendizagem      | O que foi aprendido?                    | Revisão de indicadores e processos | Repetição de erros                         |

Fonte: Autor (2026)

## 6.1 Capacidade, autonomia e cooperação no Sul Global

A discussão sobre intelligence preventiva no Sul Global deve evitar dois extremos: assumir que estes Estados são apenas recetores de tecnologia ou presumir que modelos concebidos em grandes potências podem ser replicados sem adaptação. A construção de capacidade exige identificar necessidades próprias, estabelecer prioridades e combinar recursos nacionais com cooperação externa. A questão estratégica é transformar cooperação em capacidade duradoura, e não apenas em dependência de sistemas, dados ou fornecedores.

A autonomia, neste contexto, deve ser entendida como autonomia relativa e seletiva. Poucos Estados conseguem dominar simultaneamente satélites, sensores, ciberinteligência, análise avançada, computação de alto desempenho e produção de

software. Contudo, é possível desenvolver competências nacionais em áreas críticas, estabelecer padrões de interoperabilidade, formar analistas, manter capacidade de auditoria e preservar controlo sobre os dados estratégicos. A cooperação Sul-Sul pode ainda permitir partilha de experiências e construção de soluções adaptadas a ambientes institucionais semelhantes.

No caso africano, a prevenção deve ser analisada em conexão com conflitos locais, terrorismo, criminalidade transnacional, vulnerabilidades económicas e fragilidades institucionais. O desafio consiste em construir mecanismos de alerta que consigam integrar sinais de segurança, económicos, sociais e digitais sem reduzir problemas políticos complexos a indicadores exclusivamente tecnológicos. A intelligence regional pode ser particularmente importante quando ameaças e redes ultrapassam fronteiras nacionais.

O caso brasileiro, por sua dimensão territorial e capacidade tecnológica relativa no contexto regional, oferece igualmente um espaço relevante para investigação futura sobre intelligence, guerra híbrida e soberania cognitiva. Mais do que apresentar o Brasil como modelo, importa utilizá-lo como exemplo de que capacidades tecnológicas só adquirem valor estratégico quando articuladas com instituições, doutrina, recursos humanos e objetivos nacionais.

## **7 DISCUSSÃO: UM MODELO DE INTELLIGENCE PREVENTIVA DA GUERRA HÍBRIDA**

A análise permite propor um modelo concetual em que a intelligence preventiva atua através de cinco funções interdependentes: deteção, interpretação, antecipação, ativação e aprendizagem.

A primeira função consiste na identificação de sinais relevantes em múltiplos domínios. A segunda procura estabelecer relações entre sinais e distinguir eventos isolados de campanhas coordenadas. A terceira transforma a avaliação em cenários e indicadores de alerta. A quarta conecta o conhecimento às opções de resposta:

diplomacia, comunicação estratégica, ciberdefesa, proteção de infraestruturas, medidas económicas, investigação criminal ou defesa militar. A quinta avalia os efeitos da resposta e atualiza o modelo de ameaça.

Este modelo desloca a discussão de uma visão passiva da intelligence para uma visão de capacidade preventiva. O valor não reside apenas na qualidade do relatório, mas na sua capacidade de alterar o comportamento do Estado antes de o adversário alcançar o seu objetivo.

Há, contudo, uma condição essencial: a intelligence preventiva deve estar integrada numa arquitetura de resiliência. Um Estado pode saber que uma infraestrutura está vulnerável e ser incapaz de a proteger. Pode identificar uma campanha de desinformação e não possuir mecanismos credíveis de comunicação pública. Pode atribuir um ciberataque e não possuir instrumentos diplomáticos ou económicos para responder. O conhecimento é condição necessária, mas não suficiente.

A prevenção da guerra híbrida deve, por isso, ser compreendida como uma cadeia: *intelligence* → alerta → decisão → resposta → resiliência → aprendizagem. Se qualquer elo falhar, a vantagem informacional pode não se converter em vantagem estratégica.

A experiência recente da NATO e da União Europeia confirma esta tendência. A NATO identifica uma estrutura de análise híbrida no âmbito da Joint Intelligence and Security Division, enquanto a UE desenvolveu um Hybrid Toolbox orientado para identificar campanhas complexas e coordenar respostas transeitoriais. Em março de 2026, o Conselho da UE reforçou a dimensão preventiva e de dissuasão da política contra ameaças híbridas (NATO, 2026; CONSELHO DA UNIÃO EUROPEIA, 2026).

Para o Sul Global, a principal conclusão é que a intelligence preventiva deve ser construída com base na realidade local. A prioridade não deve ser adquirir indiscriminadamente tecnologias sofisticadas, mas definir necessidades estratégicas, criar capacidade analítica, integrar fontes, desenvolver mecanismos de alerta e assegurar canais de decisão.

## 7.1 Governança, atribuição e controlo democrático

A prevenção da guerra híbrida envolve uma tensão inevitável entre necessidade de antecipação e necessidade de contenção. Quanto maior a pressão para identificar ameaças antes de se materializarem, maior pode ser a tentação de ampliar a recolha de dados e reduzir os limiares de intervenção. Uma intelligence preventiva legítima deve, por isso, distinguir claramente recolha, análise, avaliação e decisão. A identificação de um padrão de risco não equivale à demonstração de responsabilidade de um ator.

A atribuição constitui um caso paradigmático. Em ambientes híbridos, um ataque pode ser executado através de infraestruturas comprometidas, intermediários ou atores com diferentes graus de autonomia. A atribuição deve ser apresentada como avaliação graduada de confiança, acompanhada das evidências e incertezas relevantes. Esta abordagem reduz o risco de transformar uma hipótese analítica numa certeza política e permite calibrar a resposta de acordo com o grau de confiança disponível.

O controlo democrático também é essencial porque medidas preventivas podem envolver informação sensível, vigilância, proteção de infraestruturas e cooperação entre entidades públicas e privadas. O segredo operacional não deve eliminar mecanismos de supervisão institucional. A responsabilização pode assumir diferentes formas — parlamentar, judicial, administrativa ou independente — desde que exista capacidade efetiva para verificar legalidade, proporcionalidade e respeito pelos direitos fundamentais.

A experiência recente da União Europeia reforça a ideia de que a prevenção deve integrar instrumentos de proteção de infraestruturas críticas, defesa de processos democráticos, combate à manipulação de informação, cooperação internacional e medidas de dissuasão. As conclusões do Conselho de 16 de março de 2026 evidenciam precisamente uma abordagem que combina prevenção, dissuasão, resposta e resiliência, em vez de tratar as ameaças híbridas como problema exclusivamente militar (CONSELHO DA UNIÃO EUROPEIA, 2026).

---

## 7.2 Limitações e agenda de investigação

A principal limitação deste artigo é a sua natureza teórico-documental. O modelo proposto não foi testado através de estudo de caso ou indicadores quantitativos de desempenho. A sua utilidade deve, portanto, ser entendida como analítica: oferece categorias para orientar investigação empírica posterior. Os estudos futuros poderão comparar mecanismos de alerta precoce em diferentes Estados, avaliar a qualidade das previsões e examinar a relação entre intelligence e decisões efetivamente tomadas.

Uma segunda agenda de investigação deverá estudar a dimensão tecnológica de forma mais sistemática, uma vez que é necessário avaliar como sistemas de IA, análise de redes, processamento de linguagem natural e fontes abertas alteram o trabalho dos analistas e quais os novos erros introduzidos pela automação. Também será relevante estudar como atores adversários exploram modelos algorítmicos para produzir informação enganosa ou manipular indicadores.

Por fim, o Sul Global requer maior presença na produção de conhecimento sobre intelligence e guerra híbrida. A investigação comparada poderá contribuir para identificar modelos de cooperação, formas de autonomia tecnológica e soluções institucionais ajustadas a diferentes capacidades estatais. Esta agenda evita que o Sul Global seja tratado apenas como espaço de aplicação de conceitos desenvolvidos noutros contextos.

## 8 CONCLUSÃO

A guerra híbrida desloca parte significativa da competição para espaços nos quais os Estados possuem dificuldades de deteção, atribuição e resposta. A combinação de ciberoperações, desinformação, coerção económica, sabotagem, operações de influência e instrumentos militares permite explorar vulnerabilidades de forma gradual e ambígua.

Neste contexto, a intelligence assume função preventiva central. O seu principal

contributo não consiste simplesmente em saber mais sobre o adversário, mas em reduzir a incerteza relevante para a decisão. Quando corretamente orientada, permite identificar sinais precoces, compreender padrões, avaliar capacidades e intenções, localizar vulnerabilidades, construir cenários e ativar respostas antes de a campanha híbrida produzir efeitos estratégicos irreversíveis.

O argumento desenvolvido demonstra, contudo, que intelligence e prevenção não são conceitos equivalentes. A intelligence só produz prevenção quando existe ligação efetiva entre conhecimento e decisão. É necessário que o alerta seja oportuno, que os decisores estejam preparados para o utilizar, que existam instrumentos de resposta e que as instituições consigam aprender com os resultados.

No Sul Global, esta questão adquire particular relevância. A exposição a dependências tecnológicas, fragilidades institucionais, desigualdades sociais e conflitos transnacionais pode aumentar a vulnerabilidade às campanhas híbridas. Ao mesmo tempo, a cooperação regional e internacional pode reduzir custos e aumentar a capacidade de alerta. A prioridade estratégica deve ser construir autonomia suficiente para compreender e proteger o próprio ambiente de segurança, sem rejeitar a cooperação externa.

A investigação efetuada conclui que a intelligence pode ser considerada fator de prevenção da guerra híbrida em quatro condições: quando é multidomínio e integra fontes diversas; quando possui orientação prospetiva e sistemas de alerta precoce; quando está ligada a mecanismos de decisão e resposta; e quando opera sob controlo jurídico e democrático.

A principal contribuição do artigo é propor que a intelligence seja entendida como infraestrutura de prevenção e não apenas como instrumento de informação. A prevenção começa antes do ataque visível: começa na capacidade de reconhecer a combinação de sinais, compreender vulnerabilidades e transformar conhecimento em preparação. Num ambiente estratégico em que o adversário procura vencer sem declarar guerra, conhecer antes de reagir constitui uma das formas mais relevantes de defesa.

---

## REFERÊNCIAS

- ACCORD. **How can regional security mechanisms in Africa effectively address emerging hybrid threats?** 25 mar. 2026. Disponível em: <https://www.accord.org.za/analysis/how-can-regional-security-mechanisms-in-africa-effectively-address-emerging-hybrid-threats/>. Acesso em: 2 set. 2026.
- ALVES, Artur. **A prevenção e o combate às ameaças híbridas**: impacto para as Forças Armadas Portuguesas. Pedrouços: Instituto Universitário Militar, 2020.
- BRANTLY, Aaron. **The decision to attack**: military and intelligence cyber decision-making. Athens: University of Georgia Press, 2016.
- CEPIK, Marco. Inteligência. In: SAINT-PIERRE, Héctor; VITELLI, Marina (org.). **Dicionário de segurança e defesa**. São Paulo: Editora UNESP, 2018. p. 725-729.
- CONSELHO DA UNIÃO EUROPEIA. **Ameaças híbridas**. Bruxelas, 2026. Disponível em: <https://www.consilium.europa.eu/pt/policies/hybrid-threats/>. Acesso em: 2 set. 2026.
- CONSELHO DA UNIÃO EUROPEIA. **Conselho adota conclusões sobre o reforço da capacidade da UE para combater as ameaças híbridas**. Bruxelas, 16 mar. 2026. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2026/03/16/council-adopts-conclusions-on-advancing-the-eu-s-capacity-to-counter-hybrid-threats/>. Acesso em: 2 set. 2026.
- CONSELHO DA UNIÃO EUROPEIA. **Council adopts conclusions on advancing the EU's capacity to counter hybrid threats**. Bruxelas, 16 mar. 2026. Disponível em: <https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/council-adopts-conclusions-on-advancing-the-eu-capacity-to-counter-hybrid-threats/>. Acesso em: 2 set. 2026.
- EUROPEAN UNION INSTITUTE FOR SECURITY STUDIES. **Rising hybrid threats in Africa**: challenges and implications for the EU. Paris: EUISS, 2022.
- HERMAN, Michael. **Intelligence services in the information age**. London: Frank Cass, 2001.
- HOFFMAN, Frank G. **Conflict in the 21st century**: the rise of hybrid wars. Arlington: Potomac Institute for Policy Studies, 2007.
- JOHNSON, Loch K. **National security intelligence**: secret operations in defense of the democracies. 2. ed. Cambridge: Polity Press, 2017.
- KENT, Sherman. **Strategic intelligence for American world policy**. Princeton: Princeton University Press, 1951.
- LOWENTHAL, Mark M. **Intelligence**: from secrets to policy. 9. ed. Washington, DC: CQ Press, 2022.
- NATO. **Countering hybrid threats**. Brussels, 29 Jan. 2026. Disponível em: <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>. Acesso em: 2 set. 2026.

NATO. **NATO's approach to counter information threats**. Brussels, 18 Oct. 2024. Atualizado em 3 fev. 2025. Disponível em: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats>. Acesso em: 2 set. 2026.

NATO. **NATO's approach to counter information threats**. Brussels, 18 Oct. 2024. Updated 3 Feb. 2025. Disponível em: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats>. Acesso em: 2 set. 2026.

NILSSON, Niklas; WEISSMANN, Mikael; PALMERTZ, Björn. Hybrid threats and the intelligence community: priming for a volatile age. **International Journal of Intelligence and Counter Intelligence**, v. 39, n. 1, p. 109-131, 2026. DOI: 10.1080/08850607.2024.2435265.

SOARES, Luiz Claudio. **Guerra híbrida**: cenário brasileiro. Rio de Janeiro: Escola de Guerra Naval, 2025.

SUN TZU. **A arte da guerra**. Lisboa: Edições Sílabo, 2006.

### Nota de transparência sobre o uso de inteligência artificial

Durante a elaboração deste artigo foi utilizada a ferramenta de inteligência artificial generativa ChatGPT (OpenAI) como recurso auxiliar à pesquisa de fontes bibliográficas mais recentes e à organização global do artigo. A seleção e validação das fontes, a interpretação dos conteúdos, as decisões analíticas e a responsabilidade integral pelo texto final permanecem sob controlo do autor.

## Autoria

### 1 Ricardo Caiado

Oficial da GNR; PhD in Law & Security; Jurista; Auditor de Segurança Interna; Doutor em Direito e Segurança pela Faculdade de Direito da Universidade NOVA de Lisboa; Professor

<https://orcid.org/0000-0003-3655-1026> • [rarcaiado@gmail.com](mailto:rarcaiado@gmail.com)

### Como citar este artigo

CAIADO, R. *A intelligence como fator de prevenção da guerra híbrida*. **InterAção**, Santa Maria, v. 17, n. 3, e98668, p. 1-20, 2026. DOI 10.5902/2357797598668. Disponível em: <https://dx.doi.org/10.5902/2357797598668>. Acesso em: dia mês abreviado. ano.