UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e98667, p. 1-19, 2026 • https://dx.doi.org/10.5902/2357797598667
Submissão: 04/09/2026 • Aprovação: 14/09/2026 • Publicação: 02/10/2026

Artigos Dossiê

O impacto das tecnologias emergentes numa Estratégia de Segurança Nacional

The impact of emerging technologies on a National Security Strategy

Ricardo Caiado[I]

[I]Instituto Universitário de Lisboa, Lisboa, Portugal

Resumo

Este artigo analisa o impacto das tecnologias emergentes na formulação e operacionalização de uma Estratégia de Segurança Nacional (ESN), tomando como ponto de partida a relação entre segurança interna, defesa nacional, intelligence e transformação tecnológica. A investigação parte da premissa de que a evolução da inteligência artificial, big data, computação quântica, sistemas autónomos, Internet das Coisas, tecnologias espaciais, cibersegurança e outras tecnologias de uso dual altera simultaneamente as capacidades de proteção do Estado e a natureza das vulnerabilidades que este enfrenta. Metodologicamente, adota-se uma abordagem qualitativa, de natureza teórico-analítica e documental, articulando a literatura de estudos de segurança e estratégia com instrumentos normativos e estratégicos portugueses e europeus e com documentos recentes de organizações internacionais. O argumento central sustenta que as tecnologias emergentes não devem ser incorporadas numa ESN como simples instrumentos técnicos, mas como elementos estruturantes da própria capacidade estratégica do Estado. Os resultados indicam que o seu impacto se manifesta em quatro dimensões interdependentes: antecipação e intelligence; proteção de infraestruturas e ciberespaço; capacidade de decisão e resposta; e autonomia e soberania tecnológica. Conclui-se que uma ESN adequada ao ambiente contemporâneo deve combinar inovação, resiliência, interoperabilidade, autonomia tecnológica, cooperação e governação democrática, assegurando supervisão humana, proporcionalidade e proteção dos direitos fundamentais.

Palavras-chave: Tecnologias emergentes; Segurança nacional; Estratégia; Inteligência artificial; Soberania tecnológica

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

This article analyses the impact of emerging technologies on the formulation and implementation of a National Security Strategy (NSS), focusing on the relationship between internal security, national defence, intelligence and technological transformation. The study assumes that advances in artificial intelligence, big data, quantum computing, autonomous systems, the Internet of Things, space technologies, cybersecurity and other dual-use technologies simultaneously transform the State's protection capabilities and the vulnerabilities it faces. Methodologically, it adopts a qualitative, theoretical-analytical and documentary approach, combining security and strategy literature with Portuguese and European legal and strategic instruments and recent documents produced by international organisations. The central argument is that emerging technologies should not be incorporated into an NSS merely as technical tools, but as structural elements of the State's strategic capacity. The findings indicate that their impact is expressed through four interdependent dimensions: anticipation and intelligence; protection of critical infrastructures and cyberspace; decision-making and response capacity; and technological autonomy and sovereignty. The article concludes that an NSS suited to the contemporary security environment must combine innovation, resilience, interoperability, technological autonomy, cooperation and democratic governance, while ensuring human oversight, proportionality and protection of fundamental rights.

Keywords: Emerging technologies; National security; Strategy; Artificial intelligence; Technological sovereignty

1 INTRODUÇÃO

A segurança nacional encontra-se perante uma transformação que não resulta apenas da emergência de novas ameaças, mas também da alteração dos meios através dos quais os Estados identificam riscos, protegem infraestruturas, produzem conhecimento estratégico e exercem o poder. A aceleração tecnológica introduziu novos ambientes de competição e conflito, incluindo o ciberespaço, o domínio espacial e os sistemas digitais interligados, ao mesmo tempo que aproximou tecnologias civis, militares e de segurança. Neste contexto, a capacidade de um Estado para formular e executar uma ESN depende cada vez mais da sua capacidade para compreender, absorver, regular e utilizar tecnologias emergentes.

A estratégia corresponde ao emprego articulado dos diferentes instrumentos de poder, incluindo os poderes diplomático, informacional, militar e económico, aos quais se acrescenta a comunicação. A ESN deve, por conseguinte, ser compreendida como uma estratégia global, capaz de articular políticas e capacidades distintas em

função de um estado final desejado. Esta perspetiva é particularmente relevante num ambiente em que as fronteiras entre segurança interna e externa se tornam progressivamente mais ténues e em que ameaças transnacionais, tecnológicas e híbridas atravessam os tradicionais limites territoriais.

A transformação tecnológica reforça esta necessidade, devido à existência, entre outras, da robótica, do big data, da computação quântica, da impressão 3D, da internet das coisas, das nanotecnologias e das biociências como tecnologias suscetíveis de produzir mudanças profundas nos domínios económico, social e da segurança. Mais recentemente, os organismos europeus e a NATO têm igualmente identificado a inteligência artificial, a autonomia, as tecnologias quânticas, o espaço, os novos materiais, a biotecnologia, os drones e as redes de comunicações de nova geração como áreas com impacto potencialmente decisivo na segurança e defesa.

O problema de investigação que orienta este artigo pode ser formulado nos seguintes termos: de que modo as tecnologias emergentes transformam os pressupostos, as capacidades e os mecanismos de uma ESN? O objetivo geral consiste em analisar esse impacto, identificando oportunidades, riscos e requisitos de governação para uma ESN adaptada ao ambiente tecnológico contemporâneo. Como objetivos específicos, procura-se: i) enquadrar a evolução do conceito de segurança nacional e da estratégia; ii) identificar as principais tecnologias emergentes com relevância estratégica; iii) analisar os efeitos dessas tecnologias sobre a intelligence, a prevenção, a proteção, a decisão e a resposta; e iv) propor linhas orientadoras para a integração tecnológica numa ESN, com especial atenção aos desafios do Sul Global.

A pertinência do estudo decorre também da chamada do 3.º Dossiê Temático da Revista InterAção, que destaca a autonomia tecnológica, a inteligência artificial aplicada à defesa, a cibersegurança, o apoio tecnológico à decisão estratégica, a governação de tecnologias de uso dual e o impacto das tecnologias emergentes na política de defesa e na segurança internacional. O artigo procura, assim, estabelecer uma ponte entre a reflexão sobre segurança nacional presente no documento de base e a agenda tecnológica contemporânea, evitando uma leitura meramente tecnocêntrica.

2 FUNDAMENTAÇÃO TEÓRICA: ESTRATÉGIA, SEGURANÇA NACIONAL E TRANSFORMAÇÃO TECNOLÓGICA

A estratégia pode ser entendida como a articulação entre fins, meios e modos de ação. Na tradição clássica, Sun Tzu associa-a às orientações destinadas a atingir objetivos definidos pela liderança, enquanto Clausewitz relaciona a estratégia com a utilização do combate para alcançar a finalidade política da guerra. Abel Cabral Couto amplia a perspetiva ao considerar a estratégia como ciência e arte de desenvolver e utilizar forças morais e materiais para alcançar objetivos políticos. Neste paradigma, verifica-se uma convergência para uma conceção de estratégia como emprego do poder através de diferentes instrumentos e das suas inter-relações.

A segurança nacional, por seu turno, não pode ser reduzida à proteção militar do território. A expansão dos estudos de segurança conduziu à incorporação das dimensões política, militar, económica, societal e ambiental, permitindo compreender que a sobrevivência e a resiliência do Estado dependem de um conjunto diversificado de condições. A perspetiva de Buzan é particularmente útil para este efeito, pois permite pensar a segurança de forma multissetorial e relacionar ameaças, vulnerabilidades e processos de securitização (BUZAN; WÆVER; WILDE, 1998).

Esta ampliação concetual é essencial para compreender a tecnologia. Uma infraestrutura digital pode assumir relevância económica, societal e militar simultaneamente; uma interrupção de serviços de telecomunicações pode gerar efeitos sobre a economia, a administração pública, os serviços de emergência e as operações de defesa; e uma vulnerabilidade de software pode converter-se num problema de soberania. A tecnologia, portanto, deixa de ser apenas um instrumento de apoio e passa a integrar a própria estrutura material da segurança nacional.

A globalização aprofundou este fenómeno, porquanto a política externa e interna, a segurança nacional e a cooperação internacional estão cada vez mais interligadas, tornando insuficiente uma conceção exclusivamente nacional da resposta a riscos

transnacionais. A consequência é uma crescente interdependência entre segurança interna e externa e entre atores públicos, privados, nacionais e supranacionais.

No contexto português, o Conceito Estratégico de Defesa Nacional (CEDN), aprovado pela Resolução do Conselho de Ministros n.º 19/2013, define aspetos fundamentais da estratégia global do Estado para a consecução dos objetivos da política de segurança e defesa nacional. O próprio CEDN assume uma visão de conjunto da estratégia nacional e reconhece que para a realização dos objetivos de segurança e defesa concorrem diferentes instâncias do Estado e da sociedade. Embora não exista uma ESN autónoma com a designação e arquitetura defendidas no documento de base, existe um conjunto de estratégias e instrumentos setoriais que compõem, de forma fragmentada, capacidades relevantes para a segurança nacional.

A tecnologia introduz, assim, uma questão adicional: a qualidade da estratégia passa a depender não apenas da posse de capacidades, mas da capacidade de integrar conhecimento científico, dados, infraestruturas, indústria, talento e regulação. A vantagem estratégica resulta da combinação entre tecnologia e instituições. A tecnologia pode acelerar decisões, ampliar a perceção do ambiente operacional e aumentar a capacidade de proteção; contudo, também pode criar dependências externas, novos pontos de falha e assimetrias de poder.

3 METODOLOGIA

O estudo adota uma abordagem qualitativa, de natureza teórico-analítica e documental. O ponto de partida é o estudo de uma ESN, cuja análise permite identificar conceitos, problemas, propostas e referências relevantes sobre segurança nacional, segurança interna, defesa, intelligence, cibersegurança e novas tecnologias. O texto inicial foi reinterpretado e atualizado em função da literatura e dos instrumentos estratégicos mais recentes, sem perder o enquadramento concetual inicial.

A análise organiza-se em quatro dimensões. A primeira é estratégica, procurando compreender como as tecnologias alteram a relação entre fins, meios e modos de ação.

A segunda é institucional, centrada na articulação entre segurança interna, defesa nacional, intelligence, proteção civil, cibersegurança e entidades privadas. A terceira é tecnológica, incidindo sobre inteligência artificial, big data, sistemas autónomos, computação quântica, Internet das Coisas, espaço e tecnologias digitais. A quarta é normativa e política, considerando soberania, direitos fundamentais, supervisão humana, autonomia tecnológica e governação.

No desenvolvimento do presente artigo foram ainda consultados documentos oficiais portugueses, europeus e da NATO para atualizar o quadro estratégico. Entre estes destacam-se o CEDN, a Estratégia Nacional de Ciberdefesa, a Estratégia Nacional de Segurança do Ciberespaço, a estratégia europeia ProtectEU e documentos recentes sobre tecnologias emergentes e defesa. A abordagem é, portanto, essencialmente documental e concetual, não pretendendo medir empiricamente efeitos causais de tecnologias específicas.

4 TECNOLOGIAS EMERGENTES E RECONFIGURAÇÃO DO AMBIENTE DE SEGURANÇA

As tecnologias emergentes caraterizam-se pela rápida evolução, pelo potencial de transformação sistémica e pela possibilidade de utilização simultaneamente civil e militar. A sua relevância para a segurança nacional não decorre apenas do desempenho técnico, mas da capacidade de alterar relações de poder, modelos de decisão, estruturas produtivas e vulnerabilidades.

A inteligência artificial constitui um dos exemplos mais evidentes. Sistemas de aprendizagem automática, processamento de linguagem natural, visão por computador e modelos generativos podem apoiar a análise de grandes volumes de informação, a deteção de padrões, a avaliação de riscos, a tradução e a produção de conhecimento para apoio à decisão. No domínio da segurança, podem contribuir para antecipar ameaças e melhorar a consciência situacional. Contudo, a mesma tecnologia pode ser empregue para gerar desinformação, deepfakes, fraude, ciberataques automatizados

e manipulação de identidades. A Comissão Europeia assinala precisamente esta natureza ambivalente da IA e de outras tecnologias emergentes.

O big data e a análise avançada de dados alteram a capacidade de intelligence. O documento de base já assinalava a utilização de dados biográficos, forenses, imagens, voz, ADN e outros padrões de identificação, bem como o crescente recurso ao big data pelas forças e serviços de segurança. A questão estratégica passa, contudo, de recolher dados para transformar dados em conhecimento fiável e acionável, evitando enviesamentos, falsos positivos e dependência excessiva de sistemas automatizados.

Os sistemas autónomos e a robótica introduzem uma transformação adicional. Drones, veículos autónomos e sistemas de sensores podem aumentar a capacidade de vigilância, reconhecimento, proteção de infraestruturas e resposta a incidentes. Na defesa, podem reduzir a exposição humana a ambientes de elevado risco e ampliar a persistência operacional. Porém, quanto maior for a autonomia concedida a um sistema, maior é a necessidade de definir limites de decisão, responsabilidade, supervisão e regras de empenhamento.

A computação quântica e as tecnologias quânticas representam outra área de relevância estratégica. A computação quântica pode alterar capacidades de processamento e otimização, enquanto sensores quânticos podem melhorar navegação, deteção e posicionamento em ambientes onde os sistemas convencionais são degradados. Ao mesmo tempo, a computação quântica pode comprometer mecanismos criptográficos atualmente utilizados, criando uma exigência de transição para soluções pós-quânticas. A União Europeia identifica estas tecnologias como relevantes para defesa, comunicações seguras, deteção, logística e autonomia estratégica.

A Internet das Coisas, os sensores distribuídos e as redes de nova geração aumentam a interconectividade de sistemas críticos. Essa conectividade permite monitorização contínua, manutenção preditiva e resposta mais rápida, mas amplia a superfície de ataque. Quanto mais sistemas essenciais dependem de redes digitais,

mais a segurança nacional passa a depender de arquitetura de cibersegurança, redundância, segmentação, gestão de identidades e capacidade de recuperação.

As tecnologias espaciais assumem igualmente uma função crescente. Satélites e sistemas de posicionamento fornecem comunicações, navegação, observação da Terra e sincronização temporal essenciais a atividades civis e militares. A crescente dependência de infraestruturas espaciais significa que a sua proteção e resiliência devem ser consideradas no planeamento estratégico nacional.

Por fim, semicondutores, materiais avançados, biotecnologia, impressão 3D e novas tecnologias de fabrico introduzem uma dimensão industrial. A autonomia tecnológica não depende apenas de desenvolver software; depende também de assegurar acesso a componentes, matérias-primas, capacidade de produção, conhecimento e cadeias de abastecimento resilientes. A tecnologia torna-se, assim, simultaneamente uma questão de segurança económica, defesa e soberania.

5 IMPACTO DAS TECNOLOGIAS EMERGENTES NUMA ESTRATÉGIA DE SEGURANÇA NACIONAL

O impacto das tecnologias emergentes numa ESN pode ser sistematizado em quatro grandes dimensões: antecipação e intelligence; proteção e resiliência; decisão e resposta; e autonomia e soberania tecnológica. Estas dimensões são interdependentes e devem ser integradas num único ciclo estratégico.

Na primeira dimensão, a tecnologia aumenta a capacidade de antecipação. A integração de fontes abertas, dados operacionais, sensores, comunicações e informação produzida pelos serviços de informações pode permitir uma visão mais abrangente do ambiente de segurança. A intelligence constitui uma das principais capacidades para enfrentar terrorismo e ameaças transnacionais, destacando a necessidade de antecipar e prevenir. O desafio contemporâneo é transformar esta capacidade em sistemas de alerta precoce, sem confundir correlação estatística com previsão segura.

Na segunda dimensão, as tecnologias reforçam a proteção e a resiliência. A cibersegurança torna-se elemento transversal, porque infraestruturas de energia, água, transportes, saúde, finanças, comunicações e administração pública dependem de sistemas digitais. Portugal aprovou a Estratégia Nacional de Ciberdefesa em 2022, enquanto a estratégia nacional de segurança do ciberespaço já havia estruturado objetivos de resiliência, inovação e recursos. A ESN deve integrar estas capacidades numa arquitetura mais ampla, evitando a fragmentação entre cibersegurança, ciberdefesa e segurança interna.

Na terceira dimensão, a tecnologia transforma a tomada de decisão. Sistemas de apoio à decisão podem reduzir tempos de processamento e melhorar a consciência situacional, mas não eliminam a incerteza. A decisão estratégica continua a envolver valores, prioridades políticas, avaliação de consequências e responsabilidade. A tecnologia deve, portanto, apoiar o decisor e não substituir a autoridade política. Esta preocupação é particularmente relevante em sistemas de IA de elevado impacto e em aplicações militares.

Na quarta dimensão, surge a autonomia tecnológica. Um Estado pode possuir sistemas avançados e, simultaneamente, permanecer tecnologicamente dependente de fornecedores externos. Dependências relativas a semicondutores, cloud, sistemas operativos, componentes críticos, satélites, cabos, modelos de IA ou infraestruturas de dados podem transformar-se em vulnerabilidades estratégicas. A autonomia não significa autossuficiência absoluta, mas capacidade de assegurar funções críticas, diversificar dependências e manter liberdade de decisão.

A NATO reconhece que IA, drones e sistemas autónomos estão a alterar a forma como os conflitos são conduzidos e as capacidades necessárias à dissuasão e defesa. A consequência para uma ESN é clara: a inovação tecnológica deve ser acompanhada por mecanismos de aquisição, experimentação, formação, interoperabilidade e avaliação contínua. Uma estratégia que apenas enumere tecnologias sem criar capacidade institucional para as absorver terá impacto limitado.

6 TECNOLOGIA, SEGURANÇA INTERNA E DEFESA NACIONAL: UMA ABORDAGEM INTEGRADA

A separação clássica entre segurança interna e segurança externa perdeu parte da sua utilidade operacional. As ameaças contemporâneas são transnacionais, difusas e tecnológicas, podendo produzir simultaneamente efeitos internos e externos. Esta interdependência exige uma abordagem integrada na ESN.

No plano interno, a tecnologia pode apoiar prevenção criminal, proteção de fronteiras, combate ao terrorismo, investigação criminal, proteção civil e gestão de crises. No plano externo, pode sustentar defesa, intelligence, vigilância, operações conjuntas e proteção de interesses nacionais no exterior. Entre ambos os planos, existe uma infraestrutura comum de dados, comunicações e cibersegurança.

A Estratégia europeia ProtectEU, apresentada em 2025, reforça esta visão ao propor uma abordagem de toda a sociedade, com partilha de informação, cooperação entre autoridades, empresas, investigadores e sociedade civil e maior capacidade de antecipação de ameaças híbridas, terrorismo, criminalidade organizada, cibercrime e ataques a infraestruturas críticas. Esta abordagem é compatível com a ideia de sistema de sistemas.

A articulação entre forças e serviços de segurança, forças armadas, intelligence, proteção civil, entidades reguladoras e operadores privados deve ser suportada por protocolos, interoperabilidade tecnológica e regras claras de acesso e partilha de informação. O objetivo não é eliminar a autonomia institucional, mas criar capacidade de atuação conjunta quando a ameaça ultrapassa as competências de uma única entidade.

Neste modelo, o Estado deve preservar a direção política e o controlo democrático, enquanto as entidades operacionais mantêm competências especializadas. A cooperação público-privada assume particular importância porque uma parte significativa das infraestruturas digitais e tecnológicas críticas é operada por empresas privadas. A segurança nacional passa, assim, a depender de mecanismos de confiança, partilha de informação sobre riscos e capacidade conjunta de resposta.

7 DESAFIOS PARA O SUL GLOBAL: AUTONOMIA, DEPENDÊNCIA E SOBERANIA TECNOLÓGICA

A questão tecnológica assume uma dimensão particular no Sul Global. A adoção de tecnologias emergentes pode aumentar capacidades nacionais de segurança, mas também aprofundar dependências externas. Países com menor capacidade de investigação, financiamento, produção de semicondutores, computação de elevada escala e desenvolvimento de modelos de IA podem tornar-se consumidores de soluções concebidas segundo prioridades, normas e arquiteturas definidas por atores externos.

A soberania tecnológica deve, por isso, ser entendida como capacidade de tomar decisões estratégicas sobre tecnologias críticas, e não como isolamento tecnológico. Para os Estados do Sul Global, a prioridade pode consistir em identificar funções essenciais, construir competências nacionais, desenvolver ecossistemas científicos e industriais, diversificar fornecedores e estabelecer cooperação Sul–Sul. Neste particular, destaque-se a autonomia tecnológica, a indústria de defesa, a transferência de tecnologia e a cooperação militar e científica Sul–Sul como dimensões relevantes.

A cooperação internacional pode reduzir custos e acelerar a aprendizagem. Os programas conjuntos de investigação, a formação especializada, o desenvolvimento de software, a partilha de dados e a aquisição cooperativa podem criar economias de escala. Contudo, a cooperação deve ser acompanhada por mecanismos de proteção de conhecimento, segurança das cadeias de fornecimento e avaliação de dependências estratégicas.

A experiência europeia mostra que tecnologias como semicondutores e computação quântica são tratadas como elementos de segurança económica e estratégica, precisamente devido à vulnerabilidade das cadeias de abastecimento e ao potencial de utilização dual. Para o Sul Global, esta realidade recomenda políticas que integrem ciência, tecnologia, indústria, defesa e segurança num quadro estratégico comum.

A dimensão crítica não deve, contudo, transformar-se em rejeição da tecnologia. O desafio é evitar simultaneamente dois extremos: a dependência acrítica de soluções externas e o nacionalismo tecnológico inviável. Uma ESN orientada para a autonomia deve procurar capacidade de escolha, interoperabilidade e resiliência, mantendo abertura à cooperação internacional.

8 RISCOS, ÉTICA E GOVERNAÇÃO DAS TECNOLOGIAS EMERGENTES

O impacto positivo das tecnologias emergentes não é automático. A mesma tecnologia que permite melhorar a deteção de ameaças pode ser usada para vigilância abusiva, discriminação algorítmica ou manipulação. Como tal, importa garantir o equilíbrio entre segurança e liberdade, particularmente no tratamento automatizado de dados pessoais e na monitorização de comunicações.

A primeira exigência de governação é a legalidade. A recolha, tratamento e cruzamento de dados devem respeitar a Constituição, a legislação aplicável e os princípios de necessidade e proporcionalidade. A segunda é a responsabilização: deve ser possível identificar quem autorizou, desenvolveu, implementou e supervisionou um sistema. A terceira é a transparência adequada ao risco: nem todos os sistemas podem ser integralmente explicados ao público, mas as regras de utilização, finalidades e mecanismos de controlo devem ser auditáveis.

A inteligência artificial exige particular atenção. Sistemas de alto impacto podem reproduzir enviesamentos dos dados de treino, gerar resultados incorretos ou ser manipulados por adversários. Em segurança, um erro de classificação pode produzir consequências graves. Por isso, a supervisão humana, a validação independente, a rastreabilidade dos dados e os mecanismos de contestação devem integrar o ciclo de vida dos sistemas.

No domínio militar, os sistemas autónomos levantam questões ainda mais sensíveis. A título de exemplo, refira-se a controvérsia sobre a delegação de decisões críticas a sistemas autónomos e a necessidade de controlo humano. A inovação

não deve, portanto, ser avaliada apenas pela eficácia operacional, mas também pela compatibilidade com o Direito Internacional Humanitário e pelos princípios de responsabilidade e controlo político.

A governação deve ainda considerar a segurança da cadeia tecnológica. Um sistema pode ser tecnicamente robusto e, contudo, vulnerável devido ao fornecedor, à atualização de software, ao componente físico ou ao serviço de cloud. A segurança nacional deve incorporar avaliações de risco de fornecedores, requisitos de cibersegurança, planos de continuidade e capacidade de substituição.

Em síntese, uma ESN tecnologicamente orientada necessita de uma arquitetura de governação que combine inovação e contenção de riscos. A tecnologia deve ser tratada como capacidade estratégica sujeita a regras democráticas, e não como uma esfera exclusivamente técnica.

9 PROPOSTA DE UM MODELO ESTRATÉGICO DE INTEGRAÇÃO TECNOLÓGICA

Com base na análise desenvolvida, propõe-se que uma ESN contemporânea organize a integração das tecnologias emergentes através de seis funções estratégicas: antecipar, proteger, decidir, responder, recuperar e aprender.

A função de antecipação corresponde ao reforço da intelligence, da análise prospetiva, da deteção de sinais fracos e do alerta precoce. A função de proteção inclui cibersegurança, segurança física e digital de infraestruturas críticas, redundância e resiliência. A função de decisão corresponde à utilização responsável de sistemas de apoio à decisão, sempre subordinados à autoridade política e ao juízo humano. A função de resposta articula forças, serviços e capacidades tecnológicas para lidar com crises. A função de recuperação assegura continuidade e restabelecimento de serviços. Finalmente, a função de aprendizagem transforma experiências e incidentes em conhecimento para atualizar políticas e capacidades.

9.1 Matriz de integração tecnológica

Quadro 1 – Funções estratégicas da integração tecnológica

Função	Tecnologias/ capacidades	Finalidade estratégica	Principais riscos
Antecipar	Intelligence, análise prospetiva, IA, big data, sensores	Detetar sinais, padrões e ameaças emergentes	Enviesamento, falsos positivos e excesso de confiança algorítmica
Proteger	Cibersegurança, IoT, criptografia, redundância	Reduzir vulnerabilidades e aumentar resiliência	Superfície de ataque e dependência de fornecedores
Decidir	Sistemas de apoio à decisão e fusão de dados	Melhorar consciência situacional e rapidez	Automação excessiva e perda de julgamento humano
Responder	Sistemas autónomos, drones, comunicações seguras	Aumentar capacidade operacional e coordenação	Falhas técnicas, interferência e escalada
Recuperar	Cloud resiliente, backups, redes redundantes	Restabelecer funções críticas	Dependências sistémicas e pontos únicos de falha
Aprender	Análise pós-incidente, simulação e dados históricos	Atualizar políticas e capacidades	Perda de conhecimento institucional e dados de baixa qualidade

Fonte: Autor (2026)

10 DISCUSSÃO

A análise permite sustentar que o impacto das tecnologias emergentes numa ESN não é linear, visto que existem ganhos potenciais de eficiência, precisão e velocidade, mas também novos riscos e dependências. A variável decisiva é a capacidade institucional para transformar inovação tecnológica em capacidade estratégica sustentável.

A primeira implicação é que a tecnologia deve deixar de ser tratada como capítulo setorial da segurança. A sua transversalidade recomenda que a ESN integre uma dimensão tecnológica permanente, com mecanismos de avaliação de tecnologias

críticas, horizon scanning, cenários, experimentação e revisão periódica. A Comissão Europeia, por exemplo, recomenda monitorização sistemática de riscos emergentes, planeamento de cenários extremos e investimento em infraestruturas resilientes.

A segunda implicação é a necessidade de integração institucional. O modelo de sistema de sistemas estudado é particularmente pertinente: segurança do Estado e intelligence, proteção civil e segurança humana, segurança interna, defesa nacional e cibersegurança devem operar com interfaces institucionais e tecnológicas claras.

A terceira implicação é a necessidade de uma política de autonomia tecnológica. Não se trata de produzir internamente todas as tecnologias, mas de identificar dependências cuja interrupção comprometeria funções críticas. Essa avaliação deve incluir hardware, software, dados, serviços cloud, conectividade, satélites, energia e cadeias logísticas.

A quarta implicação diz respeito à democracia. Quanto maior for a capacidade tecnológica do Estado, maior deve ser a clareza sobre os limites da sua utilização. A expansão da capacidade de vigilância e análise pode reforçar a segurança, mas também aumentar o risco de intrusão. A confiança pública deve ser considerada um ativo estratégico. Uma ESN que aumente capacidades técnicas à custa da legitimidade pode, no longo prazo, reduzir a própria segurança que procura proteger.

Finalmente, para o Sul Global, a estratégia tecnológica deve ser orientada por uma combinação de autonomia, cooperação e adaptação contextual. Não basta importar modelos institucionais ou soluções tecnológicas concebidas para outros ambientes. É necessário desenvolver conhecimento próprio sobre ameaças, prioridades e capacidades nacionais, articulando tecnologia com desenvolvimento, inclusão, soberania e segurança humana.

11 CONCLUSÃO

As tecnologias emergentes estão a alterar de forma estrutural o ambiente de segurança. inteligência artificial, big data, sistemas autónomos, computação quântica,

internet das coisas, tecnologias espaciais, semicondutores e outras inovações de uso dual ampliam capacidades de prevenção, proteção e resposta, mas também criam novas vulnerabilidades, dependências e dilemas jurídicos e éticos.

O principal resultado deste estudo é que a integração tecnológica numa ESN não pode ser reduzida à aquisição de equipamentos ou software, porquanto exige uma transformação da própria arquitetura estratégica do Estado. Intelligence, segurança interna, defesa nacional, cibersegurança, proteção civil, indústria, ciência e tecnologia devem ser compreendidas como componentes interdependentes de um sistema de segurança nacional.

Como tal, verifica-se a necessidade de uma ESN global, capaz de integrar segurança interna, defesa nacional, política externa e informações e, simultaneamente, incorporar cibersegurança, segurança marítima, proteção civil, segurança alimentar e outras áreas. A tecnologia deve atravessar transversalmente estes domínios, contribuindo para a antecipação, proteção, decisão, resposta, recuperação e aprendizagem.

No contexto português, a existência do CEDN, da Estratégia Nacional de Ciberdefesa e de instrumentos de segurança do ciberespaço demonstra que existem componentes relevantes, embora permaneça pertinente discutir uma arquitetura estratégica mais integrada. O CEDN continua a constituir um referencial central para a articulação das prioridades de defesa e segurança, enquanto instrumentos mais recentes evidenciam a importância crescente do ciberespaço e das tecnologias emergentes.

Para o Sul Global, o desafio acrescenta a dimensão da autonomia. A capacidade de utilizar tecnologias emergentes de forma segura e sustentável depende do acesso a conhecimento, infraestruturas, talento, financiamento e cadeias de abastecimento resilientes. A soberania tecnológica deve ser entendida como capacidade de escolha e de proteção de funções críticas, apoiada em cooperação internacional e, sempre que possível, em redes de cooperação Sul–Sul.

Conclui-se, portanto, que uma ESN preparada para o século XXI deve ser simultaneamente tecnológica e humanamente orientada. A inovação só produz vantagem estratégica quando acompanhada de instituições capazes de compreender os seus limites, de mecanismos de governação que assegurem responsabilidade e de uma política de autonomia que reduza dependências críticas. A tecnologia deve ampliar a capacidade do Estado para proteger a sociedade e os seus valores fundamentais, sem substituir a decisão política, o controlo democrático e a responsabilidade humana.

REFERÊNCIAS

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. **Security**: a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

CARNOY, Martin. **Os custos económicos da guerra contra o terrorismo**. *In*: CASTELLS, Manuel; SERRA, Narcis (coord.). Guerra e paz no século XXI: uma perspetiva europeia. Lisboa: Fim de Século, 2007.

CNCS – CENTRO NACIONAL DE CIBERSEGURANÇA. **Estratégia Nacional de Segurança do Ciberespaço 2019-2023**. Lisboa: CNCS, 2019.

COMISSÃO EUROPEIA. **Commission presents a European internal security strategy**. Bruxelas, 1 abr. 2025. Disponível em: https://commission.europa.eu/news-and-media/news/commission-presents-european-internal-security-strategy-2025-04-01_en. Acesso em: 2 set. 2026.

COMISSÃO EUROPEIA. **How will emerging technologies reshape EU internal security?** Joint Research Centre. Bruxelas, 1 abr. 2025. Disponível em: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/how-will-emerging-technologies-reshape-eu-internal-security-2025-04-01_en. Acesso em: 2 set. 2026.

COMISSÃO EUROPEIA. **Joint Communication on an International Digital Strategy for the EU. Bruxelas**, 5 jun. 2025. Disponível em: https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu. Acesso em: 2 set. 2026.

COMISSÃO EUROPEIA. **Quantum technologies in defence**. Luxemburgo: Publications Office of the European Union, 2025. DOI: 10.2889/1727389. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/9686d753-e075-11f0-8439-01aa75ed71a1/language-en. Acesso em: 2 set. 2026.

CONSELHO DA UNIÃO EUROPEIA. **ProtectEU**: a European internal security strategy. Bruxelas, 2025.

CONSELHO DE MINISTROS. **Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro**: aprova a Estratégia Nacional de Ciberdefesa. Diário da República, 1.ª série, n. 211, 2 nov. 2022. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924. Acesso em: 2 set. 2026.

CONSELHO DE MINISTROS. **Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril**: aprova o Conceito Estratégico de Defesa Nacional. Diário da República, 1.ª série, n. 67, 5 abr. 2013. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/19-2013-259967. Acesso em: 2 set. 2026.

COUTO, Abel Cabral. **Elementos de estratégia**: apontamentos para um curso. Lisboa: Instituto de Altos Estudos Militares, 1988.

LOURENÇO, Nelson; COSTA, Agostinho. Estratégia de Segurança Nacional: Portugal Horizonte 2030. **Segurança e Defesa**, Lisboa, n. 39, p. 58-65, 2020.

NATO. **Innovation and technology adoption**. Brussels, 8 July 2026. Disponível em: https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies. Acesso em: 2 set. 2026.

NATO. **Key priorities**: innovation and emerging disruptive technologies. Brussels, 2024.

PORTUGAL. **Constituição da República Portuguesa**. Lisboa: Assembleia da República.

PORTUGAL. **Despacho n.º 13692/2013, de 28 de outubro**: Orientação para a política de Ciberdefesa. Diário da República, 2.ª série, n. 208, 28 out. 2013. Disponível em: https://diariodarepublica.pt/dr/detalhe/despacho/13692-2013-3295679. Acesso em: 2 set. 2026.

PORTUGAL. **Lei n.º 53/2008, de 29 de agosto**: Lei de Segurança Interna. Diário da República, 1.ª série, n. 167, 29 ago. 2008.

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

WÆVER, Ole. **Securitization and desecuritization**. *In*: LIPSCHUTZ, Ronnie D. (ed.). On security. New York: Columbia University Press, 1995. p. 46-86.

ZHANG, Yingying et al. The impact of artificial intelligence and blockchain on the accounting profession. **IEEE Access**, v. 8, p. 110462-110474, 2020.

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

Como citar este artigo

CAIADO, R. O contributo das tecnologias emergentes para a prevenção da criminalidade. **InterAção**, Santa Maria, v. 17, n. 3, e98667, p. 1-19, 2026. DOI 10.5902/2357797598667. Disponível em: https://dx.doi.org/10.5902/2357797598667. Acesso em: dia mês abreviado. ano.

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.