INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

O Ciberpoliciamento no Ecossistema de Segurança 4.0: Fundamentos, Desafios e Perspetiva Evolutiva

Auditor

Jean-François Gonçalves Carvalho

Lisboa, 17 de outubro de 2025

Resumo

O presente estudo, de natureza teórico-reflexiva, analisa criticamente o ciberpoliciamento enquanto modelo operativo e estratégico das organizações policiais no ecossistema de Segurança 4.0. Sustentada numa abordagem compreensiva, a investigação articula dimensões técnicas, éticas e institucionais, combinando as teorias da Escolha Racional, das Atividades Rotineiras e dos Padrões Criminais para compreender as dinâmicas e interdependências entre ofensores, vítimas e autoridades policiais no ciberespaço. A análise evidencia que o ciberpoliciamento, embora em progressiva consolidação, permanece conceptualmente fragmentado e aplicado de forma desigual entre os Estados-Membros, refletindo assimetrias na capacitação digital, na literacia institucional e na interoperabilidade tecnológica. Confirma-se que a sua eficácia depende da integração ética e transparente de tecnologias orientadas por dados, da formação especializada e da cooperação público-privada enquanto pilares de uma inteligência policial colaborativa. Modelos como o *Intelligence-Led Policing* e o *Cyber Threat Intelligence* demonstram o potencial da transformação de dados dispersos em inteligência acionável. O estudo acrescenta valor ao conhecimento científico no domínio das ciências policiais e destaca implicações práticas para a capacitação das forças de segurança e para a formulação de políticas públicas baseadas em evidência, contribuindo para o desenvolvimento organizacional e para uma práxis policial adaptada aos desafios éticos e operacionais da era digital.

Palavras-chave: agentes de ameaça racionais, cibercrime, ciberespaço, ciberpoliciamento, Segurança 4.0.

Abstract

This theoretical-reflexive study critically analyzes cyberpolicing as an operational and strategic model for police organizations within the Security 4.0 ecosystem. Based on a comprehensive approach, the research articulates technical, ethical, and institutional dimensions, combining the theories of Rational Choice, Routine Activities, and Crime Patterns to understand the dynamics and interdependencies between offenders, victims, and law enforcement authorities in cyberspace. The analysis highlights that cyberpolicing, although progressively consolidating, remains conceptually fragmented and applied unevenly across Member States, reflecting asymmetries in digital capacity, organizational literacy, and technological interoperability. It confirms that its effectiveness depends on the ethical and transparent integration of data-driven technologies, specialized training, and public-private cooperation as pillars of collaborative police intelligence. Models such as Intelligence-Led Policing and Cyber Threat Intelligence demonstrate the potential for transforming disparate data into actionable intelligence. The study adds value to scientific knowledge in the field of police science and highlights practical implications for the training of security forces and the formulation of evidence-based public policies, contributing to organizational development and police practice adapted to the ethical and operational challenges of the digital age.

Keywords: cybercrime, cyberpolicing, cyberspace, rational threat agents, Security 4.0.

Índice

Introdução

A sociedade contemporânea vive um processo de acelerada transformação digital e de crescente conetividade, impulsionado pela denominada Quarta Revolução Industrial. O ciberespaço emergiu como um novo ambiente da vida social, económica e política, contribuindo para a diluição de fronteiras físicas e jurídicas (Yar, 2006). As atividades humanas migraram para plataformas digitais, redes sociais, sistemas financeiros online e, mais recentemente, para ambientes imersivos como o metaverso (Ning et al., 2023). Essa transição trouxe consigo oportunidades significativas de inovação e desenvolvimento, mas também expôs novas vulnerabilidades exploradas por agentes de ameaça racionais.

De acordo com o Gabinete Cibercrime (2025) não é possível avaliar com rigor estatístico a real dimensão do fenómeno do cibercrime. Contudo, os dados registados em território nacional ao longo dos anos revelam que a "cibercriminalidade é um fenómeno em permanente e claríssima expansão" (Procuradoria-Geral da República, 2025, p. 4). O Sistema de Segurança Interna (SSI, 2025) e a EUROPOL (2025a) confirmam igualmente a consolidação do crescimento da cibercriminalidade, impulsionada pela evolução e disseminação das tecnologias de informação e comunicação (TIC), criadas para fins legítimos, mas facilmente instrumentalizadas para o cometimento de ilícitos *online*.

No que diz respeito ao impacto económico global, as estimativas dos custos globais da cibercriminalidade são preocupantes. Observa-se um crescimento exponencial, com prejuízos de 5,5 mil milhões de euros em 2020 — o dobro em relação a 2015 — e podendo alcançar 10,5 mil milhões de dólares em 2025 (Baldini et al., 2020; Cybersecurity Ventures, 2025).

No âmbito da estratégia de cibersegurança da União Europeia (UE) para a década 2020-2030, reconhece-se que as autoridades policiais dos Estados-Membros desempenham um papel essencial no seio das comunidades de cibersegurança, sendo a eficácia na prevenção e repressão da cibercriminalidade considerada um fator determinante para garantir a segurança coletiva (Comissão Europeia, 2020a). Nesse contexto de interdependência e complementaridade, perfila, a par da cooperação e da partilha de informações, a necessidade de reforçar, de forma integrada, as capacidades das autoridades policiais na dissuasão e investigação da cibercriminalidade, aumentando desse modo a ciber-resiliência (CNCS, 2019; Comissão Europeia, 2020a; Comissão Europeia, 2025a).

Embora a solução a este problema não dependa exclusivamente das autoridades policiais, importa reconhecer que a complexidade da cibercriminalidade exige uma

abordagem multifacetada, envolvendo múltiplos atores e uma ação abrangente na adoção, aplicação e revisão de medidas técnicas e legais. Ainda assim, é certo que a conceção dessas medidas deve ser acompanhada por estruturas organizacionais dotadas de capacidade efetiva para enfrentar a cibercriminalidade (Tropina, 2017).

No plano das organizações policiais, Dodge e Burruss (2020) defendem que é imperativo reconhecer e superar as deficiências e lacunas do policiamento no ciberespaço, em resposta ao crescimento do fenómeno do cibercrime. Importa, assim, compreender como as autoridades policiais se podem posicionar nas suas atividades e estruturas, de modo a implementar estratégias de ciberpoliciamento mais eficaz, evitando o agravamento das vulnerabilidades existentes no ciberespaço (EUROPOL, 2021b).

Historicamente, a organização da vida política, social e económica esteve sempre acompanhada do policiamento num ecossistema de constante adaptação (Yar, 2006). Para contrariar a evolução acelerada do cibercrime, torna-se necessário reinventar o policiamento, de modo a alterar o paradigma de que "Uma das maiores fragilidades da internet (...) é a ausência de um guardião (...) atento aos mais vulneráveis" (Poiares, 2019, p. 118).

A lacuna científica e institucional relativamente ao objeto de estudo é notória, uma vez que, embora exista uma vasta literatura sobre o cibercrime e cibersegurança, os estudos que abordam especificamente o ciberpoliciamento permanecem escassos (Maia, 2019; Yesmen & Ahmed, 2022). Esta investigação procura contribuir para suprir essa insuficiência, promovendo uma reflexão crítica sobre a necessária adaptação policial ao policiamento em ambiente digital, considerando tanto as vítimas como os agentes de ameaça racionais.

O problema central desta investigação reside na capacitação das práticas, competências, estruturas e recursos necessários à transformação digital e à consolidação epistemológica do ciberpoliciamento, enquanto modelo operativo e estratégico das organizações policiais na era da Segurança 4.0.

Neste quadro, estabeleceu-se os seguintes objetivos: (i) explorar teoricamente o conceito de ciberpoliciamento; (ii) analisar os desafios e potencialidades da transformação digital para o ciberpoliciamento no quadro da Segurança 4.0; (iii) refletir sobre as medidas necessárias à implementação eficaz do ciberpoliciamento; (iv) apresentar contributos úteis para o desenvolvimento futuro de um modelo integrado de ciberpoliciamento, congregando a dimensão física e digital.

Por conseguinte, o estudo será orientado para a seguinte pergunta de partida (PD): De que forma o ciberpoliciamento pode estruturar e integrar práticas tecnológicas, éticas e

operacionais capazes de responder aos desafios da sociedade contemporânea num ecossistema de Segurança 4.0?

Com base nos objetivos delineados e a questão de partida formulada, enunciam-se as seguintes hipóteses de investigação: (H1) O conceito de ciberpoliciamento encontra-se suficientemente estruturado e reconhecido na literatura e na prática policial; (H2) A consolidação do ciberpoliciamento depende da integração sistemática de competências digitais, éticas e analíticas nos processos formativos e operacionais das autoridades policiais; (H3) Os mecanismos de cooperação interinstitucional e as parcerias público-privadas constituem fatores determinantes para a integração de práticas e o fortalecimento da inteligência policial em ambiente digital; (H4) A eficácia do ciberpoliciamento depende da capacidade de as instituições policiais integrarem tecnologias de forma ética, transparente e orientada por dados, reforçando a legitimidade e a confiança social.

Metodologia

A presente investigação assume a natureza de estudo teórico-reflexiva e recorreu ao método científico dedutivo, permitindo compreender e analisar criticamente as estruturas, práticas e desafios do ciberpoliciamento no contexto contemporâneo.

A metodologia fundamenta-se numa abordagem compreensiva (*comprehensive approach*), amplamente utilizada em diversos problemas de segurança e políticas públicas por integrar múltiplas perspetivas, domínios e dimensões — técnica, institucional, social, jurídica e público-privada — na análise do problema e na investigação do objeto de estudo. No contexto europeu, esta abordagem tem sido utilizada na resposta a ameaças como o terrorismo, criminalidade organizada e cibersegurança (Brandão, 2016).

Na linha de investigação adotou-se uma estratégia assente na pesquisa qualitativa, privilegiando as seguintes técnicas: (i) pesquisa e revisão bibliográfica e documental, combinando fontes primárias e secundárias, recorrendo a plataformas de bases de dados (*Scopus*, *ScienceDirect* e *IEEE Xplore*), portais de revistas (*SciELO*), repositórios (*RCAAP* e *RENATES*), indexadores (*JSTOR*), plataformas de descoberta (*EBSCO*), bases de dados institucionais (*e.g.* EUROPOL, INTERPOL, ENISA) e documentos oficiais disponíveis no Serviço das Publicações da União Europeia; (ii) Mapeamento científico, com recurso à pesquisa por palavras-chave (Apêndice A), possibilitando o levantamento sistemático da produção académica e institucional em função do número de publicações, áreas temáticas, tipo de documentos (artigos, *conference paper*, capítulos de livros, livros e revisão de conferência), evolução temporal e distribuição geográfica por países; (iii) Análise de

material didático complementar, incluindo vídeos institucionais e reportagens (Anexo), com vista à compreensão dos modelos vigentes e das boas práticas de ciberpoliciamento implementadas em alguns Estados-Membros da UE; (iv) transcrição e tradução de entrevista pública ao Comandante da Unidade Nacional *Cyber* (*UNCyber*) em França (Apêndice B).

A seleção das fontes seguiu os seguintes critérios: (i) relevância temática para o objeto de estudo; (ii) atualidade, privilegiando publicações dos últimos 10 anos; (iii) credibilidade das fontes (indexação em bases de dados científicas, revisão por pares e instituições reconhecidas); e (iv) acesso público e legal à reprodução de conteúdo.

Como instrumento de apoio para organizar e estruturar o presente estudo recorreu-se à ferramenta metodológica de análise e planeamento 5W1H, conforme Tabela 1:

Tabela 1

Aplicação da ferramenta metodológica de análise e planeamento 5W1H à investigação sobre o ciberpoliciamento

Elemento (5W1H)	Questão	Nível de Aplicação	Foco de investigação do ciberpoliciamento
Why	Porquê?	Introdução	Contextualização introdutória, justificação e pertinência: crescimento do cibercrime, ausência de resposta estruturada, ciberpoliciamento emergente.
What	O quê?	Estado da Arte	Resposta às tipologias e taxionomias do cibercrime e *cyberdeviance*.
Where	Onde?	Estado da Arte	Para diferentes camadas do ciberespaço.
Who	Quem?	Estado da Arte	Agentes de ameaça racionais e vítimas.
When	Quando?	Perspetiva/Diretrizes	Temporalidade contínua das respostas e ameaças.
How	Como?	Perspetiva/ Diretrizes	Estruturas, modelos, mecanismos de cooperação e coordenação intra e interinstitucional, multinível (internacional, nacional e local), articulação multisetorial (público-privado), formação e recrutamento e/ou outros aspetos relevantes da práxis policial em ambiente digital.

Fonte: Elaborado pelo próprio (2025).

Nas limitações do estudo, identifica-se que a rápida evolução tecnológica e a ausência de estatísticas harmonizadas sobre o cibercrime, aliadas à fragmentação e escassez da literatura sobre o ciberpoliciamento, são passíveis de restringir a atualidade do tema e a precisão de algumas inferências. Estes fatores evidenciam a necessidade de revisões periódicas e de abordagens complementares, preferencialmente empíricas e comparativas, que permitam atualizar e reforçar a validade das conclusões teóricas apresentadas.

1. Estado de Arte

1.1. Cibercrime e comportamentos ciberdesviantes

O termo cibercrime constitui um conceito polissémico e em constante debate académico e institucional, carecendo de uma definição universalmente aceite (Curtis & Oxburgh, 2023; Matsaung & Masiloane, 2025). Esta ausência de consenso resulta da pluralidade de perspetivas — jurídica, criminológica, sociológica e tecnológica — que o analisam sob lógicas distintas e, muitas das vezes, contraditórias (Hull et al., 2018). Como reconhecem a INTERPOL (2021) e Murphy (2024), tal lacuna dificulta a harmonização normativa, a produção de estatísticas fidedignas e a própria formulação de estratégias de policiamento no ecossistema digital.

Numa perspetiva jurídica, o Conselho da Europa (2001), na Convenção de Budapeste sobre o Cibercrime, oferece um enquadramento mínimo comum ao criminalizar condutas contra a confidencialidade, integridade e disponibilidade dos sistemas informáticos, bem como dos delitos relacionados com conteúdos e a violação de direitos de autor. Contudo, este instrumento mostra-se insuficiente para abarcar a diversidade do fenómeno, uma vez que muitos dos comportamentos socialmente nocivos no ciberespaço não se enquadram nessas categorias legais. É o caso de práticas como o assédio, o *trolling* ou determinadas formas de discurso de ódio, que embora possam não necessariamente constituir crime em determinadas jurisdições, configuram práticas sociais de *cyberdeviance*, isto é, formas de desvio social digital com impacto significativo na ordem pública (Yar, 2006; Phillips et al., 2022).

No plano das tipologias definidas em ambiente académico, Wall (2001, 2007) destacou quatro áreas principais: (i) crimes contra a integridade dos sistemas (*cyber-trespass*); (ii) crimes contra a propriedade (*cyber-deceptions/thefts*); (iii) crimes contra pessoas (*cyber-pornography/violence*); e (iv) crimes contra o Estado e a sociedade *(cyber-terrorism/warfare*). Este modelo inspirou desenvolvimentos posteriores, como os de Marcum e Higgins (2019), que enfatizaram novas formas de violência interpessoal, incluindo o *cyberbullying* e *sextortion*. A criminologia tem desempenhado aqui um papel central, ao evidenciar que tais práticas podem não apenas violar normas jurídicas, como também podem incidir sobre padrões de desvio social no espaço digital.

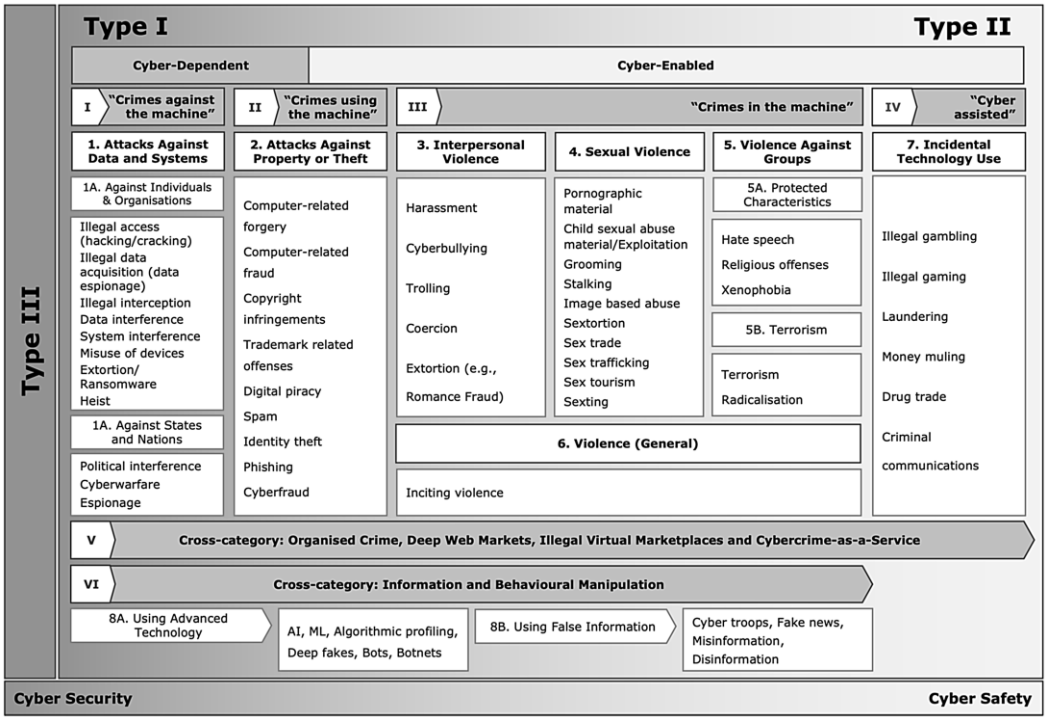
Já McGuire e Dowling (2013) propuseram a relevante distinção entre *cyber-dependent crimes* — ilícitos que só existem através de tecnologia digital, como ataques *DDoS* e *malware* — e *cyber-enabled crimes* — ilícitos tradicionais potenciados pela

tecnologia, como a fraude e a pornografia infantil. Pela sua clareza conceptual e aplicabilidade prática, esta classificação tornou-se uma das mais aplicadas em políticas públicas e estratégias de cibersegurança, incluindo na investigação criminológica aplicada ao cibercrime.

Todavia, a literatura recente tem sublinhado que nenhuma destas abordagens é, por si só, suficiente para capturar a complexidade e mutabilidade do cibercrime. Phillips et al. (2022), por exemplo, sistematizaram diferentes tipologias e taxionomias, relevando não só a diversidade de critérios de natureza jurídica, tecnológica, funcional e motivacional, mas também as suas limitações. Como demonstra a Figura 1, as classificações existentes oscilam entre modelos restritivos, centrados na criminalização mínima comum, e propostas mais amplas, que procuram abranger fenómenos híbridos ou emergentes, incluindo manifestações de *cyberdeviance*.

Figura 1

Enquadramento analítico dos cibercrimes segundo diferentes tipologias e taxionomias



Fonte: Phillips et al. (2022, p. 390).

A análise da Figura 1 reforça a ideia de que o cibercrime é um fenómeno em constante evolução e mutação, que resiste a classificações rígidas e definitivas. Como observam Zalewski (2025) e Khan (2024), as taxonomias precisam de ser suficientemente flexíveis

para integrar novos contextos, como o metaverso, a inteligência artificial (IA) ou os serviços de *crime-as-a-service*, sob pena de rapidamente se tornarem obsoletas.

Mais do que fixar uma definição única, a investigação atual tende a reconhecer a complexidade, interdisciplinaridade e carácter dinâmico do cibercrime, encarando as tipologias e taxionomias como ferramentas heurísticas, úteis, mas provisórias. Nesse sentido, o cibercrime pode ser entendido como a transformação informativa, em rede globalizada de comportamentos desviantes ou criminosos através de tecnologias digitais, exigindo uma análise que combine fundamentos jurídicos, tecnológicos, criminológicos e sociológicos (Wall, 2011; Yar, 2006). O recurso ao conceito de *cyberdeviance* alarga ainda mais este enquadramento, permitindo contemplar práticas em ambiente digital que, embora não tipificadas como crime, representam formas de desordem social com efeitos relevantes na segurança e para o policiamento contemporâneo.

1.2. Ciberespaço

O termo ciberespaço surgiu inicialmente como uma metáfora de um universo partilhado, materializado em literatura de ficção científica por Gibson (1984). Desde então, evoluiu para um conceito central em várias disciplinas, da ciência da computação à criminologia, ainda que permaneça marcado por ambiguidades, pela falta de uniformidade conceptual (Castells, 2002; Deibert, 2013; Floridi, 2011; Yar, 2006).

De uma forma geral, o ciberespaço pode ser definido como o ambiente global e interconectado resultante da interação entre pessoas, *software*, dispositivos e redes digitais, no qual circulam dados, informações e serviços (Floridi, 2011). Tal conceção aproxima-se da perspetiva de Castells (2002), que o integra na lógica da sociedade em rede, em que as interconexões digitais transformam profundamente as dinâmicas sociais, políticas e económicas. Essa visão encontra eco em Floridi (2011), ao conceptualizar a *infoesfera* como um ecossistema informacional, e em Deibert (2013), que destaca a sua dimensão política e cultural, reforçando a ideia de que o ciberespaço não é apenas uma infraestrutura tecnológica, mas também um espaço de interação humana e de poder. A sua natureza híbrida — simultaneamente material e imaterial — ajuda a explicar a dificuldade em alcançar uma definição consensual.

No plano institucional, a North Atlantic Treaty Organization (NATO, 2017) reconhece o ciberespaço como um domínio operacional, equiparável à terra, mar, ar e ao espaço, sublinhando a sua relevância estratégica no âmbito da defesa e segurança. Também a UE o conceptualiza como uma infraestrutura crítica que suporta a economia digital e os

direitos fundamentais (Murphy, 2024). Contudo, a ausência de delimitação física de fronteiras desafia a aplicação de conceitos tradicionais de soberania, jurisdição e policiamento, exigindo novas formas de cooperação internacional e regulação transnacional (Yar, 2006).

Assim, o ciberespaço deve ser entendido como um ecossistema híbrido, composto por infraestruturas físicas, protocolos, *software*, dados e utilizadores, mas também por práticas sociais e culturais. Esta conceção aproxima-se da proposta de Radulov (2019), que descreve a Segurança 4.0 como um ecossistema em que as pessoas, organizações, atores (provedores de segurança e criminosos) interagem continuadamente num ambiente tecnológico moldado pela Indústria 4.0. Tal como no ecossistema de Segurança 4.0, o ciberespaço pode ser visto como organismo vivo onde as ameaças e respostas coevoluem, exigindo que as autoridades policiais se adaptem permanentemente nas suas estratégias de intervenção.

Nesse sentido, importa reconhecer que, embora interconectado, o ciberespaço está estratificado em diferentes níveis de acessibilidade e visibilidade. Esta estrutura em camadas é fundamental para compreender as dinâmicas criminais e, consequentemente, os desafios diferenciados do ciberpoliciamento contemporâneo para a prevenção e investigação criminal (EUROPOL, 2021a). Da literatura consultada, destacam-se três níveis principais: a *Surface Web*, a *Deep Web* e a *Dark Web*, de acordo com as características descritas na Tabela 2.

Tabela 2

Camadas da Web com as principais caraterísticas diferenciadoras

Nível/Camada	Características Principais	Autor(es)
Surface Web	Parte visível e indexada a motores de busca; Estima-se que representa cerca de 5% da informação total online. Inclui páginas institucionais, redes sociais, comércio eletrónico e conteúdos acessíveis ao público em geral. Informação aberta e passível de pesquisa em *Open Source Intelligence* (OSINT).	EUROPOL (2021a); Magán-Carrión et al. (2021); Maia (2019).
Deep Web	Conteúdos não indexados pelos motores de busca, acessíveis apenas por sistema de autenticação (*e.g.* bases de dados, intranets e áreas privativas), podendo os conteúdos serem encriptados. Maioritariamente legítima, mas de difícil acesso para as autoridades policiais.	Bergman (2001); Phillips et al. (2022).
Dark Web	Subcategoria da *Deep Web*, acessível apenas por softwares de anonimato e criptografia (*e.g. Tor*, *I2P* e mensagens cifradas). Garante anonimato, liberdade de expressão, mas também é um espaço privilegiado para mercados (*e.g.* estupefaciente, armas, documentos falsificados, dados, ferramentas de *hackers*) e serviços ilícitos [*e.g. Crime-as-a-Service, Cybercrime-as-a-Service* (CaaS)]. Pode requer	Adel & Norouzifard (2024); EUROPOL (2021a); Jardine (2015); Wang et al. (2025).

	métodos *cyber forensics* e monitorização automatizada combinando com *Cyber Threat Intelligence* (CTI) e OSINT.

Fonte: Elaborado pelo próprio (2025).

Em síntese, o ciberespaço deve ser conceptualizado não apenas como uma infraestrutura tecnológica, mas também como um espaço híbrido, onde se projetam tanto oportunidades como riscos criminais. Este enquadramento é essencial para compreender as lógicas contemporâneas de ciberpoliciamento e delinear respostas eficazes no quadro da Segurança 4.0.

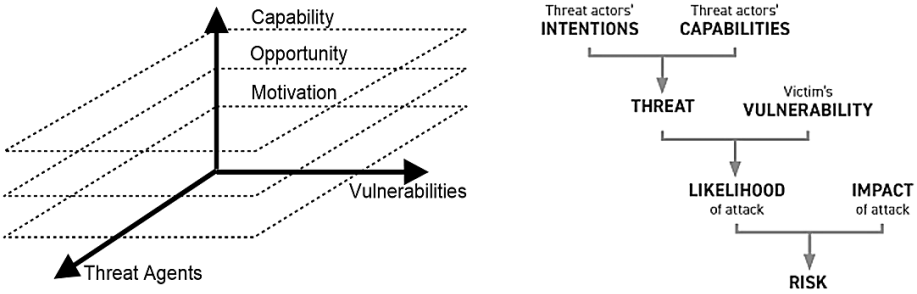
1.3. Agentes de ameaça racionais e vítimas preferenciais

Os agentes de ameaça racionais são entendidos como entidades dotadas de intencionalidade, capacidade de decisão e adaptação estratégica, que atuam de forma instrumentalizada para atingir objetivos que constituem ilícitos tanto no espaço físico como digital (Harkins, 2016; Regian & Noever, 2017; Vidalis & Jones, 2005). Estes ofensores podem assumir diferentes níveis de agregação: indivíduos, grupos, organizações e até Estado-nação, explorando vulnerabilidades técnicas, sociais e institucionais (Regian & Noever, 2017; Vidalis & Jones, 2005).

Embora não exista uma definição harmonizada, a literatura sublinha que a origem das ameaças se encontra centrada no ser humano e na sua capacidade de identificar alvos, explorar fragilidades e adaptar os métodos de ataque (Harkins, 2016). De acordo com Pfleeger et al. (2015), a exploração bem-sucedida de vulnerabilidades assenta em três elementos fundamentais: motivação, capacidade e oportunidade.

Figura 2

Matriz do agente de ameaça racional/vulnerabilidade (à esquerda) e cadeia causal da segurança do risco (à direita)



Fonte: Sharma et al.(2021, p. 8); Martin (2024, p. 8).

Segundo a Teoria da Escolha Racional, o crime resulta de um cálculo em que os ofensores procuram maximizar ganhos e reduzir custos (Becker, 1968; Cornish & Clarke, 2017). No ciberespaço, este cálculo é favorecido por assimetrias de informação, baixos custos de entrada, elevada rentabilidade e perceção reduzida de risco, o que explica a proliferação de condutas como o *phishing*, *ransomware* ou a fraude financeira (Radulov, 2019). Contudo, a racionalidade não é absoluta. De acordo com a noção de racionalidade limitada de Simon (1997), os ofensores decidem com informação incompleta e em contexto de incerteza, o que potencia a experimentação, a aprendizagem e a inovação criminal. Assim, ofensores testam novas técnicas, ajustam *modus operandi* em resposta a contramedidas policiais e recorrem ao *Crime-as-a-Service* (EUROPOL, 2024c).

Tabela 3

Categorizações da inovação criminal segundo Crenshaw (2010), com adaptação de Prosegur Research (2022) quanto à denominação operacional

Tipo	Fundamento	Exemplos
Tática	Adoção de técnicas, tecnologias e *modus operandi* para alcançar os objetivos tradicionais preestabelecidos, proporcionando mudanças substanciais na execução de crimes e redefinindo padrões de comportamento. É a mais observada e passível de difusão entre agentes de ameaça.	Usar a inteligência artificial para gerar *malware* polimórfico e ataques automatizados; *deepfakes* aplicados à fraude financeira e *sextortion*; campanhas *spear phishing* personalizadas com base em perfis de redes sociais.
Organizacional ou Operacional	Alterações na estrutura, procedimentos ou modo de funcionamento de redes criminosas, visando manter operações continuas, recrutamento e financiamento.	Estabelecer plataformas *CaaS* que oferecem *kits* de *ransomware* e *botnets*; utilizar criptomoedas com *mixers* e *tumblers* para branqueamento de capitais;

		Coordenar operações através de fóruns da *Dark Web* e canais encriptados (*e.g. Telegram*, *Signal*).
Estratégica	Redefinição de objetivos, alvos e cálculos de custo-benefício, implicando novas formas de exercer pressão e poder.	Proceder a ataques coordenados a infraestruturas críticas (*e.g.* energia, saúde, transportes); utilizar campanhas massivas de desinformação; Explorar vulnerabilidades *zero-day* para comprometer cadeias de abastecimento (*supply chain attacks*).

Fonte: Elaborado pelo próprio (2025).

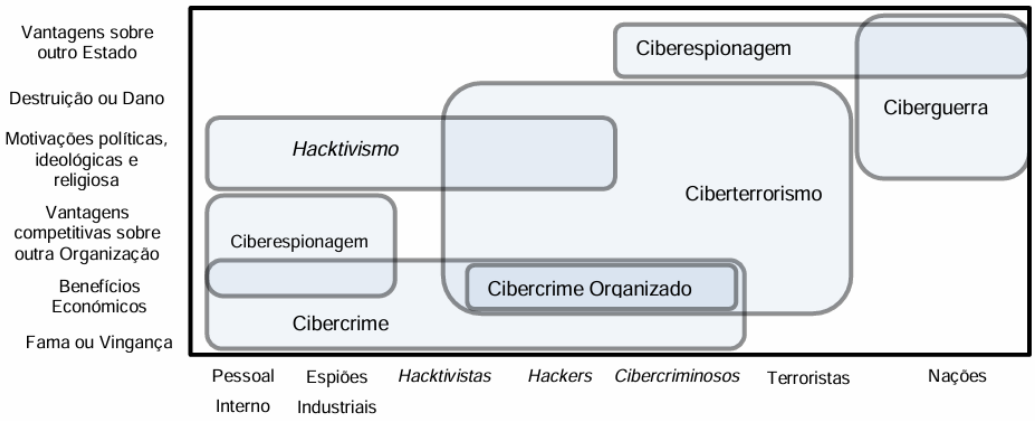
A Teoria das Atividades Rotineiras (Cohen & Felson, 1979) contribui para a análise ao explicar que o crime requer a convergência entre um ofensor motivado, um alvo adequado e a ausência de um guardião eficaz. No ambiente digital, essa convergência é amplificada pela conetividade permanente, pela fragilidade dos mecanismos de supervisão institucional e pela facilidade de ocultação de identidade (Chen et al., 2025).

Estudos posteriores demonstraram que fatores como a exposição pública, visibilidade de dados pessoais e ausência de proteção eficaz aumentam a suscetibilidade à vitimização *online* (Holt & Bossler, 2015; Reyns et al., 2011). Tal análise permite estabelecer que as vulnerabilidades resultam de duas ordens de fatores. Em primeiro lugar, de comportamentos individuais como partilha excessiva de dados, o uso de *passwords* fracas ou a ausência de medidas de autoproteção. Em segundo lugar, de fragilidades estruturais como falhas em *softwares*, ausência de encriptação, defesas insuficientes em PME ou lacunas regulatórias (Brenner, 2004; ENISA, 2024; EUROPOL, 2024c).

Quanto ao perfil dos ofensores, importa destacar que não existe um recorte de características homogéneas que se aplique a todos os autores de cibercrimes. Na verdade, existem estudos que evidenciam diferentes tipologias de ofensores, motivação e capacidades (Khan, 2024; Phillips et al., 2022).

Figura 3

Áreas de intervenções dos agentes de ameaça racionais de acordo com as suas motivações



Fonte: Carvalho (2021, p. 20).

Na compreensão dos agentes de ameaça racionais é igualmente relevante considerar a resiliência criminal. Como destaca Ayling (2009), as redes criminosas possuem uma elevada capacidade de adaptação, assegurando continuidade operacional mesmo após ações de natureza repressiva. Essa resiliência manifesta-se em estratégias como a compartimentação em células autónomas, a diversificação de atividades criminosas e a externalização do *CaaS.* Tais dinâmicas permitem às redes criminosas recomporem-se após desmantelamentos parciais, ajustando continuadamente as suas rotinas em resposta às medidas de controlo (EUROPOL, 2024c; Phillips et al., 2022).

A Teoria dos Padrões Criminais (Brantingham & Brantingham, 2017) acrescenta uma perspetiva espaciotemporal, defendendo que os ofensores não escolhem alvos aleatoriamente, mas com base em rotinas e pontos de contacto previsíveis. Embora originalmente concebida para o espaço físico, a sua aplicação no plano digital é pertinente. Como salientam Yar (2006) e Wall (2007), as dinâmicas do cibercrime reproduzem lógicas do mundo físico, sobretudo na identificação de "locais" (ou *nodes*) de oportunidade, explorando rotinas previsíveis e fluxos recorrentes de interação. Nesse sentido, fóruns da *Dark Web*, plataformas de redes sociais, serviços de mensagens encriptadas e aplicações de partilha de ficheiros configuram ambientes criminógenos de foro digital, comparáveis a *hotspots* urbanos (Phillips et al., 2022). McGuire e Dowling (2013) reforçam esta aplicabilidade ao argumentarem que as categorias de crimes *cyber-dependent* e *cyber-enabled* podem ser analisadas à luz de padrões de convergência digital.

No plano da vitimização, destacam-se grupos com maior vulnerabilidade. Entre os jovens, a elevada presença em redes sociais expõe-nos a fenómenos como o *cyberbullying*, *sextortion* e assédio *online*. Em 2023, 49% dos jovens europeus entre os 16 e 19 anos de idade afirmaram ter encontrado mensagens hostis ou degradantes *online* (EUROSTAT, 2024b), enquanto os casos de *sextortion* a menores registaram um crescimento contínuo (EUROPOL, 2024c).

Entre os idosos, a baixa literacia digital agrava a suscetibilidade a fraudes, considerando que apenas 28% da população europeia entre os 65 e 74 anos possuía competências digitais básicas em 2023, contrastando com os 70% entre os 16 e 24 anos de idade (EUROSTAT, 2024a). A INTERPOL (2021) reforça esse argumento, indicando que o aumento drástico do número de vítimas vulneráveis se deve à falta de conhecimento geral em cibersegurança e ciber-higiene.

Também as PME representam alvos privilegiados devido à sua menor maturidade em cibersegurança. Um recente Eurobarómetro da Comissão Europeia (2022) revelou que 28% das PME europeias reportam algum tipo de cibercrime, embora muitas optem por não comunicar os incidentes por receio de danos reputacionais. Na sua maioria, isto acontece pelo fundado temor de abalar a confiança dos investidores ou dos mercados onde os negócios empresariais se estabelecem (INTERPOL, 2021).

De forma convergente, um inquérito britânico evidenciou que apenas 10% das empresas vítimas de incidentes reportam à Polícia, evidenciando a preponderância de cifras negras (Department for Science, Innovation and Technology & Home Office, 2024).

Para além da cibercriminalidade formalmente tipificada, também emergem comportamentos de *cyberdeviance*, como o assédio, *trolling* ou discurso de ódio. Embora nem sempre sejam uniformemente e necessariamente criminalizados em todos os Estados-Membros, estes comportamentos geram impactos psicológicos, sociais e reputacionais relevantes (Thomas & Loader, 2000; Yar, 2006).

Em síntese, este quadro analítico evidencia que determinados grupos — jovens, idosos e PME — funcionam como alvos preferenciais, refletindo a adaptação estratégica dos agentes racionais em ambientes de baixa proteção e alta previsibilidade de rotina em contexto digital. Nesse sentido, o ecossistema deve ser entendido como um espaço de coevolução, onde a racionalidade adaptativa dos ofensores se entrelaça com a vulnerabilidade das vítimas, criando padrões previsíveis de risco. Reconhecer essa dinâmica é condição essencial para orientar políticas públicas e delinear estratégias eficazes de ciberpoliciamento.

2. Perspetivas/Diretrizes

2.1. Da conceptualização à práxis do ciberpoliciamento

Na conceção do conceito de ciberpoliciamento, a EUROPOL (2025b) define-o como uma prática institucionalizada de patrulhamento visível e uniformizado em ambientes digitais frequentados por cidadãos e exercida pelas autoridades policiais com ênfase na construção de confiança, prevenção e interrupção do crime. Para além da dimensão preventiva, o ciberpoliciamento integra também funções de investigação, permitindo a recolha de indícios e a identificação de comportamentos ilícitos em ambientes digitais (EUROPOL, 2025b).

Esta definição reinterpreta e estende os modelos tradicionais de policiamento aplicados em contextos físicos, projetando-os para o ecossistema digital (EUROPOL, 2025b). Neste sentido, Jardine (2015) destaca a utilidade de articular diferentes modalidades — o policiamento *online*, com ações de natureza uniformizada e visível, e o policiamento *offline*, frequentemente desenvolvido em ações de investigação e monitorização não uniformizada ou à civil — como dimensões complementares de um mesmo esforço em prol da segurança pública.

Historicamente, o termo ciberpoliciamento (*cyber-policing*) nem sempre foi entendido desta forma. No início dos anos 2000, era frequentemente concebido para designar a introdução de tecnologias digitais de apoio ao policiamento, como a instalação de computadores em viaturas policiais, para permitir consultas imediatas nas bases de dados e verificações de mandados (Chan et al., 2001). Na atualidade, a noção evoluiu para refletir a transposição do policiamento em espaço físico para ambientes digitais. Todavia, o policiamento da internet exige mais do que a aquisição de novos conhecimentos e capacidades; implica, sobretudo, uma transformação estrutural na forma como a polícia se relaciona com as dinâmicas de segurança digital (Wall, 2011).

A consolidação deste processo manifestou-se, principalmente, com a criação de unidades especializadas em cibercriminalidade. A literatura demonstra que, à medida que a cibercriminalidade se intensifica, as autoridades policiais tendem a estruturar o policiamento em torno dessas unidades, como resposta às crescentes pressões institucionais para adotar estratégias específicas de combate ao fenómeno (Willits & Nowacki, 2016). Neste contexto, embora a maioria dos Estados-Membros tenha privilegiado o policiamento não visível, alguns países abriram caminho para novos modelos, tendencialmente integrais e inovadores (ver Vídeos A1 e A2), que reforçam a proximidade com as comunidades virtuais.

Tabela 4

Implementação do ciberpoliciamento visível e uniformizado em alguns países da Europa, de acordo com EUCPN (2020, janeiro), EUROPOL (2025b) e INTERPOL (2023)

País/ Ano	Designação/ Estrutura	Modelo Organizacional	Orientação
Estónia (2011)	*Web-constables* - Polícia Comunitária Virtual (*Estonian Police and Border Guard Board*)	Descentralizado com equipa de pequena dimensão, mas com alcance ao nível nacional	Cerca de 13 polícias focados na prevenção e proximidade; presença visível e diálogo com comunidades; apoio às vítimas; monitorização e recolha de informações em fóruns e redes sociais. Não investigam, mas remetem informação para as unidades de investigação criminal. Inclui ainda a participação de um grupo de 21 polícias voluntários — ver Vídeo A3.
Dinamarca (2022)	*Politiets Online Patrulje*	Centralizado (departamento especializado a nível nacional)	Equipa multidisciplinar composta por 7 polícias, 1 analista, 1 profissional da comunicação e 1 chefe de equipa. Foco na prevenção, proximidade digital, investigação, deteção precoce e monitorização (OSINT). Patrulhamento visível e diálogo (via *streaming*). Presença e interação nas redes sociais (*e.g. Instagram*, *TikTok* e *Twitch*) e jogos online (*e.g. Minecraft*, *Counter-Strike* e *Fortnite*) — ver Vídeos A4 e A5.
Noruega (2018 e expandido em 2020)	*Politiets nettpatruljer*	Descentralizado totalmente em 12 distritos desde 2020	Cerca de 45 polícias dedicados à prevenção, sensibilização, proximidade, deteção e monitorização. Interação em redes sociais e grupos de comunicações (*e.g. Reddit*, *Omegle*, *Telegram*, *TikTok*, *Discord* e *Messenger*), jogos online (*e.g. Minecraft*, *Roblox*, *FIFA*, *Fortnite*, *League of Legends* e *Counter-Strike*) e *streaming* (*Facebook* e *YouTube*) — ver Vídeo A6.

Fonte: Elaborado pelo próprio (2025).

Ao nível conceptual, importa ainda notar que a própria utilização do prefixo "ciber" tem vindo a ser problematizada. Como defendem Furnell e Dowling (2019), o avanço da digitalização e a ubiquidade da tecnologia em quase todas as esferas sociais sugerem que a distinção entre o crime físico e o cibercrime — e, por consequência, entre o policiamento tradicional e o ciberpoliciamento — tenderá a esbater-se. Esta conjetura encontra sustentação nos seguintes indicadores: mais de 80% dos crimes apresentam hoje uma componente digital (Comissão Europeia, 2021); quase todas as formas de criminalidade organizada evidenciam uma pegada digital (EUROPOL, 2025c); e a Comissão Europeia (2025c) estima que 85% das investigações criminais dependem de aceder a informações digitais. Neste quadro antevê-se, a possibilidade do termo "ciberpoliciamento" ser absorvido numa conceção mais

ampla de policiamento integrado, no qual o digital deixe de constituir exceção para afirmar-se como vetor transversal.

A problematização do termo reflete-se igualmente na produção científica existente. Com efeito, os resultados do mapeamento bibliográfico sistematizado no Apêndice A demonstram que o ciberpoliciamento é conceito difuso, representado sob diferentes denominações na literatura internacional (*e.g. cyber policing*, *cyber-policing*, *cyberpolicing*, *digital policing*, *e-policing* e *online policing*). Estas variações terminológicas revelam a ausência de consenso conceptual e o carácter multidisciplinar e interdisciplinar do ciberpoliciamento (Huey & Ferguson, 2022). Tal constatação, converge com a análise de Maia (2019), que sublinha a escassez de produção científica dedicada ao ciberpoliciamento, em contraste com áreas mais consolidadas como a cibersegurança ou o cibercrime, o que confirma tratar-se de um domínio em construção. Nessa mesma linha, a EUROPOL (2025b) reconhece o caráter emergente do campo, salientando que apenas recentemente têm surgido estudos capazes de contribuir para a clarificação e estabilização do conceito. Essa pluralidade terminológica e conceptual encontra expressão no mapeamento bibliográfico realizado (Apêndice A), cujos resultados são sistematizados sinteticamente na Tabela 5.

Tabela 5

Perspetivas conceptuais e temáticas associadas ao ciberpoliciamento a partir do mapeamento científico no Apêndice A

Dimensão	Principais Evidências	Implicações para o estudo
Expressão do termo ciberpoliciamento	Uso residual em português; predominância em inglês com *cyber policing* e *online policing*.	Preenche uma lacuna terminológica e conceptual no espaço lusófono.
Hegemonia linguística	Produção científica dominada pelo inglês; termos anglófonos padronizam o campo.	Exige diálogo com o mainstream anglófono para afirmação em português.
Área temática	Maior expressão nas áreas temáticas das Ciências Sociais, Ciências da Computação e Engenharia.	Confirma natureza multidisciplinar do ciberpoliciamento e articula-se com a Segurança 4.0.
Evolução cronológica	Crescimento exponencial em *cybercrime* e *cybersecurity*; aumento mais lento, mas constante em *cyber policing*.	Confirma que o campo está em construção e em consolidação, acompanhando a tendência global.
Distribuição geográfica	EUA, Reino Unido, Índia e China lideram; países lusófonos praticamente ausentes na abordagem do ciberpoliciamento.	Evidencia a oportunidade de reforçar o posicionamento académico e institucional em Portugal e na Europa.
Natureza documental	Maioria em artigos, *conference papers* e publicações em livros.	Revela a fragmentação do campo, reforçando a necessidade de uma síntese teórica consolidada.

Tendências emergentes	Evidencia a necessidade de consolidar o ciberpoliciamento e de explorar o metaverso em novas linhas de investigação.	Sinaliza eixos prioritários de investigação futura, nomeadamente sobre o policiamento imersivo.

Fonte: Elaborado pelo próprio (2025).

No caso português, a experiência da Polícia de Segurança Pública (PSP) não traduz ainda a plena assunção do conceito de ciberpoliciamento, congruente com um patrulhamento visível e permanente no ciberespaço. Como observa Pereira (2021, p. 65), através do Núcleo de Cibercriminalidade (*nCiber*), "não existem equipas a "patrulhar" o ciberespaço constantemente. Existe um trabalho de monitorização direcionado ou um acompanhamento a determinadas tipologias de crime". Nesse sentido, o plano de atividades da PSP incorpora algumas ações de ciberpoliciamento focadas em fenómenos específicos, alinhados com estratégias de prevenção europeias e internacionais (PSP, 2025).

Face a este enquadramento, a Tabela 6 apresenta os princípios enformadores do ciberpoliciamento, constituindo uma referência para a sua consolidação no plano institucional.

Tabela 6

Princípios orientadores do ciberpoliciamento uniformizado e visível no ecossistema digital, adaptado de EUROPOL (2025b), RAN (2021) e Zalewski (2025)

Princípio orientador	Descrição	Objetivo estratégico
Presença permanente	A polícia deve manter-se continuadamente presente nas comunidades online, reforçando a prevenção e deteção de cibercrimes e comportamentos ciberdesviantes.	Reforça a legitimidade e combate a perceção de que no ciberespaço não existem regras de conduta nem mecanismos de controlo formal e informal.
Interação social	O policiamento deve relacionar-se de forma harmoniosa com as comunidades, provendo o diálogo, a partilha e a confiança, sobretudo junto dos grupos de risco (*e.g.* jovens, idosos e PME). Presença privilegiada em plataformas digitais como as redes sociais (*e.g. Instagram*, *Facebook*, *TikTok*), *YouTube* e fóruns, ou por via de jogos online (*e.g. CS:GO*, *Fortnite*: *Battle Royale*, *Fall Guys*, *Call of Duty*: *Warzone*).	Promove a proximidade com os cidadãos, encurta distâncias e contribui para a construção do capital social no espaço digital.
Transparência e legitimidade	Privilegiado a atuação uniformizada em plataformas digitais através de contas oficiais, promovendo a evidência e combatendo a desinformação e as *fake news*.	Reforça a ética policial, sustenta uma justiça inclusiva e aumenta a confiança social, bem como a resiliência contra a manipulação da informação.

Acessibilidade e conveniência	Redução de barreiras de contacto e garantia de disponibilidade permanente de mensagens e conteúdos, de forma a alcançar um maior número de cidadãos.	Facilita o acesso da sociedade à Polícia, reforça a eficácia comunicacional e institucional, mantém a população informada sobre ameaças prevalecentes.
Proatividade	Colaboração com autoridades, serviços de segurança e entidades privadas. Apoio à remoção de conteúdos nocivos ou à suspensão de atividades *online*; intervenção junto de potenciais vítimas e ofensores; realização de pesquisas em fontes abertas (OSINT) e sinalização às estruturas e entidades competentes.	Antecipa ameaças, reduz oportunidades para o crime, aumenta a eficácia preventiva e reforça a capacidade de intervenção precoce das autoridades policiais.

Fonte: Elaborado pelo próprio (2025).

De acordo com Virta (2017), a prevenção é uma das componentes essenciais do policiamento em todas as suas variantes. Segundo Khan (2024), as autoridades policiais devem desempenhar três papéis fundamentais: (i) trabalhar com as partes interessadas nas medidas de prevenção; (ii) aferir a vulnerabilidade que levou ao acontecimento do cibercrime; (iii) auxiliar na correção da vulnerabilidade por forma a evitar a reincidência.

Khan (2024) sublinha que o poder preventivo da polícia assenta em dois objetivos centrais: prevenir novos danos e facilitar a ação penal. O primeiro objetivo revela-se particularmente importante para o dispositivo uniformizado que, mediante a sua capacidade operacional, treino especializado e preparação para intervir, são responsáveis por garantir o cumprimento da lei e da ordem pública, preservando a paz pública e o reforço do sentimento de segurança.

Neste enquadramento, o ciberpoliciamento revela-se ainda um campo em construção, marcado por pluralidade conceptual, práticas emergentes e uma gradual consolidação institucional.

2.2. A cooperação e coordenação institucional no quadro da governança multinível

A repressão à cibercriminalidade na UE assenta numa arquitetura multinível, onde coexistem estruturas supranacionais e nacionais que se articulam de forma complementar. A Estratégia de Segurança da UE 2020-2025 consolidou este enquadramento, posteriormente prosseguido e reforçado na estratégia de 2025, assegurando a continuidade e o aprofundamento das prioridades estratégicas (Comissão Europeia, 2020b; Comissão Europeia, 2025b).

Figura 4

Síntese dos eixos estratégicos e áreas prioritárias da Segurança da União Europeia 2020-2025

Fonte: Comissão Europeia (2020, julho 24).

No plano supranacional, destacam-se três pilares institucionais. O Centro Europeu da Cibercriminalidade (EC3), criado em 2013, que assegura apoio a investigações complexas, avaliações de ameaças emergentes e programas de formação, funcionando como elo entre Estados-Membros, organizações internacionais (*e.g.*, INTERPOL, AFRIPOL, AMERIPOL, ASEANAPOL) e o setor privado (EUROPOL, 2025a). A Agência da UE para a Cibersegurança (ENISA), com mandato reforçado pelo Regulamento (UE) n.º 2019/881 assume a vertente regulatória e preventiva, com especial relevo para a certificação de cibersegurança, elaboração de orientações técnicas e coordenação da resiliência digital europeia (Parlamento Europeu & Conselho da União Europeia, 2019; Murphy, 2024). Já o *Computer Emergency Response Team for the European Union* (CERT-EU), em cooperação com os *Computer Security Incident Response Team* (CSIRT) nacionais, atua na resposta a incidentes e partilha em tempo real de informações, constituindo um instrumento técnico essencial de harmonização (Comissão Europeia, 2018; INTERPOL, 2021). Embora não concebidas diretamente para a redução da cibercriminalidade, contribuem decisivamente para o ciberpoliciamento, nomeadamente na preservação de provas digitais e deteção precoce de incidentes.

No nível estratégico, a Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas (EMPACT 2022-2025) reforçou o combate a fenómenos como o *CaaS*,

caraterizado pela mercantilização de *botnets*, kits de *ransomware* ou ataques de negação de serviço distribuído (DDoS), ampliando o acesso a capacidades ofensivas (Curtis & Oxburgh, 2023; EUROPOL, 2025c). Esta abordagem confirma a necessidade de cooperação transnacional para enfrentar ameaças descentralizadas e altamente adaptáveis.

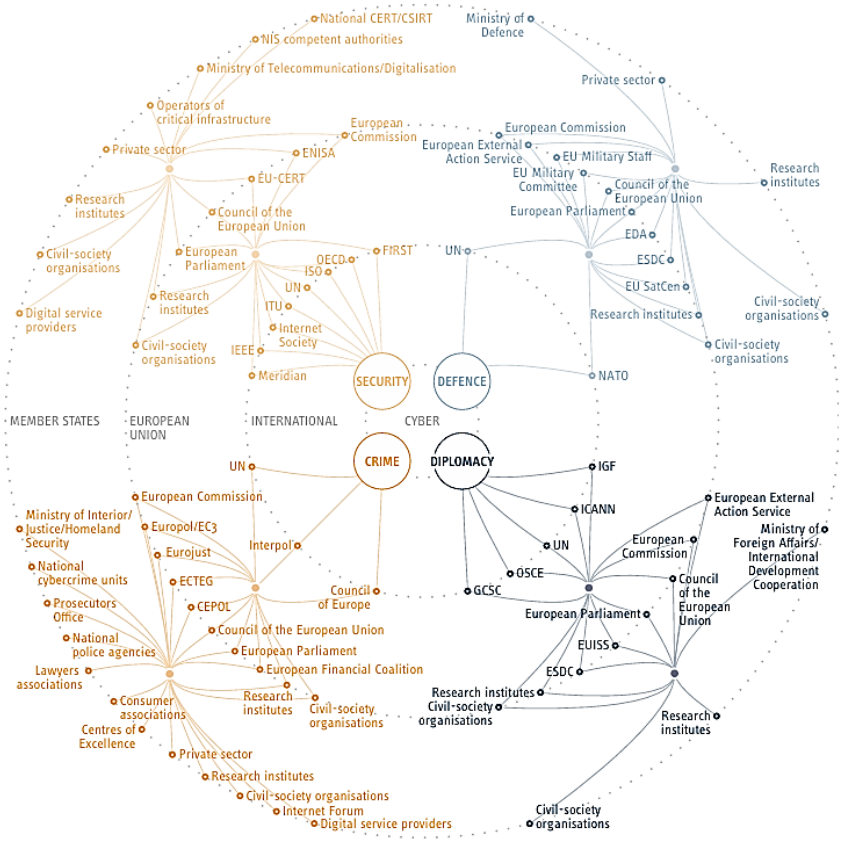
Nos Estados-Membros, a resposta organiza-se em unidades policiais especializadas em cibercrime e CSIRT nacionais. O modelo considerado mais eficaz combina uma unidade central coordenadora, apoiada por núcleos, assegurando uma cobertura territorial e pontos de contacto na rede 24/7 (Council of Europe, 2011). Contudo, a diversidade de enquadramentos jurídicos, maturidade tecnológica e prioridades nacionais impede uma uniformização plena (INTERPOL, 2021). Países como Estónia, Dinamarca e Noruega destacam-se por práticas inovadoras de ciberpoliciamento visível e uniformizado, em contraste com a maioria, que privilegia o policiamento não visível focado sobretudo na investigação criminal.

Apesar da solidez institucional deste quadro, subsistem desafios estruturais. A multiplicidade de atores proporciona sobreposições de competências e dependências da coordenação política, criando potenciais atrasos na resposta ao fenómeno (Carrapico & Barrinha, 2018). A governança europeia da cibersegurança permanece, assim, marcada por fragmentação institucional e tensões entre níveis nacionais e supranacionais, refletindo-se igualmente no domínio do ciberpoliciamento. Esta diversidade de estruturas e normativos — sistematizada no Apêndice C — evidencia simultaneamente a robustez e a complexidade da arquitetura europeia, marcada pela fragmentação e pela dependência de coordenação política.

Esta fragmentação é igualmente visível na pluralidade de atores e esferas de intervenção que integram a arquitetura europeia de governança multinível (Figura 5), revelando a coexistência de domínios de cibersegurança, ciberdefesa, cibercriminalidade e ciberdiplomacia que exigem coordenação e cooperação contínua.

Figura 5

Pluralidade de atores e esferas de intervenção na governança multinível da cibersegurança, cibercriminalidade, ciberdefesa e ciberdiplomacia



Fonte: Comissão Europeia (2018, p. 27).

Outro desafio reside na relação com o setor privado. Embora a Diretiva (UE) 2022/2555 tenha reforçado as obrigações de cooperação e reporte, a maioria das infraestruturas digitais e dos dados relevantes para investigações criminais está sob gestão de grandes empresas tecnológicas, muitas delas sediadas fora da UE. A cooperação permanece, em muitos casos, voluntária e condicionada por interesses económicos e jurídicos transnacionais (Wall, 2007; Broadhurst et al., 2014). Esta dependência fragiliza a autonomia das autoridades policiais e exige a formalização de parcerias público-privadas mais equilibradas, condição essencial para a eficácia operacional e para a ciber-resiliência (Comissão Europeia, 2018; Comissão Europeia, 2022; INTERPOL, 2021).

Neste contexto, o ciberpoliciamento deve ser entendido como uma parte integrante da governança multinível, na qual a polícia assume uma posição relativa entre múltiplos atores interdependentes (Dupont, 2020; Wall, 2011). Para que esta arquitetura se traduza em ganhos mensuráveis, é crucial adotar métricas de avaliação comuns, tais como o tempo de

resposta dos pontos de contacto 24/7, taxa de preservação e entrega de provas digitais, número de participações em operações internacionais ou de iniciativas de prevenção e proximidade *online* (Phillips et al., 2022; EUROPOL, 2025b).

Em síntese, a arquitetura evidencia um potencial acrescido, mas a sua legitimidade e eficácia dependem da capacidade de superar a fragmentação institucional, harmonizar mandatos, consolidar a cooperação público-privada e orientar a multiplicidade de atores para a coordenação de práticas favoráveis ao ciberpoliciamento, mais visível e próximo das comunidades digitais.

2.3. Formação e capacitação digital das autoridades policiais

Em diversos países europeus têm emergido experiências positivas de prevenção virtual no ciberespaço, particularmente em plataformas sociais e fóruns digitais, evidenciando o potencial do ciberpoliciamento enquanto extensão das práticas preventivas tradicionais (Virta, 2017). Apesar desses avanços, as próprias autoridades policiais reconhecem a existência de lacunas de formação que comprometem a capacidade de resposta face ao crescimento exponencial da cibercriminalidade. Esta insuficiência traduz-se numa menor eficácia tanto na investigação como na prevenção criminal, exigindo um investimento contínuo e sustentável em capacitação (Hull et al., 2018).

A literatura sublinha que a formação impacta não apenas o desempenho técnico, mas também a perceção pública da polícia. Curtis e Oxburgh (2023) demonstram que a qualificação adequada permite normalizar as respostas às denúncias, melhorar a comunicação com os cidadãos e reforçar a experiência de proximidade. Em contrapartida, a insuficiência de competências gera desconfiança social, compromete a legitimidade institucional e reduz a eficácia da resposta policial (Khan, 2024).

O défice formativo constitui, assim, um dos problemas mais urgentes para o ciberpoliciamento contemporâneo. Yar (2006) já salientava a dificuldade em recrutar e reter profissionais com competências técnicas especializadas. Mais recentemente, Matsaung e Masiloane (2025) confirmam que, para além das lacunas de conhecimento, a própria escassez de recursos alocados agrava o défice operacional, contribuindo para a morosidade e ineficácia das respostas policiais.

Este diagnóstico encontra eco no plano prático. Como reconhecido em entrevista constante em Apêndice B, “a formação é uma questão-chave, porque o combate à cibercriminalidade é, ainda assim, um domínio técnico (…) se nos dotarmos dos meios para uma formação extremamente rigorosa” (p. 59). Esta perspetiva sublinha a importância da

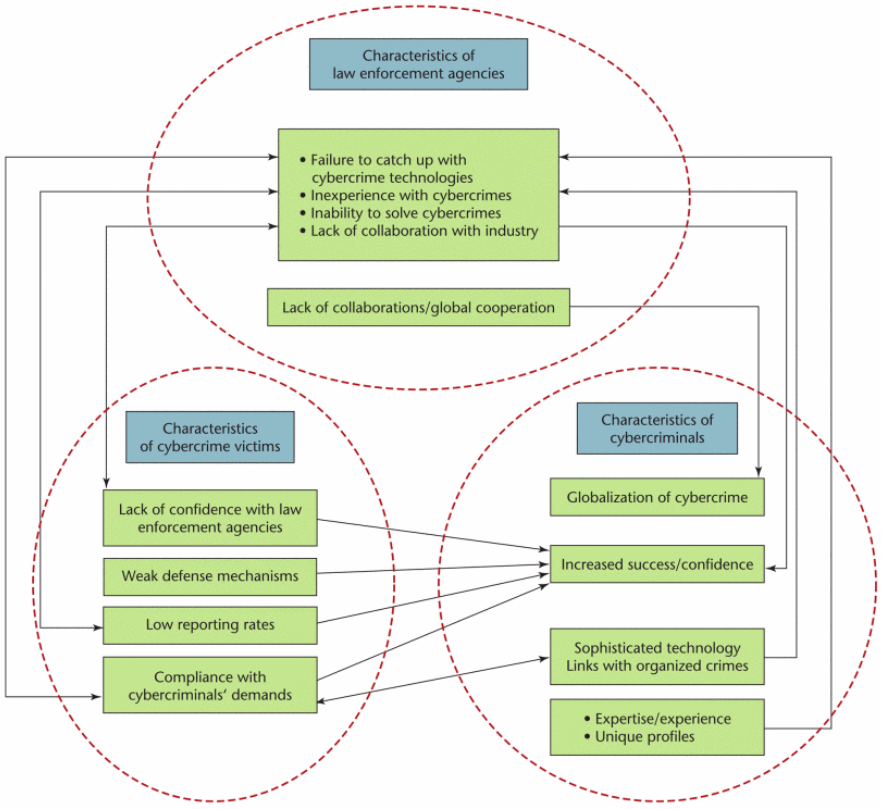
integração das competências digitais desde a entrada nas instituições policiais, reforçando a ideia de que a capacitação deve ser contínua e sistemática.

Contudo, a formação não deve se cingir a um processo meramente técnico. A Radicalisation Awareness Network (RAN, 2021) destaca que o ciberpoliciamento exige igualmente competências de comunicação digital, gestão de redes sociais, reconhecimento de comunidades virtuais, utilização de técnicas OSINT e sensibilização em cibersegurança. Estes elementos são cruciais para reforçar a confiança das comunidades, prevenir fenómenos como a radicalização *online* e os comportamentos ciberdesviantes.

Por outro lado, a capacitação deve ser enquadrada numa lógica organizacional mais ampla. A Figura 6 demonstra que as barreiras enfrentadas pelas autoridades policiais, vítimas e ofensores são interdependentes, em que a incapacidade de acompanhar a evolução tecnológica e consolidar colaborações eficazes agrava a confiança das vítimas, ao mesmo tempo que favorece a sofisticação e globalização das práticas criminosas (Kshetri, 2006).

Figura 6

Interdependências estruturais entre autoridades policiais, vítimas e cibercriminosos no ecossistema do cibercrime

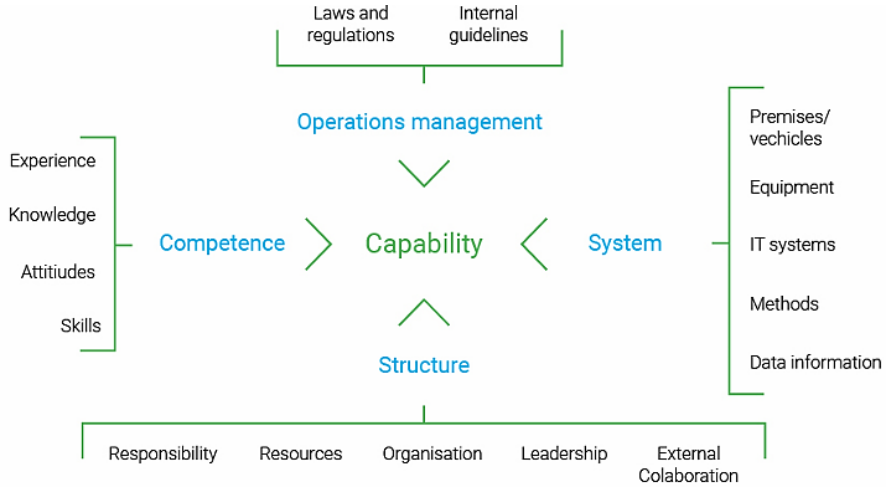


Fonte: Kshetri (2006, p. 35).

A superação destas barreiras depende da capacidade institucional de integrar múltiplas dimensões — competências individuais, sistemas tecnológicos, estruturas organizacionais — de forma coerente (Figura 7). Assim, a capacidade deve ser analisada não apenas num plano micro (ao nível do indivíduo), mas também no plano macro, considerando as lideranças, recursos, sistemas e colaborações externas.

Figura 7

Modelo de capacidade organizacional aplicado ao ciberpoliciamento



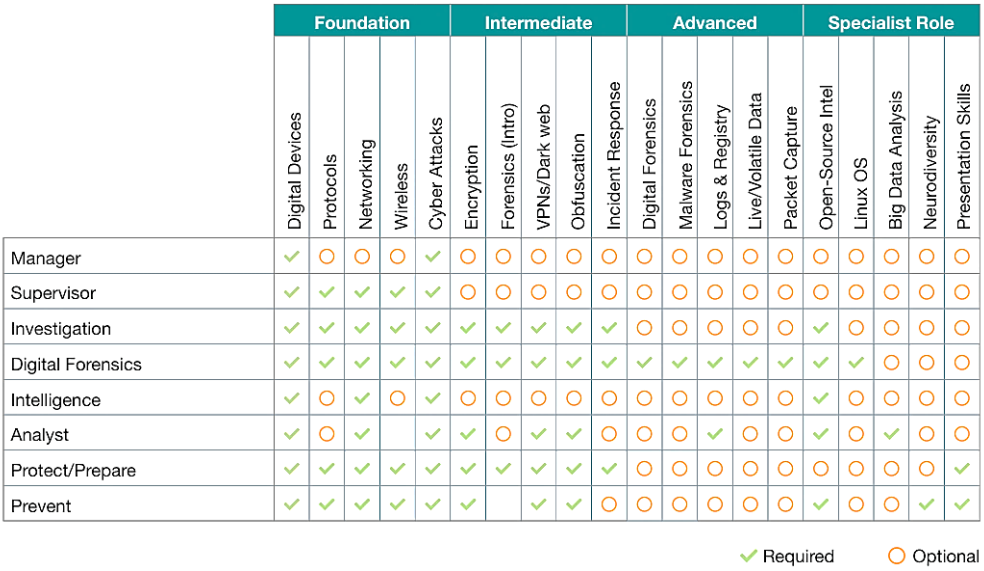
Fonte: EUROPOL (2025b, p. 12).

A este respeito a Comissão Europeia (2018) sublinha a importância da articulação entre entidades como a CEPOL, a EUROPOL e o *European Cybercrime Training and Education Group* (ECTEG), que promovem padrões comuns de formação e asseguram uma integração mais eficaz das autoridades policiais no ecossistema europeu de segurança.

Um aspeto decisivo consiste na diferenciação formativa. Como observa CMAGE (2022), embora algumas competências sejam transversais, nem todo o dispositivo policial necessita do mesmo tipo de instrução. Os planos formativos devem ajustados às funções operacionais, forenses, de inteligência ou preventivas, assegurando uma distribuição eficiente dos recursos disponíveis. A Figura 8 exemplifica esta diferenciação, evidenciando que a progressão formativa pode ser estruturada em níveis (fundamental, intermédio, avançado e especialista) e ajustada às funções específicas desempenhadas.

Figura 8

Requisitos de formação diferenciada para funções policiais no ciberpoliciamento



	Foundation					Intermediate					Advanced					Specialist Role				
	Digital Devices	Protocols	Networking	Wireless	Cyber Attacks	Encryption	Forensics (Intro)	VPNs/Dark web	Obfuscation	Incident Response	Digital Forensics	Malware Forensics	Logs & Registry	Live/Volatile Data	Packet Capture	Open-Source Intel	Linux OS	Big Data Analysis	Neurodiversity	Presentation Skills
Manager	✓	○	○	○	✓	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Supervisor	✓	✓	✓	✓	✓	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Investigation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	○	○	○	○	✓	○	○	○	○
Digital Forensics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	○	○
Intelligence	✓	○	✓	○	✓	○	○	○	○	○	○	○	○	○	○	✓	○	○	○	○
Analyst	✓	○	✓		✓	✓	○	✓	✓	○	○	○	✓	○	○	✓	○	✓	○	○
Protect/Prepare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	○	○	○	○	○	○	○	○	✓
Prevent	✓	✓	✓	✓	✓	✓		✓	✓	○	○	○	○	○	○	✓	○	○	✓	✓

✓ Required ○ Optional

Fonte: CMAGE (2022, p. 51).

Em síntese, a capacitação digital constitui um vetor estratégico para o ciberpoliciamento. A sua eficácia dependerá da superação de barreiras estruturais e da criação de mecanismos dinâmicos, colaborativos e permanentemente atualizados de formação. Tal implica uma abordagem multinível, que vá da aquisição de competências técnicas especializadas até ao reforço da comunicação às comunidades.

2.4. Dos dados à inteligência policial

No ciberpoliciamento, a escassez de informação estruturada, interoperável e tempestiva tem conduzido, com frequência, a respostas predominantemente reativas, evidenciando os limites dos métodos tradicionais perante fenómenos dinâmicos e transnacionais (Willits & Nowacki, 2016). Tal constatação reforça a importância da adoção do modelo de policiamento orientado pela inteligência (*Intelligence-Led Policing* - ILP), que visa transformar dados dispersos em inteligência utilizável, constituindo uma estrutura epistemológica e operacional que orienta a decisão policial para respostas antecipatórias, estratégicas e cooperativas (Matsaung & Masiloane, 2025; Ratcliffe, 2016).

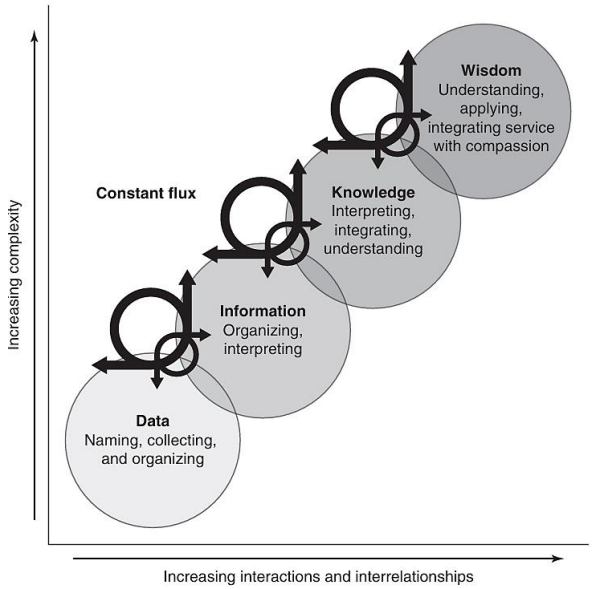
O ILP insere-se no paradigma *data-driven*, segundo o qual o policiamento se organiza em torno da recolha, integração e análise de dados provenientes de fontes heterogéneas, convertendo-os em conhecimento com valor operacional e estratégico. Esta transição é, simultaneamente, técnica e cultural: requer não apenas infraestrutura

tecnológica, mas também literacia de dados, formação especializada e cultura organizacional orientada para a evidência (Bravo, 2022; Dodge & Burruss, 2020).

Um modelo útil para compreender este processo é o *continuum DIKW*, que explicita a passagem de registos brutos a conhecimento aplicado. Segundo Rowley (2007), a ascensão nesta hierarquia depende de processos de contextualização e análise, e não de mera acumulação de dados. No contexto policial, dados brutos (*e.g. logs* de rede, metadados, denúncias) tornam-se informação quando normalizados e correlacionados; transformam-se em conhecimento quando agregados em padrões e *modus operandi*; e atingem o nível de sabedoria quando sustentam decisões estratégicas, como a definição de prioridades, afetação de meios ou desenho de medidas preventivas.

Figura 9

Modelo DIKW (Data, Information, Knowledge, Wisdom)



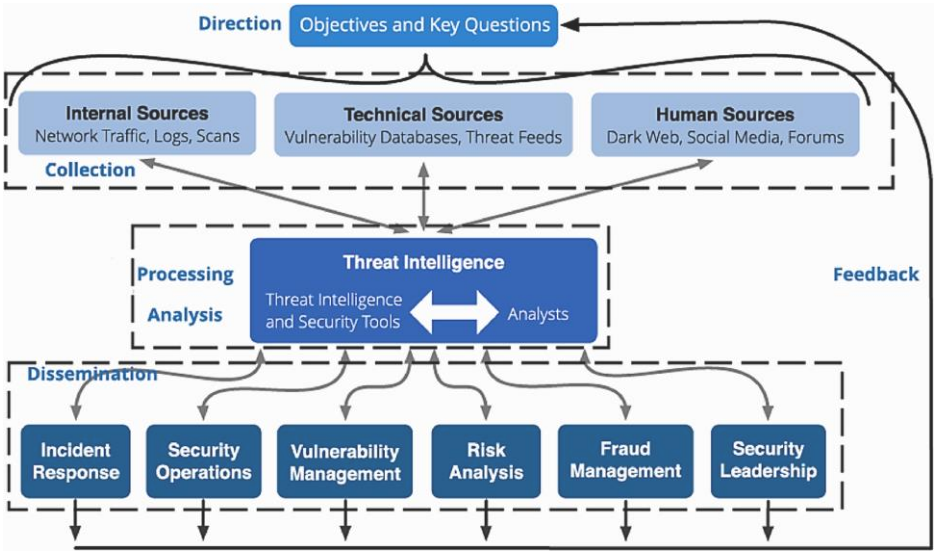
Fonte: American Nurses Association (2015, p. 5).

Neste contexto, o *Cyber Threat Intelligence* (CTI) assume um papel central no desenho operativo do ILP. O CTI estrutura-se num ciclo contínuo de direcionamento, recolha, processamento, análise, disseminação e retroalimentação, integrando fontes técnicas, humanas e abertas, transformadas por ferramentas e analistas em inteligência operacional (Cascavilla et al., 2021). O seu valor reside menos na recolha em si e mais na transformação constante de dados em conhecimento com aplicabilidade direta na investigação criminal, gestão de incidentes, prevenção e liderança estratégica.

A Figura 10 ilustra este ciclo replicado ao ciberpoliciamento, revelando a natureza interativa do processo e o papel decisivo do *feedback* para o aperfeiçoamento contínuo da resposta institucional.

Figura 10

Ciclo do CTI com aplicação ao ciberpoliciamento



Fonte: Cascavilla et al. (2021, p. 51).

A adoção do CTI aproxima as autoridades policiais de uma lógica preditiva de segurança, permitindo compreender padrões, em concordância com a Teoria dos Padrões Criminais, antecipar movimentos dos agentes de ameaça racionais e reduzir os tempos de resposta. Contudo, a eficácia do ciclo depende de parcerias público-privadas robustas, uma vez que grande parte das infraestruturas críticas e dados relevantes se encontra sob gestão de entidades privadas, frequentemente transnacionais (Tropina, 2017; EUROPOL, 2025b).

Neste contexto, a iniciativa *Police CyberAlarm* do Reino Unido ilustra uma prática de valor acrescentado e um exemplo de inteligência colaborativa por constituir um sistema de telemetria voluntária que capta metadados de tentativas de intrusão, encripta-os e envia-os a um centro nacional, partilhando os dados com as autoridades policiais e gerando relatórios de vulnerabilidades e de alertas em tempo real para diversas organizações (NEN, 2023).

De igual relevância é a integração de OSINT, vertente cada vez mais estruturante do ciberpoliciamento contemporâneo. A recolha e análise sistemática de informação proveniente de fontes abertas — redes sociais, fóruns, blogs e *marketplaces* e *Dark Web* —

ampliam a consciência situacional e permitem detetar precocemente tendências e comportamentos ciberdesviantes (Bravo, 2022; Cascavilla et al., 2021).

Conforme evidenciado na entrevista transcrita em Apêndice B "enfrentamos uma problemática de dados massivos (…) O nosso trabalho é captar esses dados, extraí-los e, depois, tratá-los (…) [para fornecer] uma leitura suficientemente clara aos nossos investigadores e analistas" (pp. 61-62). Tal relato evidencia o problema da sobrecarga informacional e a urgência de dotar as autoridades policiais de competências analíticas e ferramentas avançadas de *machine learning* e *natural language processing* para tratamento de grandes volumes de dados.

Ainda de acordo com a entrevista em Apêndice B, aplicações como a "Diagonal" e "GEND'élus" refletem o uso de dados e inteligência para reforçar a prevenção e a cidadania digital. Enquanto o primeiro realiza diagnósticos de vulnerabilidade e mede a ciber-higiene de entidades locais, a segunda promove a interação direta entre cidadãos e polícia, agilizando respostas e difundindo boas práticas. Estes exemplos projetam a noção de inteligência participativa, onde a informação é cocriada entre o Estado e cidadãos, num ecossistema de segurança partilhada (Comissão Europeia, 2018; RAN, 2021).

Em suma, a transição dos dados à inteligência policial consubstancia uma mudança de paradigma: do volume à relevância, da reação à antecipação, e da fragmentação à cooperação. Trata-se, portanto, de integrar a ciência de dados, inteligência colaborativa e aumentar a literacia institucional numa cultura de decisão informada, transparente e enquanto condição para a consolidação do ciberpoliciamento num ecossistema de segurança 4.0.

Discussão/Conclusão

O presente estudo analisou criticamente o ciberpoliciamento enquanto modelo operativo e estratégico das organizações policiais no contexto da Segurança 4.0, articulando dimensões teóricas, técnicas e institucionais. A análise permitiu compreender que o ciberpoliciamento se encontra num processo de consolidação conceptual e prática, refletindo as tensões entre inovação tecnológica, ética policial e governação multinível da segurança.

Os resultados obtidos permitem afirmar que a hipótese H1 foi refutada, uma vez que o conceito de ciberpoliciamento ainda não se encontra plenamente estruturado nem uniformemente reconhecido na literatura científica e na prática institucional. Apesar do crescente interesse académico e da sua integração progressiva nas organizações policiais de

diversos Estados-Membros, subsiste uma fragmentação terminológica, epistemológica e operacional.

A hipótese H2 foi confirmada, demonstrando que a consolidação do ciberpoliciamento depende da integração sistemática de competências digitais, analíticas, e éticas nos processos formativos e operacionais das autoridades policiais. A capacitação assume-se, assim, como vetor estratégico, não apenas técnico, mas também cultural e comunicacional, reforçando a legitimidade e a confiança social nas instituições policiais.

A hipótese H3 foi igualmente confirmada, evidenciando que a eficácia do ciberpoliciamento requer uma arquitetura de cooperação interinstitucional e parcerias público-privadas sólidas. A análise demonstra que a governação multinível constitui simultaneamente um potencial e desafio, dependendo da harmonização normativa, da interoperabilidade tecnológica e da partilha responsável de dados.

Por sua vez, a hipótese H4 foi corroborada, ao verificar-se que a eficácia depende da capacitação das autoridades policiais para integrar tecnologias emergentes de forma ética, transparente e orientada por dados. Modelos como o ILP e o CTI revelam-se essenciais para a transição de respostas reativas para abordagens preditivas e estratégias.

Do ponto de vista prático, o estudo sublinha a necessidade de políticas públicas e estratégias institucionais que reforcem a formação especializada, a interoperabilidade tecnológica e a literacia digital das autoridades policiais. A legitimação do ciberpoliciamento dependerá da sua capacidade para traduzir inteligência em ação preventiva e transformar a presença digital da polícia num instrumento de proximidade e proteção das comunidades.

Recomenda-se, para o caso português, a implementação de um modelo integrado de ciberpoliciamento na PSP, cuja configuração — centralizada ou descentralizada — atenda à capacitação humana e institucional, bem como à criação de equipa(s) multidisciplinar(es) capazes de integrar a prevenção, repressão, informações e investigação criminal. O modelo deverá assegurar interoperabilidade, análise colaborativa de dados e métricas de desempenho como as propostas no Apêndice D, promovendo a presença digital proativa, inteligência colaborativa e formação continua.

Por fim, em consonância com a linha de investigação futura identificada na Tabela 5, propõe-se aprofundar o estudo do ciberpoliciamento no metaverso, tomando como referência projetos-pilotos desenvolvidos pela EUROPOL (2022) e INTERPOL (2024), de modo a examinar criticamente os desafios éticos, jurídicos e operacionais associados à presença policial em espaços digitais imersivos.

Referências

Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the Dark Net: The question of detection and application. *Big Data and Cognitive Computing*, *8*(8), 91. https://doi.org/10.3390/bdcc8080091.

American Nurses Association. (2015). *Nursing Informatics: Scope and Standards of Practice*. Nursesbooks.org. https://cdn2.hubspot.net/hubfs/4850206.pdf.

Ayling, J. (2009). Criminal organizations and resilience. *International Journal of Law, Crime and Justice*, *37*(4), 182-196. https://doi.org/10.1016/j.ijlcj.2009.10.003.

Baldini, G., Barrero, J., Draper, G., Duch-Brown, N., Eulaerts, O., Geneiatakis, D., Joanny, G., Kerckhof, S., Lewis, A., Martin, T., Nativi, S., Neisse, R., Papameletiou, D., Hernandez Ramos, J. L., Reina, V., Ruzzante, G. L., Sportiello, L., Steri, G., Tirendi, S., Kounelis, I., (2020). *Cybersecurity, our digital anchor: a European perspective*. Publications Office of the European Union. https://doi.org/10.2760/352218.

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*(2), 169-217. https://doi.org/10.1086/259394.

Bergman, M. (2001). The deep web: Surfacing hidden value. *Journal of Electronic Publishing*, *7*(1). https://doi.org/10.3998/3336451.0007.104.

Brandão, A. (2016). European Union security actorness: the Comprehensive Approach hampered by policy differentiation. *Nação e Defesa*, *144*, 103-131.

Brantingham, P., & Brantingham, P. (2017). Environment, routine, and situation: Toward a pattern theory of crime. In R. Clarke & M. Felson (Eds.), *Routine activity and rational choice: Advances in criminological theory* (pp. 259-294). Routledge. https://doi.org/10.4324/9781315128788.

Bravo, R. (2022). *Segurança da Informação, Cibersegurança e Cibercrime: contributos para um alinhamento de conceitos*. https://www.academia.edu/40494857.

Brenner, S. (2004). Toward a criminal law for cyberspace: Distributed Security. *School of Law Faculty Publications*. https://ecommons.udayton.edu/cgi/viewcontent.cgi.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime,

International Journal of Cyber Criminology, *8*(1), 1-20. https://research-management.mq.edu.au/ws/portalfiles/portal/62156293/Publisher%20version%20(open%20access).pdf.

Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, *19*(3), 299-303. https://doi.org/10.1080/23745118.2018.1430712.

Carvalho, A. (2021). *A importância das informações para a segurança no ciberespaço*. Universidade de Lisboa. https://fenix.tecnico.ulisboa.pt/1126295043839208.pdf.

Cascavilla, G., Tamburri, D., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 1-29. https://doi.org/10.1016/j.cose.2021.102258.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199255771.001.0001.

Chan, J., Brereton, D., Legosz, M., & Doran, S. (2001). *E-policing: The impact of information technology on police practices*. Criminal Justice Commission. https://www.ccc.qld.gov.au/sites/default/files/2020-03/E-policing-Report-2001.pdf.

Chen, H., He, M., Xu, X., & Atkin, D. (2025). Examining older adults' vulnerability to online health scams: insights from routine activity theory. *Frontiers in Public Health*, *13*, 1-12. https://doi.org/10.3389/fpubh.2025.15858.

CMAGE. (2022). *Good Practice Guide: Establishing an Effective Law Enforcement Cybercrime Unit*. CREST. https://www.crest-approved.org/wp-content/uploads/2022/08/Establishing-an-Effective-Law-Enforcement-Cybercrime-Unit.pdf.

CNCS. (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608. https://doi.org/10.2307/2094589.

Comissão Europeia. (2018). *Operational guidance for the EU's international cooperation on cyber capacity building*. Publications Office. https://doi.org/10.2815/05153.

Comissão Europeia. (2020a). *Comunicação conjunta sobre a Estratégia de cibersegurança da UE para a década digital*. https://op.europa.eu/pt/publication-detail/-/publication/708647a6-3f94-11eb-b27b-01aa75ed71a1/language-pt.

Comissão Europeia. (2020b). *Comunicação sobre a Estratégia da UE para a União da Segurança*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605.

Comissão Europeia. (2020, julho 24). Estratégia da UE para a União da Segurança: integrar as medidas individuais num novo ecossistema de segurança. https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_1379.

Comissão Europeia. (2021). *Comunicação sobre a estratégia da UE para lutar contra a criminalidade organizada (2021-2025)*. eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021DC0170&from=IT.

Comissão Europeia. (2022). *SMEs and cybercrime: summary*. Publications Office of the European Union. https://doi.org/10.2837/89101.

Comissão Europeia. (2025a). *Comunicação sobre a estratégia da UE para lutar contra a criminalidade organizada (2021-2025)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0170.

Comissão Europeia. (2025b). *Comunicação sobre a ProtectEU: uma Estratégia Europeia de Segurança Interna*. https://op.europa.eu/pt/publication-detail/-/publication/035e206d-0fdb-11f0-b1a3-01aa75ed71a1/language-pt.

Comissão Europeia. (2025c). *Comunicação sobre o roteiro para o acesso lícito e efetivo aos dados para efeitos da aplicação da lei*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52025DC0349.

Conselho da Europa. (2001). *Convenção sobre Cibercrime*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Cornish, D., & Clarke, R. (2017). *The reasoning criminal: Rational choice perspectives on offending*. Taylor and Francis. https://doi.org/10.4324/9781315134482.

Council of Europe. (2011). *Specialised cybercrime units - Good practice study*. Data Protection and Cybercrime Division. https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33.

Crenshaw, M. (2010). *The consequences of counterterrorism*. Russell Sage Foundation.

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573-592. https://doi.org/10.1177/0032258X221107584.

Cybersecurity Ventures. (2025, maio 28). Cybercrime To Cost The World $12.2 Trillion Annually By 2031. *Cybercrime Magazine.* https://cybersecurityventures.com/official-cybercrime-report-2025/.

Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. Signal.

Department for Science, Innovation and Technology & Home Office. (2024). *Cyber Security Breaches Survey 2024*. UK Government. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024.

Dodge, C., & Burruss, G. (2020). Policing cybercrime: Responding to the growing problem and considering future solutions. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (pp. 339-358). Routledge.

Dupont, B. (2020). The ecology of cybercrime. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (pp. 389-407). Routledge.

ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. https://doi.org/10.2824/0710888.

EUCPN. (2020, janeiro). *Web-constables*. https://eucpn.org/document/web-constables.

EUROPOL. (2021a). *IOCTA 2021: internet organised crime threat assessment 2021.* Publications Office of the European Union. https://doi.org/10.2813/113799.

EUROPOL. (2021b). *The cyber blue line.* Publications Office of the European Union. https://doi.org/10.2813/26064.

EUROPOL. (2022). *Policing in the metaverse: what law enforcement needs to know: an observatory report from the Europol innovation lab*. Publications Office of the European Union. https://doi.org/10.2813/81062.

EUROPOL. (2024a). *AI and policing: the benefits and challenges of artificial intelligence for law enforcement*. Publications Office of the European Union. https://doi.org/10.2813/0321023.

EUROPOL. (2024b). *Decoding the EU's most threatening criminal networks*. Publications Office of the EU. https://doi.org/10.2813/811566.

EUROPOL. (2024c). *Internet organised crime threat assessment (IOCTA)*. Publications Office of the European Union. https://doi.org/10.2813/442713.

EUROPOL. (2025a). *Europol Programming Document 2025–2027*. EUROPOL. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf.

EUROPOL. (2025b). *Policing in an online world: relevance in the 21st century*. EUROPOL. https://doi.org/10.2813/4083983.

EUROPOL. (2025c). *The changing DNA of serious and organised crime: 2025*. Publications Office of the EU. https://doi.org/10.2813/0758057.

EUROSTAT. (2024a). *Digital economy and society statistics*. Publications Office of the European Union. https://ec.europa.eu/eurostat/statistics-explained/.

EUROSTAT. (2024b). *Young people's digital lives*. Publications Office of the European Union. https://ec.europa.eu/eurostat/statistics-explained/.

Floridi, L. (2011). *The philosophy of information*. Oxford University Press.

Furnell, S., & Dowling, S. (2019). Cyber-crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13-26. https://doi.org/10.1108/JCRPP-07-2018-0021.

Gabinete Cibercrime. (2025). *Nota Informativa: Cibercrime - Denuncias Recebidas 2024*. Procuradoria-Geral da República. https://cibercrime.ministeriopublico.pt/sites/default/files/2025-03.pdf.

Gibson, W. (1984). *Neuromancer*. Ace Books.

Harkins, M. (2016). *Managing risk and information security: Protect to enable*. Springer Nature. https://doi.org/10.1007/978-1-4842-1455-8.

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge. https://doi.org/10.4324/9781315775944.

Huey, L., & Ferguson, L. (2022). Cyberpolicing in Canada: a scoping review. *CrimRxiv*. https://doi.org/10.21428/cb6ab371.566eed0a.

Hull, M., Eze, T., & Speakman, L. (2018). Policing the cyber threat: Exploring the threat from cybercrime and the ability of local law enforcement to respond. In *2018 European Intelligence and Security Informatics Conference* (pp. 15-22). IEEE. https://doi.org/10.1109/EISIC.2018.00011.

INTERPOL. (2021). *National Cybercrime Strategy Guidebook*. https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf.

INTERPOL. (2023). *INTERPOL Global Cybercrime Conference 2023: Creating communities to protect communities*. https://www.interpol.int/en/content/download/20960/file/INTERPOL%20Global%20CybercrimeEST%20Conference%202023%20-%20Outcome%20Report.pdf.

INTERPOL. (2024). *Metaverse - A Law Enforcement Perspective: Use cases, Crime, Forensics, Investigation, and Governance*. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf.

Jardine, E. (2015). The Dark Web dilemma: Tor, anonymity and online policing. In *Global Commission on Internet Governance Paper Series*, (21). Centre for International Governance Innovation and Chatham House. https://dx.doi.org/10.2139/ssrn.2667711.

Khan, A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, *13*(44), 1-19. https://doi.org/10.3390/laws13040044.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, *4*(1), 33-39. https://doi.org/10.1109/MSP.2006.27.

Magán-Carrión, R., Abellán-Galera, A., Maciá-Fernández, G., & García-Teodoro, P. (2021). Unveiling the I2P web structure: a connectivity analysis. *Computer Networks*, *194*. https://doi.org/10.48550/arXiv.2101.03212.

Maia, C. (2019). *Ciberpoliciamento das redes sociais: o contributo das ciências tecnológicas*. ISCPSI. https://comum.rcaap.pt/handle/10400.26/34925.

Marcum, C., & Higgins, G. (2019). Cybercrime. In E. Viano (Ed.), *Handbook on crime and deviance* (pp. 459-475). Springer International Publishing.

Martin, P. (2024). Tem top tips on insider risk. *Crest Security Review*. https://crestresearch.ac.uk/download/5229/csr19_martin.pdf.

Matsaung, P., & Masiloane, D. (2025). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *African Security Review*, *34*(2), 152-167. https://doi.org/10.1080/10246029.2024.2421225.

McGuire, M., & Dowling, S. (2013). *Cyber Crime: A Review of the Evidence*. Home Office. https://assets.publishing.service.gov.uk/government/uploads.pdf.

Murphy, C. (2024).*Understanding cybercrime*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf.

NATO. (2017). *Warsaw Summit Key Decisions*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf.

NEN. (2023). *Police Cyber Alarm - A review*. https://www.nen.gov.uk/wp-content/uploads/2023/05/NEN_CyberAlarm_v0.4.pdf.

Ning, H., Lin, Y., Wang, W., Wang, H., Shi, F., Zhang, X., & Daneshmand, M. (2023). Cyberology: Cyber–physical–social-thinking spaces-based discipline and interdiscipline hierarchy for metaverse (general cyberspace). *IEEE Internet of Things Journal*, *10*(5), 4420-4430. https://doi.org/10.1109/JIOT.2022.3217821.

Parlamento Europeu, & Conselho da União Europeia. (2019). Regulamento (UE) 2019/881 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação de cibersegurança das TIC (Cybersecurity Act). *Jornal Oficial da União Europeia*, *L 151*, 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj.

Pereira, S. (2022). *Cibersegurança: o papel da Polícia de Segurança Pública na prevenção do cibercrime*. ISCPSI. http://hdl.handle.net/10400.26/41482.

Pfleeger, C., Pfleeger, S. & Margulies, J. (2015). *Security in Computing*. Pearson.

Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398. https://doi.org/10.3390/forensicsci2020028.

Poiares, N. (2019). Cibersegurança, literacia e resiliência digital dos idosos. *Anuário Janus*, *19*, 118-119.

Polícia de Segurança Pública. (2025). *Plano de Atividades da PSP 2025*. https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Plano%20de%20Atividades/2025%20-%20Plano%20de%20Atividades%20da%20PSP.pdf.

Procuradoria-Geral da República. (2025). *Estratégia Cibercrime 2025/2027: mais eficácia na investigação*. https://www.ministeriopublico.pt/sites/default/files/2025-03/estrategia-cibercrime-marco-2025.pdf.

Prosegur Research. (2022). *Criminal technological innovation*. Prosegur Research. https://www.prosegurresearch.com/dam/jcr.pdf.

Radulov, N. (2019). Ecosystem of Security 4.0. *Security & Future*, *3*(3), 69-70. https://stumejournals.com/journals/confsec/2019/3/69.full.pdf.

RAN. (2021). *Community police and the online dimension*. https://home-affairs.ec.europa.eu/system/files/2022-05/ran_pol_community_police_and_the_online_dimension_05072021_en.pdf.

Ratcliffe, J. (2016). *Intelligence-led policing*. Routledge. https://doi.org/10.4324/9781315717579.

Regian, J., & Noever, D. (2017). Generative representation of synthetic threat actors for simulation and training. *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*, Paper 17140. https://www.researchgate.net/publication/323943187.

Reyns, B., Henson, B., & Fisher, B. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169. https://doi.org/10.1177/0093854811421448.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of information science*, *33*(2), 163-180. https://doi.org/10.1177/0165551506070706.

Sharma, G., Vidalis, S., Menon, C., Anand, N., & Kumar, S. (2021). Analysis and implementation of threat agents profiles in semi-automated manner for a network traffic in real-time information environment, *Electronics*, *10*(15), 1-18. https://doi.org/10.3390/electronics10151849.

Simon, H. (1997). *Models of bounded rationality: Empirically grounded economic reason*. The MIT Press. https://doi.org/10.7551/mitpress/4711.001.0001.

Sistema de Segurança Interna. (2025). *Relatório Anual de Segurança Interna 2024*. https://www.portugal.gov.pt/download-ficheiros.pdf.

Thomas, D., & Loader, B. (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.

Tropina, T. (2017). Cyber-policing: the role of the police in fighting cybercrime. *European Police Science and Research Bulletin*, (2), 287-294. https://doi.org/10.2825/13491.

Vidalis, S., & Jones, A. (2005). Analyzing threat agents and their attributes. In *4th European Conference on Information Warfare and Security 2005*, *ECIW 2005* (pp. 369-379). Academic Conferences International. https://www.researchgate.net/publication/220947230.

Virta, S. (2017). Future preventive policing. *European Police Science and Research Bulletin*, (2), 135-142. https://doi.org/10.2825/13491.

Wall, D. (2001). Cybercrimes and the internet. In D. Wall (Ed.), *Crime and the internet* (pp. 1-17). Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press

Wall, D. (2011). Policing cybercrimes: Situating the public police in networks of security within cyberspace. Police Practice and Research: *An International Journal*, *8*(2), 183-205. https://doi.org/10.1080/15614260701377729.

Wang, Y., Arief, B., & Hernandez-Castro, J. (2025). Secure in the dark? An in-depth analysis of dark web markets security. *International Journal of Information Security*, *24*(3), 1-15. https://doi.org/10.1007/s10207-025-01015-1.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies*, *29*(2), 105-124. https://doi.org/10.1080/1478601X.2016.1170282.

Yar, M. (2006). *Cybercrime and Society*. Sage Publications.

Yesmen, N., & Ahmed, N. (2022). The nature and challenges of cyber policing: A study on criminal investigation department. *Asian Journal of Sociological Research*, *5*(1), 210-214. https://journalsociology.com/index.php/AJSR/article/view/71.

Zalewski, P. (2025). Selected aspects of cyberspace security. The Internet as a “service area” of the virtual patrol of the Polish Police. *Security Dimensions*, (49), 159-181. https://www.researchgate.net/publication/394925723.

Apêndice A

Mapeamento científico com representações gráficas e tabelas complementares

Tabela A1

Resultados da pesquisa por palavras-chave segundo o tipo de fonte

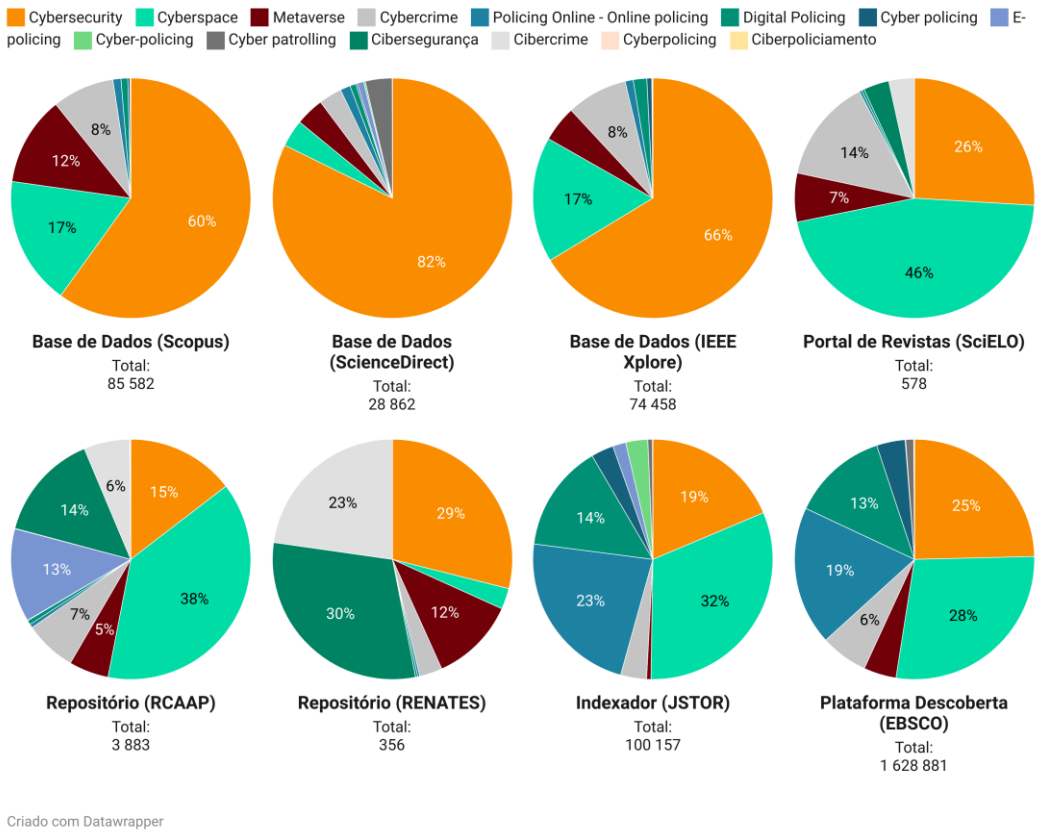
Palavras-chave	Bases de Dados			Portal de Revistas	Repositórios		Indexador	Plataforma Descoberta
	Scopus	Science Direct	IEEE Xplore	SciELO	RCAAP	RENATES	JSTOR	EBSCO
Cibercrime	7	1	3	20	240	81	10	561
Ciberpatrulhamento	0	0	0	0	0	0	0	0
Ciberpoliciamento	0	0	0	0	4	0	0	4
Cibersegurança	14	6	0	20	563	108	39	1217
Cyber patrolling	18	1044	73	0	0	0	626	17399
Cyber policing	245	62	497	0	2	0	3047	62671
Cyber-policing	21	62	10	0	2	0	2971	294
Cybercrime	7134	898	6111	81	271	11	3498	104044
Cyberpolicing	6	2	0	0	2	0	1	62
Cyberspace	14805	1057	12579	265	1494	10	31643	453795
Cybersecurity	51290	23743	49394	150	566	103	18684	401010
Digital policing	787	232	1359	2	23	1	14513	210600
E-policing	24	252	16	0	489	0	1772	886
Metaverse	10303	1108	3607	38	208	41	591	71678
Policing online <OR> Online policing	928	395	809	2	19	1	22762	304660

Fonte: Elaborado pelo próprio (2025).

Nota. Os dados foram recolhidos entre 29 de agosto de 2025 e 1 de setembro de 2025. As pesquisas foram realizadas em português e em inglês, sem delimitação temporal prévia. Os números apresentados refletem o total bruto de documentos, privilegiando, a pesquisa por palavras-chave, título e resumo (*abstract*). Os resultados podem incluir duplicações decorrentes da existência de diferentes versões do mesmo documento em distintas fontes.

Gráfico A1

Representação percentual dos resultados da pesquisa por palavras-chave, segundo o tipo de fonte



Fonte: Elaborado pelo próprio (2025). Gráfico interativo disponível em https://danet/T8snx/2/.

Tabela A2

Distribuição de resultados da pesquisa por palavras-chave, categorizados segundo as áreas temáticas da Scopus

Palavras-chave	Ciências Sociais	Ciência da Computação	Engenharia	Medicina	Ciências da Decisão	Negócios, Gestão e Contabilidade
Cibercrime	6	1	1	1	0	0
Ciberpatrulhamento	0	0	0	0	0	0
Ciberpoliciamento	0	0	0	0	0	0
Cibersegurança	8	6	0	0	0	0
Cyber patrolling	2	13	6	1	5	1
Cyber policing	172	104	55	20	9	18
Cyber-policing	17	5	4	0	2	2
Cybercrime	2880	4257	1995	572	867	619
Cyberpolicing	4	3	3	2	1	0
Cyberspace	6578	6733	3489	737	981	1165

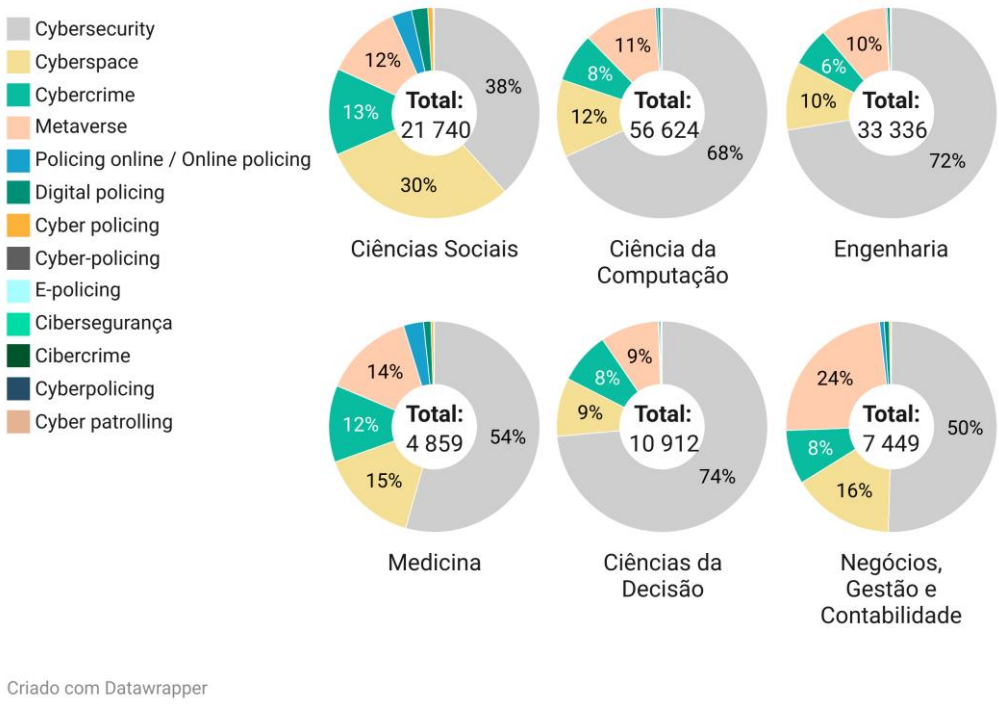
Cybersecurity	8332	38635	24133	2643	8022	3761
Digital policing	542	236	135	55	23	59
E-policing	9	12	8	1	2	4
Metaverse	2518	6421	3435	678	979	1768
Policing online <OR> Online policing	672	198	72	149	21	52

Fonte: Elaborado pelo próprio (2025).

Nota. Os dados foram recolhidos da Scopus entre 29 de agosto de 2025 e 1 de setembro de 2025. As pesquisas foram realizadas em português e em inglês, sem delimitação temporal prévia. Os números apresentados refletem o total bruto de documentos, restrito às áreas temáticas mais representativas, privilegiando a pesquisa por palavras-chave, título e resumo (*abstract*). Os resultados podem incluir duplicações decorrentes da existência de diferentes versões ou registos do documento na base de dados.

Gráfico A2

Representação percentual dos resultados da pesquisa por palavras-chave, conforme a categorização temática da Scopus



Fonte: Elaborado pelo próprio (2025). Gráfico interativo disponível em https://danet/BOKrY/1/.

Tabela A3

Distribuição de resultados da pesquisa por palavras-chave, segundo o tipo de documentos definidos pela Scopus

Palavras-chave	Artigo	*Conference Paper*	Capítulo de Livro	Livro	Revisão de Conferência	Outros
Cibercrime	6	1	0	0	0	0

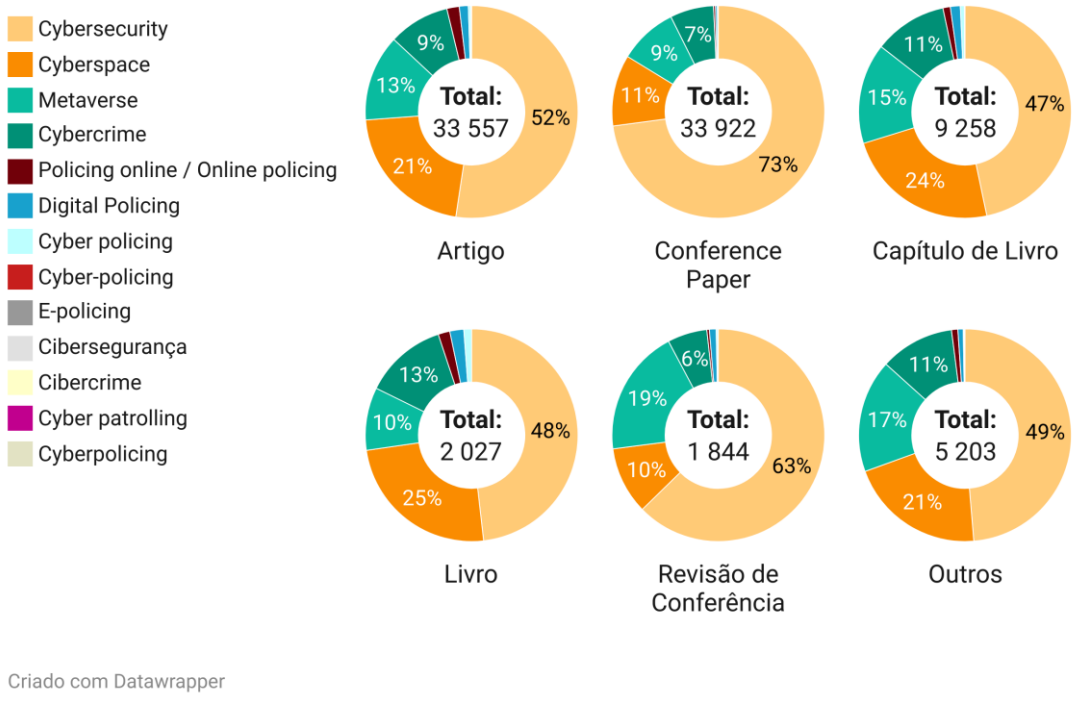
Ciberpatrulhamento	0	0	0	0	0	0
Ciberpoliciamento	0	0	0	0	0	0
Cibersegurança	9	4	0	0	0	1
Cyber patrolling	4	10	2	0	0	2
Cyber policing	119	30	58	24	5	9
Cyber-policing	15	3	1	0	0	2
Cybercrime	3121	2249	1031	256	111	588
Cyberpolicing	3	2	1	0	0	0
Cyberspace	7182	3680	2176	497	189	1081
Cybersecurity	17579	24721	4324	977	1156	2533
Digital Policing	460	94	139	43	19	42
E-policing	11	5	4	0	1	0
Metaverse	4415	3025	1418	194	356	895
Policing online <OR> Online policing	633	98	104	36	7	50

Fonte: Elaborado pelo próprio (2025).

Nota. Os dados foram recolhidos da Scopus entre 29 de agosto de 2025 e 1 de setembro de 2025. As pesquisas foram realizadas em português e em inglês, sem delimitação temporal prévia. Os números apresentados refletem o total bruto de documentos, por tipo de documentos mais representativos, privilegiando a pesquisa por palavras-chave, título e resumo (*abstract*). Os resultados podem incluir duplicações decorrentes da existência de diferentes versões ou registos do documento na base de dados.

Gráfico A3

Representação percentual dos resultados da pesquisa por palavras-chave, segundo o tipo de documentos definidos pela Scopus



Fonte: Elaborado pelo próprio (2025). Gráfico interativo disponível em https://danet/F1gLl/2/.

Tabela A4

Resultados por palavras-chave organizados por país na base de dados da Scopus

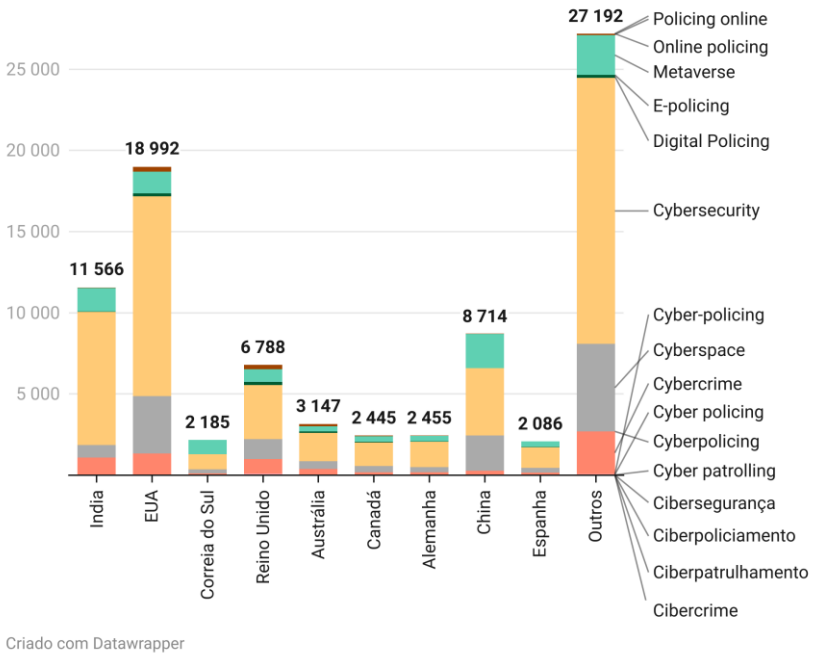
Palavras-chave	Índia	EUA	Coreia do Sul	Espanha	Reino Unido	Austrália	Canadá	Alemanha	China	Outros
Cibercrime	0	0	0	2	0	0	0	0	0	5
Ciberpatrulhamento	0	0	0	0	0	0	0	0	0	0
Ciberpoliciamento	0	0	0	0	0	0	0	0	0	0
Cibersegurança	0	1	0	0	0	0	1	0	0	12
Cyber patrolling	1	6	0	1	2	0	1	0	1	6
Cyber policing	15	36	2	2	83	38	16	10	4	39
Cyber-policing	0	0	0	0	4	8	3	1	1	4
Cybercrime	1080	1293	104	162	903	350	164	181	266	2631
Cyberpolicing	3	2	1	1	0	0	0	0	0	0
Cyberspace	760	3527	260	295	1229	475	390	304	2182	5383
Cybersecurity	8203	12305	924	1269	3334	1734	1433	1564	4134	16390
Digital Policing	25	184	5	6	211	91	51	26	14	174
E-policing	3	5	0	0	4	1	2	1	0	5
Metaverse	1452	1332	879	336	763	322	331	348	2095	2445
Policing online <OR> Online policing	24	301	10	12	255	128	53	20	17	98

Fonte: Elaborado pelo próprio (2025).

Nota. Os dados foram recolhidos da Scopus entre 29 de agosto de 2025 e 1 de setembro de 2025. As pesquisas foram realizadas em português e em inglês, sem delimitação temporal prévia. Os números apresentados refletem o total bruto de documentos, pelos países mais representativos, privilegiando a pesquisa por palavras-chave, título e resumo (*abstract*). Os resultados podem incluir duplicações decorrentes da existência de diferentes versões ou registos do documento na base de dados.

Gráfico A4

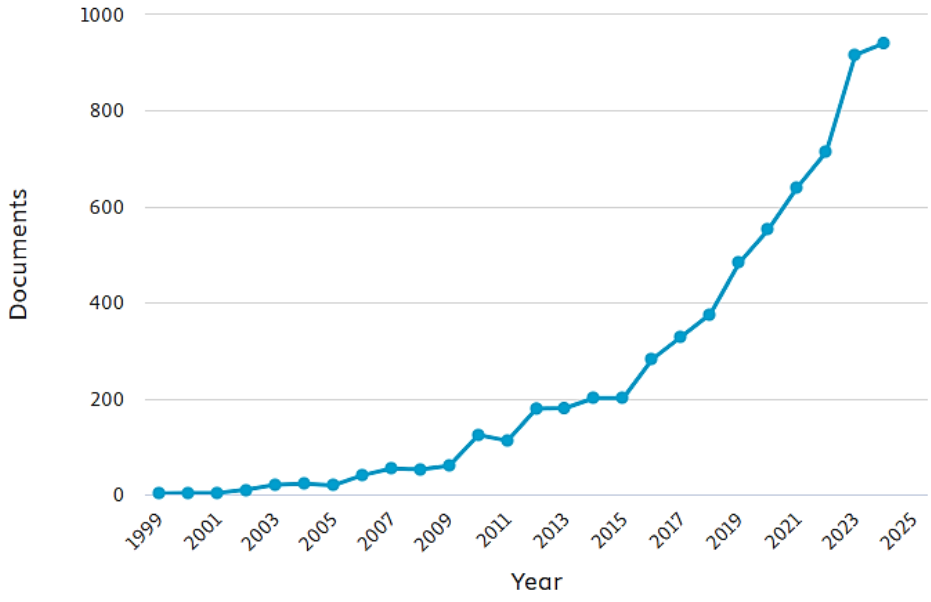
Distribuição dos resultados da pesquisa por palavras-chave, pelos países mais representativos de acordo com os dados da Scopus



Fonte: Elaborado pelo próprio (2025). Gráfico interativo disponível em https://danet/PW1pE/1/.

Gráfico A5

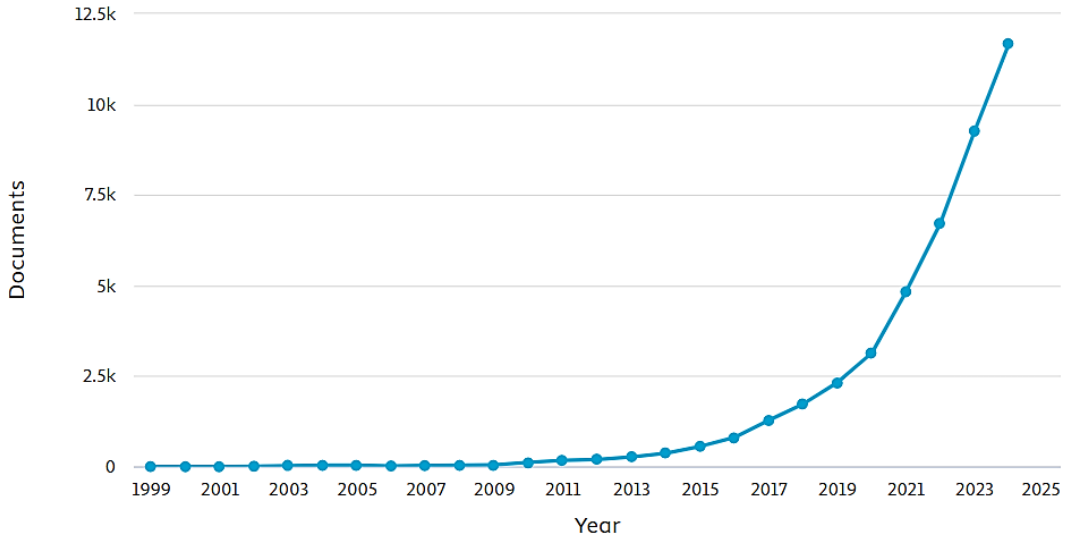
Evolução da produção científica do cibercrime até 2024 através da pesquisa da palavra-chave "cybercrime", de acordo com os dados da Scopus



Fonte: Scopus (2025, agosto 30). Disponível em https://www.scopus.com/term/analyzer.uri.

Gráfico A6

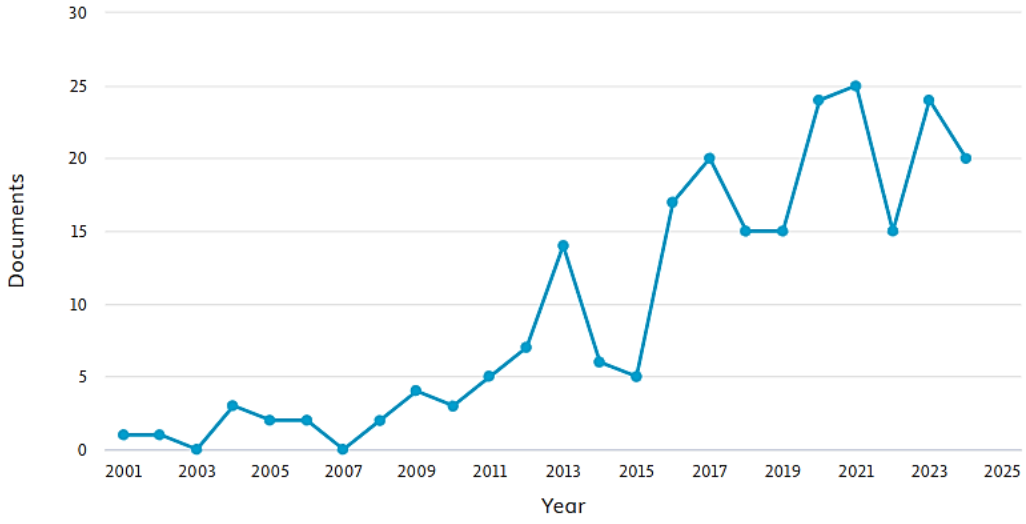
Evolução da produção científica do cibersegurança até 2024 através da pesquisa da palavra-chave "cybersecurity", de acordo com os dados da Scopus



Fonte: Scopus (2025, agosto 30). Disponível em https://www.scopus.com/term/analyzer.uri.

Gráfico A7

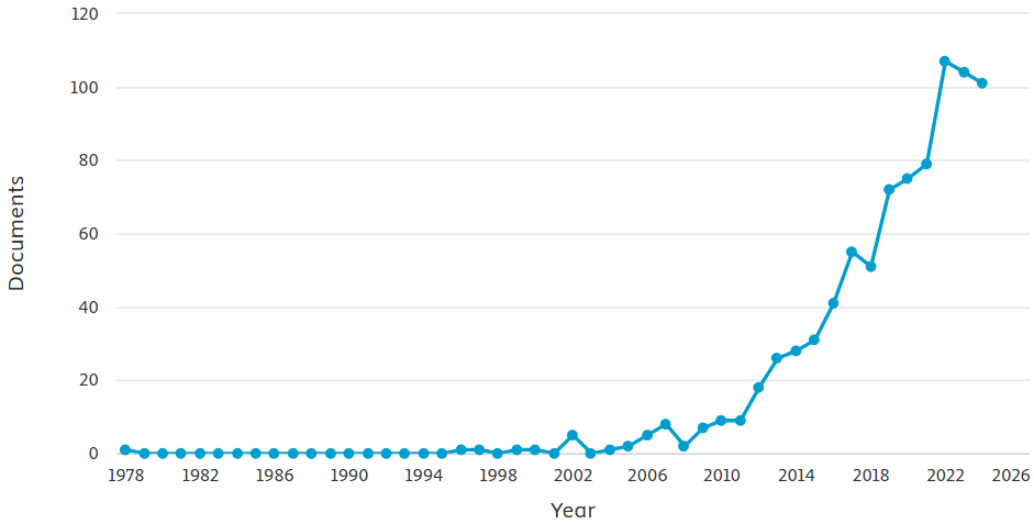
Evolução da produção científica do ciberpoliciamento até 2024 através da pesquisa da palavra-chave "cyber policing", de acordo com os dados da Scopus



Fonte: Scopus (2025, agosto 30). Disponível em https://www.scopus.com/term/analyzer.uri.

Gráfico A8

Evolução da produção científica do ciberpoliciamento até 2024 através da pesquisa das palavras-chave "online policing" e "policing online" de acordo com os dados da Scopus



Fonte: Scopus (2025, agosto 30). Disponível em https://www.scopus.com/term/analyzer.uri.

Apêndice B

Transcrição e tradução bilingue (francês/português) de entrevista

Tabela B1

Elementos essenciais de informação no âmbito da transcrição e tradução de entrevista

Elementos essenciais de informação	Descrição
Fonte (nome do canal e entidade)	Francophone Business TV – Youtube.
Título original do vídeo	*Interview du colonel Hervé PETRY chef de l'Unité Nationale Cyber par Ali JIAR*.
Link (URL) e acesso integral	https://www.youtube.com/watch?v=sDIjiYswehk. Disponível no Vídeo A2.
Data e hora da publicação	2024-12-18 às 10:38:27 GMT.
Entrevistado	Coronel Hervé Marie Bernard Pétry.
Entrevistador	Ali Jiar.
Idioma original/traduzido	Francês/Português.
Tradução	Elaborado pelo próprio.
Duração	14:45.
Observações	O objetivo da entrevista é dar a conhecer, através do responsável pela Divisão de Proximidade Digital da *Gendarmerie Nationale* em França, as atribuições e missões da Unidade Nacional Cyber, denominada por *UNCyber*.

Fonte: Elaborado pelo próprio (2025).

00:11 – Entrevistador (Ali Jiar): Bonjour à tous. Bienvenue sur ce nouveau format d'information de l'unité nationale cyber. Aujourd'hui, nous avons la chance de recevoir le colonel Pétry. Mon colonel, bonjour.

Tradução: Bom dia a todos. Bem-vindos a este novo formato de informação sobre a unidade nacional *cyber*. Hoje, temos a sorte de receber o Coronel Pétry. Meu coronel, bom dia.

00:19 – Entrevistado (Coronel Pétry): Bonjour Ali.

Tradução: Bom dia, Ali.

00:20 – Entrevistador (Ali Jiar): Alors, mon colonel, vous avez pris le commandement de l'unité nationale cyber le 1er février. Mais avant cela, parlez-nous un petit peu de, de votre parcours.

Tradução: Ora, meu coronel, assumiu o comando da unidade nacional *cyber* a 1 de fevereiro. Mas, antes disso, fale-nos um pouco do, do seu percurso.

00:27 – Entrevistado (Coronel Pétry): D'abord, merci pour cette invitation et merci de me recevoir. Eh bien, tout simplement, moi je suis un colonel de gendarmerie qui a 27 ans de service, et qui a un profil, avant tout en police judiciaire, et spécialiste aussi des questions de renseignement, renseignement criminel. Donc, un profil assez atypique, on va dire, en Gendarmerie. Puis, puisque tourné très tôt vers l'investigation au sens large, avec un parcours également à l'international, avec 4 années passées en ambassade à Pékin, qui m'a aussi ouvert

sur toutes les problématiques de criminalité organisée, de manière sur les aspects transnationaux. Donc voilà un peu quel est, quel est mon parcours 27 ans de service, un passage en gendarmerie départementale, gendarmerie mobile, en administration centrale et puis, depuis maintenant une quinzaine d'années, en police judiciaire.

Tradução: Antes de mais, obrigado pelo convite e por me receberem. Pois bem, sou coronel da *Gendarmerie*, tenho 27 anos de serviço e um perfil, antes de mais, em polícia judiciária, sendo também especialista em questões de informação, informação criminal. Portanto, um perfil bastante atípico, diria, na *Gendarmerie*, por estar muito cedo orientado para a investigação em sentido amplo, com um percurso também internacional: passei 4 anos numa embaixada em Pequim, o que me abriu o horizonte sobre todas as problemáticas da criminalidade organizada, nos seus aspetos transnacionais. Eis, em suma, o meu percurso: 27 anos de serviço, uma passagem pelos Departamentos da *Gendarmerie*, *Gendarmerie* Móvel, pela administração central e, há cerca de quinze anos, na Polícia Judiciária.

01:12 – Entrevistador (Ali Jiar): Oui, et puis un passage à la direction centrale de la police judiciaire. Vous étiez le numéro deux du service central de renseignement criminel, mon colonel. Donc, effectivement, une belle expérience sur ces questions d'investigation. Mon colonel, avant de commencer, comment est née cette unité nationale, et quelles sont ses missions pour les gens qui, qui nous regardant?

Tradução: Sim, e também uma passagem pela Direção Central da Polícia Judiciária. Foi o número dois do Serviço Central de Informação Criminal, meu Coronel. Portanto, de facto, uma bela experiência nestas questões de investigação. Meu coronel, antes de começarmos: como nasceu esta unidade nacional e quais são as suas missões para quem nos está a ver?

01:27 – Entrevistado (Coronel Pétry): Alors, la gendarmerie s'est pas réveillée hier matin pour se doter de compétence et de capacité en matière de cyber. En faite, ça fait déjà plus d'une vingtaine d'années qu'on a des entités dédiées à la lutte contre la cybercriminalité. Mais, à partir de 2021, la direction générale de la gendarmerie a décidé d'agréger ses forces pour constituir, bem... une force de frappe en réalité. Et, de 2021 à 2023, on avait un commandement qui s'appelait le "ComCyberGend" à l'époque. Et puis, fin 2023, il a été décidé, par le ministre de l'Intérieur, de créer un service à compétence nationale, au sein du Ministère, pour agréger un peu tout, toutes les, les forces dédiées à la cybercriminalité du ministère de l'Intérieur, aussi bien gendarmerie, que police, que préfecture de police. Donc, il est né, au sein de ce Ministère, un service à compétence nationale, pour le ministre qui s'appelle le Commandement du Ministère de l'Intérieur dans le Cyberespace. Et la création de ce service, à compétence nationale, encore une fois, qui a vocation à agréger un peu le travail de tout le monde, bem, nous a amené, au sein de la Gendarmerie, à revoir un peu notre organisation, et de modifier le "ComCyberGend" d'avant, et d'en faire une nouvelle unité nationale cyber, l'unité nationale cyber que je commande depuis le 1er février. Donc, en gros, naissance de l'unité nationale cyber à la faveur d'un arrêté de fin d'année 2023, et moi, je prends le commandement le 1er février 2024, avec pour feuille de route, dans un premier temps, bem, de poser les bases de cette nouvelle unité, mettre en ordre de marche, organiser, tout en continuant être sur les, les dossiers, les dossiers d'investigation, les grands,

les grandes enquêtes que nous menons, et lancer l'ensemble. Voilà, voilà. Donc, c'est comme ça qui est né cette nouvelle unité nationale cyber.

Tradução: A *Gendarmerie* não acordou ontem de manhã para dotar-se de competências e capacidades em matéria de *cyber*. Na verdade, já há mais de vinte anos que temos entidades dedicadas ao combate à cibercriminalidade. Mas, a partir de 2021, a Direção-Geral da *Gendarmerie* decidiu agregar as suas forças para constituir, enfim… uma verdadeira força de choque. Entre 2021 e 2023, tínhamos um comando chamado, à época, "ComCyberGend". E, no final de 2023, foi decidido pelo Ministro do Interior criar um serviço com competência nacional, no seio do Ministério, para agregar um pouco todas as forças dedicadas à cibercriminalidade do Ministério do Interior — tanto *Gendarmerie*, como Polícia [Nacional], como a Prefeitura de Polícia. Assim nasceu, no seio deste Ministério, um serviço com competência nacional para o Ministro, chamado Comando do Ministério do Interior para o Ciberespaço. E a criação deste serviço, com competência nacional, que tem vocação para agregar o trabalho de todos, levou-nos, no seio da *Gendarmerie*, a rever a nossa organização, a modificar o antigo "ComCyberGend" e a transformá-lo numa nova unidade nacional *cyber* — a unidade nacional *cyber* que comando desde 1 de fevereiro. Em suma: nascimento da unidade nacional *cyber* por força de um decreto do final de 2023, e eu assumo o comando a 1 de fevereiro de 2024, com a missão inicial de estabelecer as bases desta nova unidade, colocá-la em ordem de marcha, organizá-la, continuando ao mesmo tempo nos processos, os processos de investigação, as grandes investigações que conduzimos, e prosseguir em conjunto. É assim que nasceu esta nova unidade nacional *cyber*.

03:03 – Entrevistador (Ali Jiar): Alors, mon, mon colonel, vous êtes justement au plus près de nos concitoyens. Et récemment, vous étiez donc avec votre unité et vos équipes au sein du Salon des Maires, du 19 au 21 novembre. Quels sont les messages que vous avez passé aux maires et aux élus des collectivités territoriales, quand on sait que ce sont souvent les premières victimes de ces cyberattaques?

Tradução: Meu, meu coronel, está precisamente muito próximo dos nossos concidadãos. Recentemente, esteve com a sua unidade e as suas equipas no *Salon des Maires*, de 19 a 21 de novembro. Que mensagens transmitiu aos Presidentes de Câmara Municipal e aos eleitos das coletividades territoriais, sabendo que são, muitas vezes, as primeiras vítimas destes ciberataques?

03:20 – Entrevistado (Coronel Pétry): Ben, ce qu'il faut comprendre, d'abord, c'est que on ne fait pas de la lutte contre la cybercriminalité uniquement par un volet répressif. Si on veut être bon, il faut déjà élever la posture national de sécurité, et ça passe par une sensibilisation, à la fois des usagers, des entreprises, et aussi des élus, parce que ce sont des cibles extrêmement régulières des groupes criminels. Donc, participer à ce genre de salón, ça nous permet de nous rapprocher des élus et de diffuser un certain nombre de messages de prévention et de sensibilisation. L'unité nationale cyber que je commande, hein, c'est un… c'est un système intégré qui va de la prévention à la répression. C'est très important de le comprendre. Et donc, à la faveur ce Salon des Maires, qui est un salon important pour la gendarmerie, hein, on a investi plusieurs, plusieurs stands, avec… si, si, si… gendarmes qui

sont présents à temps complet sur les trois jours. Ben, les messages qu'on a diffusé aux maires, c'est les messages de prévention. C'est les messages aussi destiné également…, enfin, on a mené un certain nombre… enfin, on a rappelé quelles étaient nos capacités en matière d'accompagnement de ces élus, pour ben, justement, leur permettre de détecter leurs failles… leur vulnérabilité, pardon**,** ce qui passe par des diagnostics que nous faisons pour les collectivités locales, avec un dispositif qui s'appelle "Diagonal". Alors, c'est pas un audit à proprement parler, hein, mais c'est un dispositif qui permet, en fait, de faire un état de lieu, un panorama, ben, de l'état de l'art dans leur collectivité locale, et de détecter leur vulnérabilité, pour leur dire: ben, là, vous devriez accentuer vos efforts pour combler ce trou, ce manque, rappeler les actes essentiels, pour que vos personnel aient une hygiène numérique, comme on dit, beaucoup plus élevée. Et, encore une fois, afin d'être plus, plus fort face au risque d'ataque, qui sont… bah… qui sont extrêmement réguliers, et qui affectent ce genre de collectivité. Donc, c'est un peu le message que l'on a passé. Passé message de de protection, des audits, et puis, plus globalement on a mis en place, en Gendarmerie, depuis quelques temps, une application qui s'appelle "GEND'élus", hein, qui est une application numérique, qui permet à ses élus, dès qu'ils ont une question, et ben, d'aller sur l'application, dans laquelle… et poser les questions, et avoir les réponses surtout, instantanément. Donc, c'est un gros effort qu'a fait la gendarmerie, on en est assez fier. C'est un peu près le pendant de ce qui existe pour tout un chacun, qui s'appelle aussi "Ma sécurité", qui est une application qu'on peut télécharger en ligne, sur… voilà… pour qu'on les mette sur nos téléphonies, sur nos téléphones. Et donc, pour les élus, c'était ça, et ce salon du maire nous a permis de de diffuser ces messages.

Tradução: O que é preciso perceber, antes de mais, é que não se combate a cibercriminalidade apenas pelo vetor repressivo. Para sermos eficazes, é necessário elevar a postura nacional de segurança, e isso passa pela sensibilização dos utilizadores, das empresas e também dos eleitos, porque são alvos extremamente frequentes dos grupos criminosos. Participar neste tipo de salão permite-nos aproximar dos eleitos e difundir um conjunto de mensagens de prevenção e sensibilização. A unidade nacional *cyber* que comando é um sistema integrado que vai da prevenção à repressão. É muito importante entendê-lo. Assim, aproveitando o *Salon des Maires*, que é um salão importante para a *Gendarmerie*, investimos vários *stands*, com guardas presentes a tempo inteiro nos três dias. As mensagens que difundimos aos Presidentes de Câmara são mensagens de prevenção. São também mensagens destinadas a recordar as nossas capacidades de acompanhamento desses eleitos, para lhes permitir detetar as suas falhas — as suas vulnerabilidades, perdoem-me —, o que passa por diagnósticos que realizamos para as coletividades locais, com um aplicativo apelidado de “Diagonal”. Não é uma auditoria, em rigor, mas um aplicativo que permite aferir a situação, um panorama do estado da arte na sua coletividade local e detetar as suas vulnerabilidades, para lhes dizer: “aqui deveriam reforçar os esforços para colmatar esta lacuna”, recordar os atos fulcrais, para que o vosso pessoal tenha uma c*yber hygiene*, como se diz, muito mais elevada. Mais uma vez, para serem mais fortes face ao risco de ataque, que é extremamente frequente e afeta este tipo de coletividade. Foi esta, em suma, a mensagem que transmitimos: mensagem de proteção, diagnósticos e, mais globalmente, implementámos na *Gendarmerie*, há algum tempo, uma aplicação denominada

“GEND’élus”, uma aplicação digital que permite aos cidadãos, sempre que tenham uma questão, aceder à aplicação, colocar as perguntas e, sobretudo, obter respostas de forma instantânea. É um grande esforço feito pela *Gendarmerie*, do qual nos orgulhamos. É, grosso modo, o equivalente do que existe para qualquer cidadão, chamada “Ma Sécurité”, uma aplicação que se pode descarregar *online* para instalar nos nossos telemóveis. E, portanto, para os cidadãos, foi isso, e este salão permitiu-nos difundir estas mensagens.

05:46 – Entrevistador (Ali Jiar): Alors, un salon où on a remarqué la présence du ministre de l'Intérieur, d'ailleurs, qui est passé vous, vous rencontrez, et de nombreux ministres, de nombreuses personnalités politique. Est-ce que, justement, les, les maires vous sollicitent beaucoup, mon coronel?

Tradução: Ora, um salão em que se notou a presença do Ministro do Interior — que, aliás, passou por aí para vos encontrar, tal como muitos ministros e personalidades políticas. Os Presidentes de Câmara solicitam-vos muito, meu Coronel?

05:58 – Entrevistado (Coronel Pétry): Alors, bien sûr, les maires nous sollicitent beaucoup, d'autant que nous, nous sommes sur la quasi totalité du territoire, dans la profondeur du territoire, métropolitain comme ultramarin. Donc, on est au contact en H24 avec les élus. Donc, et bien souvent, on est le seul service public aussi, dans, dans ces territoires, voilà. Donc, il y a un lien de proximité avec les maires, evidente. Efectivement, ils viennent souvent nous voir. Alors, vous l'avez noté, effectivement, le ministre de l'Intérieur, le ministre délégué à la sécurité quotidienne, monsieur Daragon, monsieur Nasrou Othman également, enfin, tous les, tous les ministres, euh, rattachés au ministère de l'Intérieur, effectivement, sont, sont venus nousvoir pour, ben, pour, pour mieux connaître ce qu'on, ce qu'on faisait, mais aussi avoir un échange avec nous, et pour qu'on puisse aussi leur dire sur quoi on, on agissait prioritairement. Donc, voilà un peu les messages qu'on passait, que, que nous passons aux élus, et que nous demandent les maires. C'est souvant des, des, des messages de, de bon sens, hein, et donc, et il nous font part aussi des difficultés qu'il rencontrent, et, au besoins, on apporte une réponse, ou on fait en sorte d'envoyer du personnel, ben, pour remédier aux difficultés rencontrées.

Tradução: Claro que os Presidentes de Câmara nos solicitam bastante, tanto mais que estamos praticamente em todo o território, no interior do território, metropolitano e ultramarino. Estamos em contacto 24 horas por dia com os cidadãos. E, muitas vezes, também somos o único serviço público nesses territórios. Portanto, existe um vínculo de proximidade evidente com os Presidentes de Câmara; de facto, vêm muitas vezes ter connosco. Como referiu, o Ministro do Interior, o Ministro Delegado para a segurança quotidiana, o senhor Daragon, o senhor Nasrou Othman igualmente — enfim, todos os ministros ligados ao Ministério do Interior — vieram ver-nos para conhecer melhor o que fazemos, mas também para trocar connosco, para que lhes pudéssemos dizer quais são as nossas prioridades de ação. Eis, portanto, as mensagens que transmitimos aos cidadãos e aos Presidentes de Câmara que nos solicitam. São, muitas vezes, mensagens de bom senso, e dão-nos também conta das dificuldades que encontram e, se necessário, damos uma resposta ou fazemos por enviar pessoal para suprir as dificuldades encontradas.

07:03 – Entrevistador (Ali Jiar): Les aider et les conseiller... Mon colonel, vous, vous parlez justement de collaboration, d'écosystème de la cybersécurité. Comment, aujourd'hui, l'unité collabore-t-elle avec des entités nationales, peut-être européennes et internationales, sur les investigations?

Tradução: Ajudá-los e aconselhá-los… Meu Coronel, fala precisamente de colaboração, do ecossistema de cibersegurança. Como é que, hoje, a unidade colabora com entidades nacionais, eventualmente europeias e internacionais, nas investigações?

07:15 – Entrevistado (Coronel Pétry): Alors, comme je disais tout à l'heure, encore une fois, en fait, au sein du ministère de l'Intérieur, la gendarmerie n'est pas seule, même si elle occupe une part importante. Mais, je n'oublie pas les partenaire policiers, de la police nationale et de la préfecture de police de Paris. Donc on travaille tous ensemble, au, au, au même fin. Tout ça, sous la coupe des magistrats, et notamment la juridiction nationale de lutte contre la criminalité organisée, la "JUNALCO" et son parquet, la section J3 spécialisée dans la cybercriminalité, qui, en fait, coordonne l'ensemble des forces dédié à la lutte contre la cybercriminalité. Donc, des forces du ministère de l'intérieur, chapauté par des magistrats, qui coordonnent l'ensemble. Ça d'une part. Deuxème, deuxièmement, en matière de cybercriminalité, on ne peut pas travailler sans avoir des liens avec des partenaires étranger, puisque la cybercriminalité, c'est, c'est un domaine où l'international joue. Il y a pas de frontière en cybercriminalité. Donc, on est obligé de travailler avec des partenaires étrangers, et nos alliés traditionnels, je dirais, qu'ils soient européens, ou américains, ou anglosaxon de manière générale. Et donc, on a des rapports extrêmement serrés, avec, avec ces dras. Donc, ça, c'est sur l'aspect purement enquête. Après, vous avez un volet, le volet plus technique, avec l'Agence Nationale de Sécurité des Systèmes d'Information, l' ANSI, qui est le, le, le, le pilote en matière de cybersécurité. La cybersécurité, c'est quoi? Ben, c'est l'ensemble des mesures qui permettent de protéger les systèmes d'information des usagers, des administrations, mais aussi des entreprises. Et ça, c'est chapaoté par l'ANSI, et notamment pour les entreprises d'importance vitale. Voilà. Donc, l'ANSI c'est un partenaire clé. C'est, c'est, c'est le partenaire national par excellence. Et puis, sous la coupe de l'ANSI, il y a d'autres types de partenaires comme "cybermalveillance" qui est un groupement d'intérêt public… extrêmement… d'intérêt public, pardon, qui est extrêmement précieux. J'invite tout le monde à aller sur, sur cybermalveillance.gouv.fr, qui diffuse tout un tas de, de préconisations, de, de, de renseignements sur, ben, les risques en courouru, mais aussi lorsqu'on a été victime, que faire face à une attaque. Donc voilà. Nous, on, on travaille avec toute une myriade de partenaires, sans oublier — important — les partenaires économiques, les opérateurs, les opérateurs de, de téléphonie, d'Internet. Et, à travers mon unité, j'ai toute un une section dédiée à ce relationnel, parce qu'on ne fait pas d'enquête sans recourir à ces opérateurs. Et donc, pour recourir à ces opérateurs, il faut les connaître, il faut du contact, il faut savoir ce qu'on peut leur demander, à qui, et comment. Quand je fais une réquisition judiciaire, il faut que je puisse l'envoyer à quelqu'un. Donc, voilà un peu la galaxie avec laquelle, dans laquelle nous évoluons.

Tradução: Como dizia há pouco, no seio do Ministério do Interior a *Gendarmerie* não está sozinha, ainda que tenha um papel importante. Não esqueço os parceiros policiais, da Polícia Nacional e da Prefeitura de Polícia de Paris: trabalhamos todos juntos, com o mesmo fim. Tudo isto sob a alçada dos magistrados e, nomeadamente, da jurisdição nacional de luta contra a criminalidade organizada, a "JUNALCO", e do seu Ministério Público, através da Secção J3, especializada em cibercriminalidade, que coordena o conjunto das forças dedicadas ao combate à cibercriminalidade. Ou seja, forças do Ministério do Interior, sob a tutela de magistrados que coordenam o todo. Em segundo lugar, em matéria de cibercriminalidade, não se pode trabalhar sem ligações com parceiros estrangeiros, pois é um domínio onde o internacional pesa: não há fronteiras em cibercriminalidade. Somos, portanto, obrigados a trabalhar com parceiros estrangeiros — os nossos aliados tradicionais, quer europeus, quer americanos, quer anglo-saxónicos de modo geral — e mantemos relações estreitas com esses atores. Isso no aspeto puramente de investigação. Depois, há um outro plano, mais técnico, com a Agência Nacional de Segurança dos Sistemas de Informação, a "ANSI", que é a entidade piloto em matéria de cibersegurança. E o que é a cibersegurança? É o conjunto de medidas que permitem proteger os sistemas de informação dos utilizadores, das administrações e também das empresas. E isso é tutelado pela ANSI, nomeadamente no que toca às empresas de importância vital. Portanto, a ANSI é um parceiro-chave, é o parceiro nacional por excelência. E, sob a sua égide, há outros tipos de parceiros, como o "cybermalveillance", que é um agrupamento de interesse público que é extremamente precioso. Convido toda a gente a visitar cybermalveillance.gouv.fr, onde se difunde um vasto conjunto de recomendações e informações sobre os riscos incorridos e, também, o que fazer quando se é vítima de um ataque. Nós trabalhamos com uma miríade de parceiros, sem esquecer — importante — os parceiros económicos: os operadores de telecomunicações e de Internet. Na minha unidade, tenho uma secção inteiramente dedicada a esta relação, porque não se faz investigação sem recorrer a esses operadores. Para recorrer a eles, é preciso conhecê-los, ter contacto, saber o que lhes podemos pedir, a quem e como. Quando faço uma requisição judicial, preciso de a poder enviar a alguém. Eis, portanto, a galáxia com a qual e na qual evoluímos.

09:48 – Entrevistador (Ali Jiar): Une galaxie très riche et très diverse, et, et qui avance dans le même sens. Mon colonel, quelle est l'importance de la formation? Vous parliez, tout à l'heure effectivement de prévention, de messages justement pour les, pour les citoyens. Quelle est la place de l'information, de la sensib... de la sensibilisation, pardon, au sein de votre unité?

Tradução: Uma galáxia muito rica e muito diversa, e que avança no mesmo sentido. Meu Coronel, qual é a importância da formação? Falou, há pouco, de prevenção, de mensagens dirigidas aos cidadãos. Qual é o lugar da informação e da sensibilização, perdoe-me, no seio da sua unidade?

10:03 – Entrevistado (Coronel Pétry): Bien sûr, c'est une question clé, hein, la formation, parce que la lutte contre la cybercriminalité, c'est quand même un domaine technique. Mais technique d'un point de vue vraiment presque scientifique, d'une certaine manière, mais aussi

technique judiciaire. Donc, il faut à la fois des techniciens et des officiers de police judiciaire. Donc, c'est c'est une alchimie qui est pas, au final, très complexe, si on se donne les moyens d'une formation extrêmement rigoureuse. À l'heure où je vous parle, avant de rentrer dans une unité telle que la mienne, il faut un certain nombre d'années. C'est… il faut rentrer en école de gendarmerie, il faut devenir ensuite sous-officier de carrière, ensuite passer tout un tas de diplôme avant de d'espérer arriver chez nous. On est en train de transformer les choses, de manière à pouvoir faciliter l'accès dans la filière, dès quasiment l'entrée en école de sous-officiers.

Tradução: Claro, a formação é uma questão-chave, porque o combate à cibercriminalidade é, ainda assim, um domínio técnico, mas técnico do ponto de vista científico, de certo modo, mas também técnico do ponto de vista judicial. Fazem falta, tanto técnicos como agentes de polícia judiciária. É uma alquimia que não é, no fim de contas, muito complexa, se nos dotarmos dos meios para uma formação extremamente rigorosa. No momento em que vos falo, antes de entrar numa unidade como a minha, são necessários vários anos: é preciso entrar na Escola da *Gendarmerie*, tornar-se depois subalterno na carreira e, a seguir, obter toda uma série de diplomas antes de poder aspirar a chegar até nós. Estamos a transformar as coisas, de modo a facilitar o acesso à fileira praticamente desde a entrada na Escola da *Gendarmerie*.

10:43 – Entrevistador (Ali Jiar): Aux spécialistes, aux gens qui ont une expertise?

Tradução: Para especialistas, para pessoas com perícia/conhecimento?

10:46 – Entrevistado (Coronel Pétry): Et qu'ils aient une expertise ou pas, tous ceux qui veulent s'orienterdans la filière cyber le pourront quasiment dès l'entrée. Donc, ça, c'est une révolution qui va nous permettre de multiplier par deux, assez rapidement, nos cyber enquêteurs de, de, de haut niveau. Et donc, tout ça avec une formation adaptée, renforcée, avec une pluralité aussi de parcours. Enfin, donc la formation est un domaine clé. On se donne les moyens, il y a un gros effort fait par la gendarmerie en ce moment, justement pour se donner les moyens de la réussite.

Tradução: Tenham eles perícia/conhecimento ou não, todos os que quiserem orientar-se para a fileira *cyber* poderão fazê-lo quase desde a sua entrada. Isto é uma revolução que nos permitirá duplicar, com bastante rapidez, os nossos ciberinvestigadores de alto nível, e tudo com uma formação adequada, reforçada, e também com uma pluralidade de percursos. Portanto, a formação é um domínio essencial. Estamos a dotar-nos dos meios; há um grande esforço feito pela *Gendarmerie* neste momento para garantir o sucesso.

11:13 – Entrevistador (Ali Jiar): Alors, vous pouvez peut-être, mon colonel, nous partager quelques succès. Parler d'investigation, d'enquete, de collaboration internationale et européenne. Est-ce que vous avez quelques succès à nous partager, au niveau national ou international?

Tradução: Ora, talvez possa, meu Coronel, partilhar connosco alguns sucessos. Falou de investigação, de inquéritos, de colaboração internacional e europeia. Tem alguns êxitos para partilhar, a nível nacional ou internacional?

11:24 – Entrevistado (Coronel Pétry): Bien sûr, on a, on a des succès.

Alors, mais la première chose à dit en la manière, il faut rester extrêmement humble et modeste, parce que les, les revers de fortune sont aussi rapides parfois que les, les succès qu'on peut avoir. Mais c'est vrai que, depuis, depuis quelques temps, la gendarmerie enchaîne un certain nombre de, de réussite. Ben, il y a eu des, des affaires emblématiques, comme celle d'EncroChat, qui était une solution de téléphonie chiffrée, qui était utilisée par la crimin... la criminalité mondiale, avec une flotte de 60000 téléphones qu'on a réussi à, à, à démanteler. Ben, cette EncroChat, c'est une opération clé, mais qui date déjà de, de, de 2021, à peu près. Récemment, on peut citer quoi? Des dossiers de, de démantèlement de trafic d'armes 3D sur internet, des interpellations parmi les, les, les… comment dire… les, les, ah, je… les rançongiciel, les, les groupes criminels qui se livrent à de la… du… de l'extorsion par rançongiciel, notamment le groupe *LockBit*, hein, qui est le groupe… le… qui était le plus, le plus actif, hein, contre lequel on, on continue d'ailleurs à mener une action, mais petit à petit. On interpelle les individus, à l'étranger le plus souvent, et on commence à démanteler, euh, le groupe, hein, petit à petit. Euh... des succès aussi contre des plateformes, euh, des plateformes qui, qui permettent la commission d'un certain nombre d'infractions. On pense à, à la plateforme "Coco", hein, qu'on a, qu'on a fait fermer, et sur laquelle continue à avoir une enquete, du reste. Donc, importante, ce genre de, de, de plateforme, parce que ça sert… ce sont des infrastructures de criminalité. Donc, on s'est aussi attaqué, en lien avec la juridiction J3, à la plateforme de messagerie Telegram, hein, qui ne répondaient pas à nos réquisitions, qui manifestement avait de grosses lacunes en matière de modération de ses contenus. Voilà. Donc, voilà tout un tas de succès. Et puis, en lutte contre la pédocriminalité, on pourra en rajouter plusieurs. En matière de lutte contre le trafic de stup sur Internet, trafic d'armes — je l'ai dit — trafic d'identité sur Internet. Donc, voilà, on a plusieurs succès en ce moment-là.

Tradução: Claro, temos sucessos. Mas a primeira coisa a dizer nesta matéria é que é preciso manter-se extremamente humilde e modesto, porque os reveses podem ser, por vezes, tão rápidos quanto os sucessos que se alcançam. Mas é verdade que, há algum tempo, a *Gendarmerie* tem encadeado vários êxitos. Houve casos emblemáticos, como o do *EncroChat*, que era um recurso de telecomunicação cifrada usada pela criminalidade mundial, com uma rede de 60 000 telefones que conseguimos desmantelar. O *EncroChat* é uma operação-chave, mas que já datava, aproximadamente, de 2021. Mais recentemente, podemos citar processos de desmantelamento de tráfico de armas 3D na Internet; detenções entre os… como dizer… os grupos de *ransomware* que se dedicam à extorsão por *ransomware*, nomeadamente o grupo *LockBit*, que era o mais ativo, contra o qual continuamos, aliás, a conduzir uma ação, mas paulatinamente. Vamos detendo indivíduos, muitas vezes no estrangeiro, e começamos a desmantelar o grupo, pouco a pouco. Também tivemos êxitos contra plataformas que permitem a prática de um certo número de infrações. Recordo a plataforma “Coco”, que fizemos encerrar e sobre a qual continua a decorrer uma

investigação. Este tipo de plataforma é importante, porque serve… são infraestruturas da criminalidade. E, em ligação com a jurisdição J3, atacámos também a plataforma de mensagens *Telegram*, que não respondia às nossas requisições e que manifestamente tinha grandes lacunas na moderação dos seus conteúdos. Portanto, há uma série de sucessos. E, no combate à pedocriminalidade, poderíamos acrescentar vários. No combate ao tráfico de estupefacientes na Internet, ao tráfico de armas — como disse —, ao tráfico de identidades na Internet. Temos, pois, vários êxitos neste momento.

13:26 – Entrevistador (Ali Jiar): Des réussites qui, qui confirment effectivement l'efficacité de de votre unité, dans cet écosystème. Puisque vous disiez, mon colonel, vous travaillez en bonne intelligence avec toutes les unités de police, de manière nationale et internationale. Mon, mon colonel, quels sont les principaux défis auxquels vous êtes confronté pour ces prochaines années?

Tradução: Êxitos que confirmam, efetivamente, a eficácia da sua unidade neste ecossistema, já que, como disse, trabalha em boa articulação com todas as unidades policiais, a nível nacional e internacional. Meu coronel, quais são os principais desafios com que se confrontará nos próximos anos?

13:40 – Entrevistado (Coronel Pétry): Alors, pour les prochaines années, les défis sont de trois ordres. On va dire, il y a un défi de la formation, encore une fois. Il y a un défi technologique, parce que les c'est un domaine en sans cesse en évolution. Donc il faut toujours être à la page. Donc, technologiquement, il faut, il faut suivre et former les personnels en conséquence. Et puis, plus globalement, on est face à une problématique de, de données massives, hein. On croule sous la donnée, hein. Nous, notre boulot, justement, c'est de capter cette donnée, l'extraire, ensuite la traiter. Donc, comment on traite convenablement des téra, et des téra, et des téra de données? Ça, c'est un véritable enjeu, pour lequel on investit beaucoup, en science de la donnée, de manière à être en capacité de fournir, via des outils de traitement de cette données, eh bien, une lecture à nos enquêteurs ou à nos analystes, suffisamment limpide pour qu'ils puissent mener leurs enquetes. Et ça, c'est un défi majeur, en plus de l'intelligence artificielle, du cloud et du poste quantique, qui vont arriver.

Tradução: Para os próximos anos, os desafios são de três ordens: há um desafio da formação, uma vez mais; há um desafio tecnológico, porque é um domínio em constante evolução, pelo que é preciso estar sempre atualizado — tecnologicamente, é preciso acompanhar e formar o pessoal convenientemente; e, mais globalmente, enfrentamos uma problemática de dados massivos: estamos soterrados em dados. O nosso trabalho é captar esses dados, extraí-los e, depois, tratá-los. Como tratar devidamente terabytes e terabytes de dados? Esse é um verdadeiro desafio, para o qual investimos muito em ciência de dados, de modo a estarmos em condições de fornecer, através de ferramentas de tratamento desses dados, uma leitura suficientemente clara aos nossos investigadores e analistas, para que possam conduzir os seus inquéritos. E isso é um desafio maior, a par da inteligência artificial, da *cloud* e do pós-quântico que aí vêm.

14:33 – Entrevistador (Ali Jiar): Ce sera le mot de la fin. Mieux traiter la donnée pour être plus efficace vis-à-vis de ces nouvelles innovations. Merci, mon colonel, pour ce témoignage, et je vous dis peut-être à très bientôt pour une nouvelle émission. À très bientôt.

Tradução: Fica a palavra final: tratar melhor os dados para ser mais eficaz face a estas novas inovações. Obrigado, meu Coronel, por este testemunho, e dir-lhe-ei talvez até muito em breve, para uma nova emissão. Até muito em breve.

Apêndice C

Principais estruturas e mecanismos da UE, dos Estados-Membros e do setor privado em resposta à cibercriminalidade

Tabela C1

Síntese das missões, mecanismos operacionais e base legal de atuação dos principais atores no âmbito da cibercriminalidade e cibersegurança

Estrutura Institucional	Missão	Mecanismos Operacionais (com hiperligações)	Base Legal (com hiperligações)
EC3 (EUROPOL)	Reforçar a resposta policial ao cibercrime; apoiar investigações complexas; produzir inteligência estratégica	*Secure Information Exchange Network Application* (SIENA); Planos de Ação Operacional (OAPs) - EMPACT 2022-2025; *Joint Cybercrime Action Taskforce* (J-CAT); *Secure Platform for Accredited Cybercrime Experts* (SPACE)	Decisão 2009/371/JAI; Diretiva 2013/40/UE; Regulamento (UE) 2016/794; Regulamento (UE) 2022/991; Diretiva (UE) 2023/977
ENISA	Reforçar a resiliência da EU; certificação e políticas de cibersegurança	Rede CSIRT; certificação; *guidelines*.	Regulamento (UE) 2019/881;
CERT-EU	Ponto de coordenação de intercâmbio de informações sobre cibersegurança e resposta a incidentes	Cooperação com ENISA, CSIRT e EC3;	NIS2 - Diretiva (UE) 2022/2555; Memorando de entendimento em 15 de fevereiro de 2021.
EUROJUST	Coordenação judicial em investigações transnacionais	SIRIUS; *Joint Investigation Teams* (JIT); Prova eletrónica; Cooperação com o EC3;	Regulamento (UE) 2018/1727; Regulamento (UE) 2023/1543; Diretiva (UE) 2023/1544.
CSIRT nacionais	Monitorizar e responder a incidentes no plano nacional	Rede CSIRT; cooperação transnacional.	NIS2 - Diretiva (UE) 2022/2555; Lei n.º 46/2018, de 13 de agosto; DL n.º 65/2021, de 30 de julho
Unidades policiais especializadas de cibercriminalidade	Investigação criminal, forense digital, informações criminais e cooperação	JIT; SIENA; SIRIUS. Possibilidade de uso de comunicações seguras, através do I-24/7 da INTERPOL.	Diretiva 2013/40/UE; Convenção de Budapeste com protocolo adicional 1 e 2; Decisão (UE) 2023/436.
Unidades de ciberpoliciamento	Policiamento proativo no	Aprofundado na Tabela 4 e 6.	Estratégias institucionais e nacionais;

	ciberespaço tendencialmente integral (prevenção, repressão, investigação criminal e informações policiais)		Estratégia da UE para a União da Segurança (COM/2020/605 final); Estratégia Europeia de Segurança Interna (COM/2025/148)
Parcerias público-privadas / *Information Sharing & Analysis Centres* (ISACs)	Partilha de informação setorial sobre ameaças.	ISCAC (*e.g.* energia, saúde, finanças); cooperação voluntária.	Estratégia de cibersegurança da UE para a década digital; NIS2 - Diretiva (UE) 2022/2555;
Operadores privados	Fornecimento de dados e colaboração em investigações; proteção de infraestruturas críticas	Resposta a pedido de dados; colaboração na preservação da prova digital; mecanismos do *Digital Services Act* (DSA): sinalização de conteúdos ilegais online (art.º 16); *Trusted Flaggers* (art.º 22) – sinalizadores de confiança; *E-evidence Package*.	Diretiva (UE) 2023/1544. Regulamento (UE) 2023/1543; Regulamento (UE) 2022/2065.

Fonte: Elaborado pelo próprio (2025).

Apêndice D

Métricas de desempenho para o ciberpoliciamento

Tabela D1

Métricas para prevenir o cibercrime e comportamentos ciberdesviantes no ciberpoliciamento com enfoque na identificação precoce, educação, monitorização digital e moderação, adaptado de CMAGE (2022) e Comissão Europeia (2018)

Prevenir	
Métrica	**Descrição**
Novos indivíduos identificados	Número de pessoas identificadas em risco ou que possam representar um risco acrescido para potenciais vítimas.
Métodos inovadores	Identificação numérica de novos métodos ou modus operandi desenvolvidos pelos agentes de ameaça racionais.
Planos de moderação	Número de estratégias desenvolvidas ou reformuladas para prevenir ou mitigar processos de radicalização, manifestações extremistas ou dinâmicas associados ao discurso de ódio.
Intervenções online realizadas	Número de ações concretas para prevenir ameaças.
Campanhas de prevenção	Número de participações em iniciativas públicas associadas ao cibercrime e à prevenção da radicalização.
Casos de proteção	Número de casos que envolvem a recomendação de medidas de autoproteção e medidas complementares de proteção junto das vítimas, iniciados pelas autoridades policiais e passíveis de envolver parceiros (entidades públicas e/ou privadas).
Encaminhamento externo	Número de casos encaminhados, após sinalização, de indivíduos com comportamentos ciberdesviantes ou possíveis de cometimento de facto ilícito ou de facto que constitua um cibercrime.

Fonte: Elaborado pelo próprio (2025).

Tabela D2

Métricas de proteção e preparação com enfoque na redução de vulnerabilidades e reforço da resiliência de infraestruturas, instituições e comunidades, adaptado de CMAGE (2022) e Comissão Europeia (2018)

Proteger e Preparar	
Métrica	**Descrição**
Projetos e campanhas desenvolvidos	Número de iniciativas estratégicas criadas com foco na proteção preventiva ou preparação institucional.
Campanhas de proteção/preparação implementadas	Número de ações concretas realizadas no terreno ou remotamente para aumentar a resiliência digital de públicos-alvo (*e.g.* jovens, idosos e PME).
Interações com indústria e parceiros externos	Número de colaborações formais ou informais com entidades privadas, académicas ou internacionais.
Exercícios de sensibilização	Número de simulações, workshops ou ações práticas destinadas a aumentar a consciência pública sobre ameaças digitais. (*e.g. EMPACT Action Week* – ver Vídeo A8)
Eventos e apresentações públicas realizadas	Número de sessões informativas, conferências ou seminários com foco em cibersegurança e na prevenção de comportamentos.

Sessões de formação para forças de segurança	Número de formação/treinos especializados ministrados a polícias sobre o cibercrime, sua prevenção (monitorização, deteção, sinalização e interação comunitária), respostas a incidentes e investigação criminal em ambiente digital.
Plano de Formação	Número de ações sobre o cibercrime ministradas em estabelecimento de ensino universitário policial e no ensino politécnico policial no âmbito da ESPOL.
Sessões de formação para a indústria	Número de sessões para capacitação técnica e estratégica dirigida a empresas, operadores críticos ou setores vulneráveis.
Análises operacionais de ameaças emergentes	Número de debriefings para reforço de identificação e antecipação de novas tipologias de ameaça.
Protocolos	Número de protocolos estabelecidos no âmbito de parcerias público-privadas.

Fonte: Elaborado pelo próprio (2025).

Tabela D3

Métricas que envolvem a investigação, repressão e responsabilização de indivíduos, grupos ou organizações, adaptado de CMAGE (2022) e Comissão Europeia (2018)

Perseguir	
Métrica	**Descrição**
Pedidos - Rede 24/7	Número de diligências solicitadas, requeridas e materializadas com êxito no âmbito da Rede 24/7 (art.º 35 da Resolução da Assembleia da República n.º 88/2009)
Casos atribuídos	Número total de casos oficialmente alocados para investigação.
Investigações ativas	Número de casos em curso com diligências de investigação.
Mandados judiciais e buscas realizadas	Número de mandados emitidos e de operações de busca executadas no âmbito de investigações ao cibercrime.
Detenções efetuadas	Número de indivíduos detidos em conexão direta com os casos investigados.
Resultados na justiça criminal	Número de decisões judiciais obtidas, incluindo condenações, absolvições ou arquivamentos, bem como medidas judiciárias complementares (suspensão provisória do processo; medidas de coação; apreensão de bens; perda a favor do Estado; e obrigação de frequentar programas de reabilitação).
Encerramento ou interrupção temporária de domínios	Número de plataformas digitais, websites ou infraestruturas tecnológicas ilegais desativadas.
Relatórios de avaliação de ameaça	Número de documentos analíticos que identificam, categorizam e avaliam potenciais ameaças cibernéticas.
Operações internacionais lideradas ou apoiadas	Número de intervenções nacionais e transnacionais com participação ativa ou apoio logístico das autoridades (judiciárias e policiais) associadas à coordenação e cooperação internacional.

Fonte: Elaborado pelo próprio (2025).

Anexo

Vídeos e recursos ilustrativos sobre práticas internacionais de ciberpoliciamento

Vídeo A1

A unidade cyber da Gendarmerie Nationale em França, com modelo integral de ciberpoliciamento

Fonte: Gendarmerie nationale (2024, junho 9). Disponível em https://www.youtube.com/watchI.

Vídeo A2

Entrevista ao Comandante da Gendarmerie, Coronel Hervé Pétry, responsável pela "UN Cyber"

Fonte: Francophone Business TV (2024, dezembro 18). Disponível em https://www.youtube.com/wat.

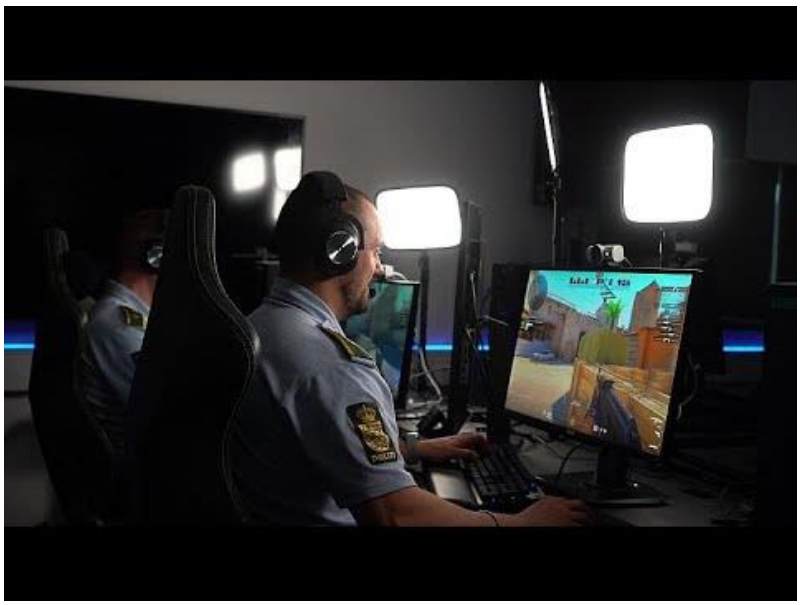
Vídeo A3

Web Constables da polícia comunitária na Estónia

Fonte: EU Knowledge Hub (2023, outubro 17). Disponível em https://www.youtube.com/wat.

Vídeo A4

Equipa de patrulhamento online da polícia dinamarquesa prevenindo e reprimindo através de jogos online e interagindo com jovens nas redes sociais



Fonte: Euronews Next (2025, julho 03). Disponível em https://www.youtube.com/watch?v.

Vídeo A5

Ciberpoliciamento da polícia dinamarquesa

Fonte: NET25 New and Information (2023, junho 30). Disponível em https://www.youtube.com/watch?.

Vídeo A6

Ciberpoliciamento da polícia norueguesa

Fonte: Kripos (2023, outubro 9). Disponível em https://www.youtube.com/watch?v=75tNpSHfLeI.

Vídeo A7

Plataforma de prevenção e sensibilização com possibilidade de assistência a vítimas através de um serviço de linha gratuita, incluindo a intervenção de um profissional especializado ou, se necessário, de um polícia por chat

Fonte: Cybermalveillance-gouv-fr (2025, abril 11). Disponível em https://www.youtube.com/watch?v=.

Vídeo A8

EMPACT Action Week — Semana operacional coordenada ao nível do ciberpoliciamento com a presença de sete países, incluindo Islândia, Dinamarca, Suécia e Países Baixos

Fonte: Kripos (2023, novembro 23). Disponível em https://www.youtube.com/watch?v=YMo-lsHz.