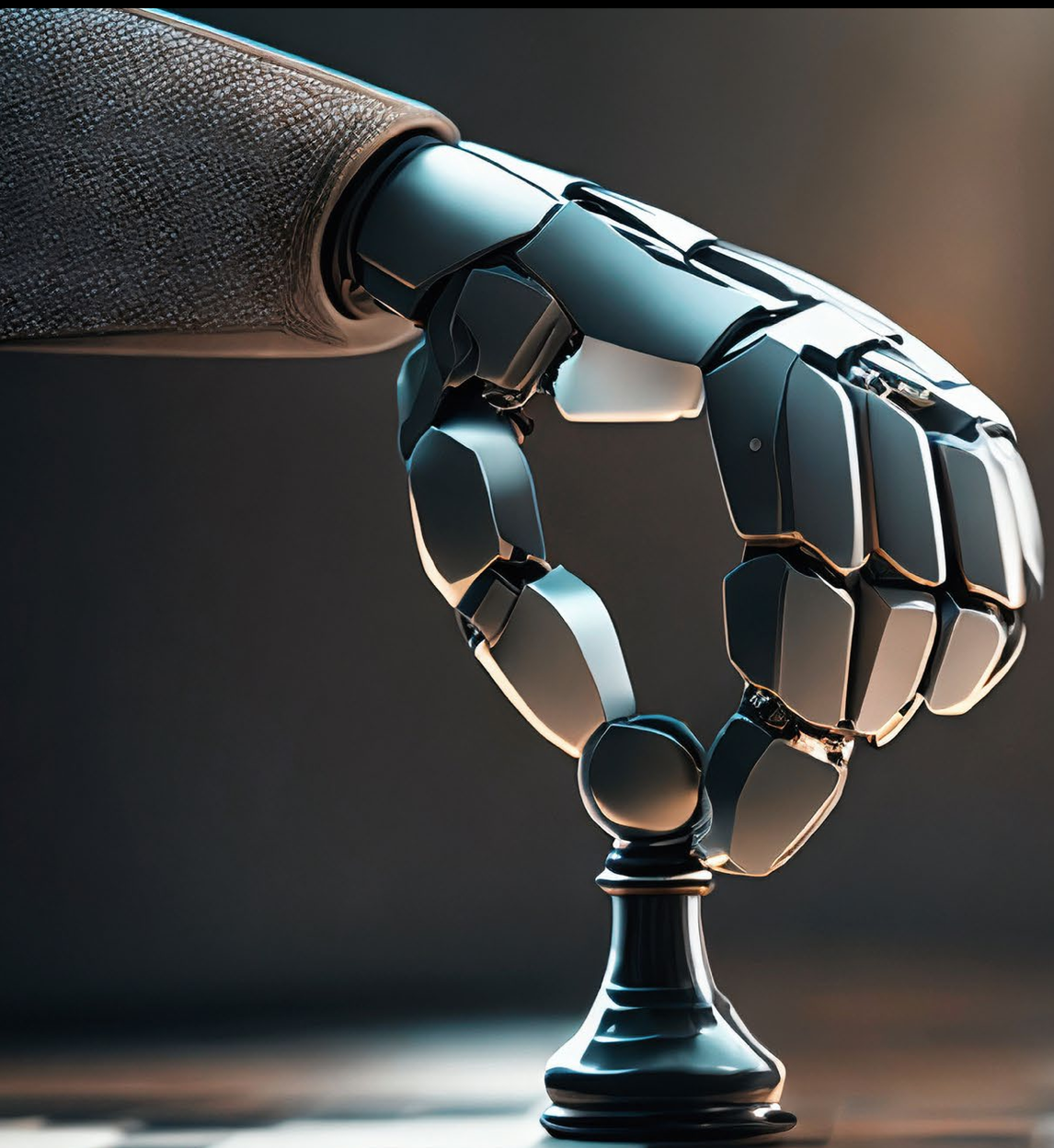
IT Insight SECURITY

#16 FEVEREIRO 2024



IA O IMPACTO NA CIBERSEGURANÇA

COMO A INTELIGÊNCIA ARTIFICIAL IMPACTA A CIBERSEGURANÇA

POR RUI DAMIÃO

A INTELIGÊNCIA ARTIFICIAL VEIO PARA FICAR E AS IMPLICAÇÕES PARA A CIBERSEGURANÇA SÃO MAIS DO QUE MUITAS. SE, POR UM LADO, QUEM ATACA VAI INOVAR AS SUAS TÁTICAS, POR OUTRO, VAI AJUDAR QUEM DEFENDE A SER MAIS EFICAZ.

Em 2023 presenciámos o advento da Inteligência Artificial (IA). Mesmo que a tecnologia não tenha sido criada no último ano, foi durante o ano passado que as organizações começaram a olhar 'com olhos de ver' para como é que a tecnologia pode ajudar nas suas operações e na sua transformação digital.

Se é verdade que a IA vai impactar todas as indústrias, todos os verticais e todas as tecnologias de alguma maneira, é verdade, também, que irá impactar a cibersegurança. Quem ataca e quem defende olha para a tecnologia e procura perceber como pode tirar o máximo partido desta para atingir os seus objetivos.

Paulo Pinto, Business Development Manager da Fortinet Portugal, refere que "os agentes de ameaças têm cada vez mais soluções para orquestrar os ciberataques", principalmente com IA. As perspetivas para 2024 "sugerem que, ao confiarem nas crescentes funcionalidades das suas ferramentas, os adversários irão aumentar a sofisticação das suas atividades, tornando cada tática do ciclo de ataque mais eficiente". Apesar desta previsão, "a verdade é que, no caso do phishing, por exemplo, a IA já tem vindo a ser utilizada pelos ciberatacantes para automatizar a criação destes emails. Através desta, não só conseguem amplificar o volume de ataques de phishing, como conseguem corrigir alguns indicadores que, anteriormente, associávamos facilmente como sendo um ataque, como é o caso da gramática, ortografia e formatação".

Rui Barata Ribeiro, Security Sales Leader da IBM Portugal, diz que a utilização de IA generativa e de *Large Language Models* (LLM) será "mais prevalente em ciberataques como phishing, SMS e outras operações de engenharia social", onde "os atacantes poderão, de forma cada vez mais fácil e direcionada, criar notícias falsas, através de fotos e vídeos *deepfake*". Na sua opinião, a IA vai permitir "uma maior escala no cibercrime", que "os ataques sejam mais individualizados" e uma "adaptação mais rápida face às estratégias de defesa".

Luís Rato, NSO da Microsoft Portugal, indica que, do lado de quem ataca, a IA "permite a identificação, de uma forma mais rápida e detalhada, de possíveis vulnerabilidades em sistemas de segurança e tem a capacidade de explorá-las para obter acesso não autorizado a sistemas e dados. A mesma tem sido um recurso para estes agentes na criação de conteúdos fictícios próximos da realidade e controlo da mensagem que se quer transmitir".

Já Ben Gelman, Senior Data Scientist da Sophos, defende que "as atitudes dos ciberatacantes" na utilização de IA "estão divididas, com sentimentos que vão da esperança à hostilidade total". Gelman explica que "os atacantes pioneiros nesta adoção estão a partilhar ferramentas, mesmo que os resultados não sejam particularmente impressionantes. Outros decidiram que os LLM ainda não estão suficientemente maduros para ajudar nos ataques".

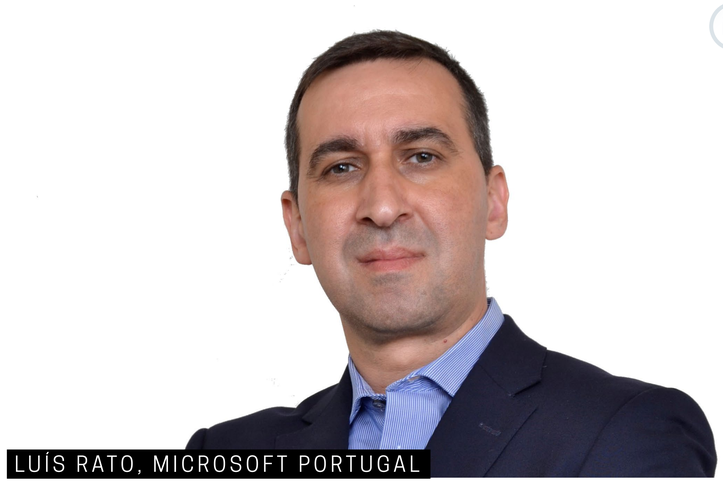
Por seu lado, Bruno Castro, Fundador e CEO da VisionWare e especialista em cibersegurança e análise forense, não tem dúvidas que esta será "uma das grandes tendências dos próximos anos" e que

BEN GELMAN, SOPHOS

merece "particular vigilância", até pelo "potencial disruptivo" da IA ao lado dos cibercriminosos. "Os algoritmos de machine learning potenciam ataques direcionados com maior precisão (como spear phishing) e também malware mais sofisticado e disruptivo. Também em termos de fraude, a integração da IA é uma preocupação, já que observamos cada vez mais um aprimoramento em técnicas de falsificação de identidade e deteção de padrões de comportamento financeiro", explica.

"OS ATACANTES PODERÃO, DE FORMA CADA VEZ MAIS FÁCIL E DIRECIONADA, CRIAR NOTÍCIAS FALSAS, ATRAVÉS DE FOTOS E VÍDEOS DEEPFAKE". NA SUA OPINIÃO, A IA VAI PERMITIR "UMA MAIOR ESCALA NO CIBERCRIME", QUE "OS ATAQUES SEJAM MAIS INDIVIDUALIZADOS" E UMA "ADAPTAÇÃO MAIS RÁPIDA FACE ÀS ESTRATÉGIAS DE DEFESA".

BEN GELMAN, SENIOR DATA SCIENTIST DA SOPHOS



LUÍS RATO, MICROSOFT PORTUGAL

INTELIGÊNCIA ARTIFICIAL NA DEFESA

Rui Barata Ribeiro explica que, no lado de quem defende, há, "essencialmente, seis dimensões em que a IA pode ser utilizada na deteção proativa de ciberameaças", nomeadamente: mantendo uma análise automática da superfície de ataque; incorporando, de forma automática, inteligente e em contexto, informações de segurança; identificando potenciais ameaças com base na análise do histórico e contexto; computando mais elementos simultaneamente nos processos de decisão; acelerando o processo de adaptação das organizações ao padrão de ameaças e à tipologia de vulnerabilidades existente; e utilizando algoritmos preditivos para elevar ou baixar o nível de prontidão da defesa.

Luís Rato diz que a IA já "é uma ferramenta importantíssima" e permite "que as equipas de segurança possam rapidamente identificar e responder a estas ameaças antes que se tornem um problema crítico para a organização". No entanto, alerta, "não substitui o agente humano que deve estar preparado para treinar estes modelos de forma a serem cada vez mais responsivos e eficazes na deteção".

Ben Gelman indica que a IA se foca na telemetria, uma vez que "a quantidade de dados que uma base de clientes, mesmo relativamente pequena, pode gerar é enorme. Descobrir padrões e trazê-los à atenção dos analistas humanos é indispensável nas soluções modernas de cibersegurança".

> PERMITE A IDENTIFICAÇÃO, DE UMA FORMA MAIS RÁPIDA E DETALHADA, DE POSSÍVEIS VULNERABILIDADES EM SISTEMAS DE SEGURANÇA E TEM A CAPACIDADE DE EXPLORÁ-LAS PARA OBTER ACESSO NÃO AUTORIZADO A SISTEMAS E DADOS. A MESMA TEM SIDO UM RECURSO PARA ESTES AGENTES NA CRIAÇÃO DE CONTEÚDOS FICTÍCIOS PRÓXIMOS DA REALIDADE E CONTROLO DA MENSAGEM QUE SE QUER TRANSMITIR
>
> LUÍS RATO, NSO DA MICROSOFT PORTUGAL

Na mesma linha, Bruno Castro relembra que a IA tem "a capacidade de analisar grandes quantidades de dados em tempo real, identificar padrões, adaptar-se a novos cenários e torna-se assim uma ferramenta poderosa para a deteção proativa de ciberameaças". Como tal, "um desvio do padrão normal pode indicar uma possível ameaça e a IA vai detetar esse comportamento eficazmente e em tempo real. Além da análise de comportamento, também os algoritmos de processamento de linguagem natural conseguem analisar mensagens e conteúdos escritos e assim identificar possíveis ameaças em emails, mensagens instantâneas e outras formas de comunicação".

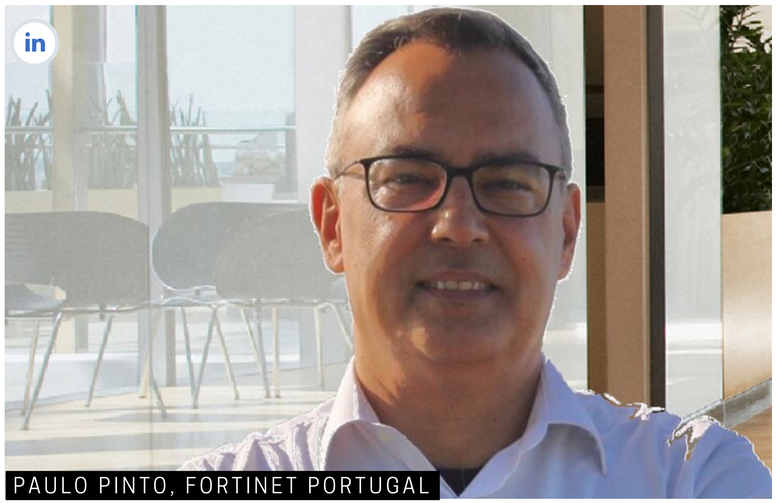
Paulo Pinto defende que, "da mesma forma que a IA pode ser utilizada para impulsionar táticas de ataque mais eficientes, também pode ser utilizada para prevenir e deter estes ataques. A adição desta ferramenta às soluções de cibersegurança tem sempre como objetivo ajudar as organizações a reduzir o tempo necessário para identificar e conter ameaças, além de condensar os prazos de investigação e correção".

A ABORDAGEM

É certo que a IA traz vários benefícios para a ciberdefesa da organização, mas, como diz Luís Rato, "também apresenta desafios para a segurança das suas infraestruturas". Explica o representante da Microsoft que "as organizações, nas mais diversas áreas de atividades, devem sobretudo munir-se das melhores soluções para dar resposta ao aumento de ciberataques e para que tal aconteça é essencial começar com uma avaliação cuidadosa das necessidades de segurança da organização e, em seguida, selecionar as soluções de IA que melhor respondam a essas necessidades".

Ben Gelman defende que as organizações "devem planear cuidadosamente a curadoria dos dados" na altura de integrar IA, uma vez que "é fácil cair na armadilha de armazenar dados e rotular informações ao acaso devido à sua escala e diversidade, mas os dados de qualidade são a 'tábua de salvação' da IA. Um fraco planeamento da recolha de dados pode causar atrasos de meses e incorrer em custos elevados para gerar rótulos especializados".

Bruno Castro refere que é preciso uma "abordagem estratégica cuidadosa" para "garantir que existem condições e capacidades" para incorporar eficazmente IA na cibersegurança. Assim, é "importante medir o risco e a recompensa, começando por avaliar os desafios específicos de segurança, avaliar as áreas onde a IA pode trazer melhorias significativas e as necessidades da própria organização. Outro fator fundamental será a definição de objetivos, isto é, estabelecer metas claras e mensuráveis para a implementação da IA na cibersegurança, determinar os resultados desejados e como melhorar a deteção de ameaças e resposta a incidentes".



PAULO PINTO, FORTINET PORTUGAL

Paulo Pinto, da Fortinet, explica que deve existir "uma abordagem holística em todas as camadas da arquitetura de segurança para uma proteção abrangente de toda a organização" que vai desde a "análise avançada de dados para identificar padrões e ameaças em tempo real", até à "automatização da resposta a incidentes". Ao mesmo tempo, acrescenta, é fundamental a adaptabilidade, exigindo-se que os algoritmos de IA "evoluam com as mudanças nas ciberameaças".

"A ADIÇÃO DESTA FERRAMENTA ÀS SOLUÇÕES DE CIBERSEGURANÇA TEM SEMPRE COMO OBJETIVO AJUDAR AS ORGANIZAÇÕES A REDUZIR O TEMPO NECESSÁRIO PARA IDENTIFICAR E CONTER AMEAÇAS, ALÉM DE CONDENSAR OS PRAZOS DE INVESTIGAÇÃO E CORREÇÃO".

PAULO PINTO, BUSINESS DEVELOPMENT MANAGER DA FORTINET PORTUGAL

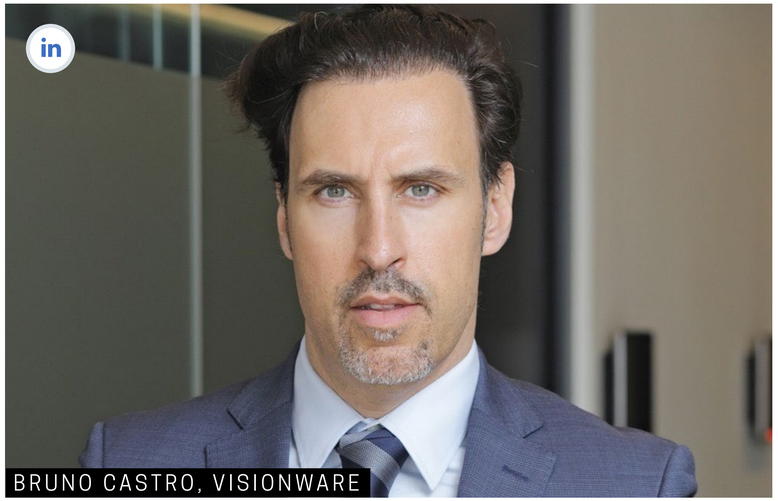
Para Rui Barata Ribeiro, as "duas grandes linhas de força estratégica" entre a cibersegurança e a IA são "como proteger as organizações usando IA" e "como proteger as diversas dimensões de utilização de IA nas organizações". O representante da IBM refere, com base no estudo "*Enterprise Generative AI: State of the market*" do IBM Instititute of Business Value, "que 84% dos executivos vê a cibersegurança (ou a falta de) como um dos principais bloqueios à adoção generalizada de IA no seu negócio".

RELAÇÃO HUMANO-MÁQUINA

Se é certo que a IA traz benefícios e desafios na sua implementação, a relação entre o humano e os sistemas de inteligência artificial tem de funcionar da melhor maneira possível. Ben Gelman refere que é preciso "criar confiança nos analistas humanos", até porque esta é uma preocupação "para as organizações que implementam" IA. "É raro que os modelos de IA apresentem explicações satisfatórias para as suas previsões, exigindo, por isso, avaliações

"IMPORTANTE MEDIR O RISCO E A RECOMPENSA, COMEÇANDO POR AVALIAR OS DESAFIOS ESPECÍFICOS DE SEGURANÇA, AVALIAR AS ÁREAS ONDE A IA PODE TRAZER MELHORIAS SIGNIFICATIVAS E AS NECESSIDADES DA PRÓPRIA ORGANIZAÇÃO".

BRUNO CASTRO, FUNDADOR E CEO DA VISIONWARE



BRUNO CASTRO, VISIONWARE

exaustivas e testes alargados para entrarem em produção. A proliferação de LLM nos fluxos de trabalho de cibersegurança está também a introduzir novos desafios jurídicos e de privacidade nesta área".

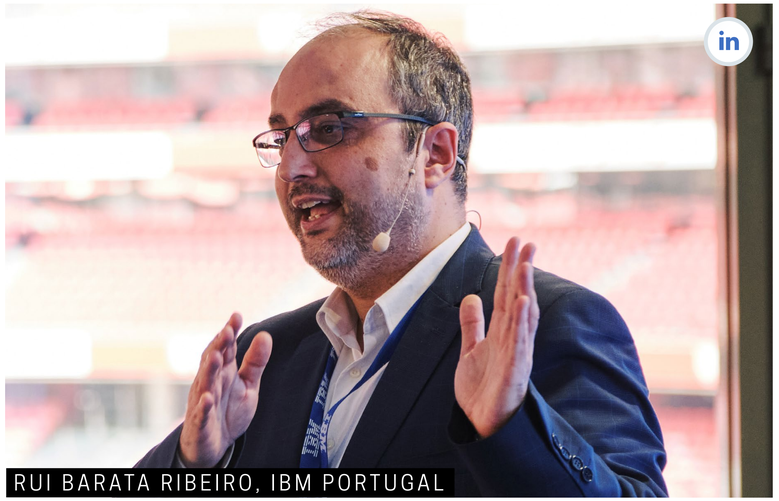
O representante da Sophos diz ainda que "a IA funciona como um multiplicador de forças, aumentando a produtividade e criando oportunidades", sendo importante notar que a IA "pode apresentar informações incorretas como se fossem factos". Assim, esta tecnologia "continua a ser uma solução altamente eficaz para muitos problemas, mas não elimina totalmente a necessidade de intervenção humana e de controlo de qualidade", ainda que no futuro se possa "assistir a uma mudança de paradigma".

Para Bruno Castro, a colaboração entre a IA e as equipas humanas "será fundamental para enfrentar os desafios complexos" do cenário de ciberameaças. "A IA vai colaborar com as equipas em várias vertentes: automatizar tarefas repetitivas e assim deixar mais tempo para que os profissionais se foquem em tarefas mais críticas; potenciar a deteção proativa de ameaças avançadas; fornecer *insights* com base em análises avançadas de grandes quantidades de dados; tornar mais rápida a resposta a incidentes e assim minimizar o impacto; classificar e priorizar alertas de segurança, destacando aqueles que exigem atenção imediata por parte dos profissionais; e,

ainda, a disponibilização de uma maior compreensão da natureza das ameaças para que os profissionais tomem decisões mais informadas e estratégicas", explica.

No caso da Fortinet, diz Paulo Pinto, a inteligência artificial é vista "como uma aliada poderosa para as equipas humanas" onde a tecnologia "não veio para substituir", mas sim "complementar as competências humanas". Para além da deteção avançada e da resposta rápida a incidentes, "a IA é particularmente eficaz na automatização de tarefas repetitivas, permitindo que as equipas humanas se concentrem em atividades mais estratégicas e complexas".

Já há vários anos que a IBM utiliza a expressão "inteligência aumentada" para a combinação de mecanismos de IA com aquilo que o humano pode trazer – como "perspetivas, conhecimento, experiência, intuição e inteligência". Não só no caso da cibersegurança, mas sim em tudo o que envolva IA,



RUI BARATA RIBEIRO, IBM PORTUGAL

refere Rui Barata Ribeiro, existe uma "necessidade de colaboração", até porque "todos os algoritmos e modelos fundacionais de IA devem ser explicáveis, de forma que os humanos os possam entender, bem como aos seus resultados" e, também, deve existir uma "equidade na forma como indivíduos ou grupos são processados e tratados, dependendo do contexto no qual o sistema de IA é usado".

"TODOS OS ALGORITMOS E MODELOS FUNDACIONAIS DE IA DEVEM SER EXPLICÁVEIS, DE FORMA QUE OS HUMANOS OS POSSAM ENTENDER, BEM COMO AOS SEUS RESULTADOS" E, TAMBÉM, DEVE EXISTIR UMA "EQUIDADE NA FORMA COMO INDIVÍDUOS OU GRUPOS SÃO PROCESSADOS E TRATADOS, DEPENDENDO DO CONTEXTO NO QUAL O SISTEMA DE IA É USADO".

RUI BARATA RIBEIRO, SECURITY SALES LEADER DA IBM PORTUGAL

Por seu lado, Luís Rato defende que "a relação homem-máquina é essencial para a eficácia dos modelos de linguagem de IA que procuramos desenvolver, a partir desta relação tirar o máximo partido desta tecnologia. Se a partir desta tecnologia as equipas conseguem dar resposta de uma forma bastante mais rápida às suas tarefas, isto trará benefícios para toda a organização, nomeadamente ao nível da segurança de toda a estrutura e informação".

O FUTURO DOS INVESTIMENTOS

Sabendo que a inteligência artificial já começa a ser implementada no seio dos processos internos das organizações – como na vertente de recursos humanos –, Bruno Castro refere que as organizações compreendem a "complexidade e constante evolução das ameaças cibernéticas" e estão a "alocar recursos substanciais para desenvolver e implementar soluções de IA avançadas. As organizações estão a explorar tecnologias emergentes, como redes neurais profundas e de processamento de linguagem natural, para aprimorar a capacidade de identificar e mitigar ameaças sofisticadas".

Paulo Pinto refere que "a implementação da IA nas empresas poderá ajudar na monitorização preventiva dos riscos e na melhoria das competências dos trabalhadores em matéria de cibersegurança", sendo que, em Portugal – e com base num estudo da Public First encomendado pela Google –, poderá mitigar 690 milhões de euros de riscos de cibersegurança.

Rui Barata Ribeiro explica que, atualmente, as tendências de utilização de inteligência artificial na ciberdefesa das organizações existe no contexto da "aquisição de soluções que incorporam capacidades de IA para o seu funcionamento", atrás de "um certo *hype*, às vezes pouco estruturado". No entanto, existem plataformas que têm desenvolvido modelos fundacionais para informação de cibersegurança que poderá ser implementada pelas organizações para "uma alimentação segura e controlada de informação a várias plataformas de cibersegurança diferentes".

Com o aumento do número e severidade dos ciberataques contra organizações, "o investimento em IA e soluções de cibersegurança tornou-se sem dúvida uma das maiores prioridades para os mais diversos quadrantes da nossa sociedade", afirma Luís Rato.

Para Ben Gelman, é "evidente, numa perspetiva de ciberdefesa, que a cibersegurança como serviço é uma parte inevitável e significativa do futuro". No caso dos SOC, a "IA é uma componente obrigatória" para o seu sucesso de grande escala "devido às limitações das equipas internas" e permite "uma quantidade limitada de conhecimentos humanos opere a uma escala global". ◀