BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

DEZEMBRO 2022 | nº 4/2022

DESTAQUES

Inteligência Artificial (IA)

A IA é uma inteligência não biológica, criada por humanos, capaz de realizar objetivos complexos de forma autónoma ou semiautónoma. Resulta em sistemas computacionais que recolhem dados do ambiente, eventualmente incompletos, de modo a realizar tarefas. As melhorias no processamento computacional, a disponibilidade de dados e o uso de algoritmos de aprendizagem permitiram grande avanços na IA (Tegmark, 2019).

IA e cibersegurança

Verifica-se uma crescente aplicação da IA na área da cibersegurança. Este uso tem benefícios para a segurança em si (e.g. na criação de sistemas de deteção de ameaças), mas também tem utilidade para os agentes de ameaça, como seja na criação de *deep fakes* para engenharia social na realização de fraudes ou em desinformação. Além disso, a opacidade dos algoritmos (falta de explicabilidade) também é um problema de segurança e confiança.

Regulamentação

A UE empreendeu um esforço regulatório em matéria de IA mediante uma proposta de Regulamento para a IA, a qual estabelece que certas aplicações de IA são proibidas (e.g. técnicas subliminares, classificação social) e que outras são consideradas de alto risco (e.g. identificação biométrica à distância, sistemas de recrutamento e seleção). Estas últimas devem sujeitar-se a algumas regras (e.g. análise de risco, garantia de robustez e registo dos dados).

PANORÂMICA

A ENISA – Agência da UE para a Cibersegurança apresentou, no dia 11 de novembro, uma análise prospetiva relativamente às principais ameaças emergentes para 2030. O abuso da IA é considerada a 10ª ameaça mais relevante num *ranking* de 10.

Este abuso é caracterizado como uma manipulação de algoritmos e de dados para atividades maliciosas, tais como a criação de conteúdos falsos e desinformação, a exploração de preconceitos, a recolha indevida de dados sensíveis ou o comprometimento de dados.

Em face das suas caraterísticas, o abuso da IA está presente de forma transversal em muitas das outras ameaças: na criação de campanhas avançadas de desinformação, na vigilância em práticas autoritárias, nos ataques a dispositivos inteligentes ou nas ameaças híbridas.

O *ENISA Threat Landscape 2022* mostra que a IA já é utilizada em alguns dos contextos de ameaça no presente, por exemplo, na criação de conteúdos que promovem fraudes e desinformação e no forjar de comunidades mediante *bots* que produzem comentários falsos.

As exfiltrações de grandes quantidades de dados, ou o acesso aos mesmos através de intrusões, podem também contribuir para os usos abusivos da IA, nomeadamente mediante o comprometimento desses dados e, em resultado, dos processos de decisão da IA.

PERSPETIVA

1 As tecnologias emergentes nem sempre são desenvolvidas com preocupações de segurança. Um dos problemas da Internet é não ter sido criada de raiz com funcionalidades suficientemente seguras. A cibersegurança tornou-se demasiadas vezes uma solução que surge depois da experiência de insegurança ocorrer e mostrar as vulnerabilidades dos sistemas. Para combater essa situação há que exigir que a segurança seja embebida nos sistemas logo na sua conceção.

2 É possível destacar 5 tarefas de cibersegurança a realizar na conceção da tecnologia: 1) compreender o seu contexto, de modo a conhecer as suas implicações (e.g. a cadeia de valor); 2) reduzir as possibilidades de ser atacada (e.g. evitando acessos desnecessários); 3) garantir a sua resiliência (e.g. mantendo cópias de segurança); 4) facilitar a deteção de um ataque (e.g. registando eventos); e 5) minimizar efeitos de possíveis ataques (e.g. segmentando os sistemas) (NCSC).

3 É importante aplicar estas ações no sentido de minimizar os riscos de uma nova tecnologia. O Regulamento da IA, de alguma forma, reproduz esta abordagem no campo regulatório de uma tecnologia específica. Alguns esforços nos EUA, nomeadamente o *The Blueprint for an AI Bill of Rights*, e *recomendações da OCDE* sobre a IA, também vão no sentido de criar mecanismos de regulação que promovam, entre outros aspetos, a segurança no desenvolvimento da IA.

4 Para uma IA segura, existem alguns desafios de longo prazo: desconfiança (a autonomização dos processos induz suspeita no humano); maior superfície de ataque e uso em serviços essenciais (a sua generalização cria oportunidades de ataque); complexidade e opacidade (a diversidade de competências e linguagens desafia a compreensão comum); e o uso abusivo de dados pessoais (a utilização de dados dos utilizadores periga o cumprimento do RGPD) (ENISA, 2018).

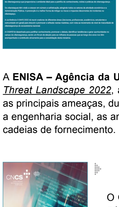
5 Não obstante estas questões, a IA é cada vez mais utilizada como solução de cibersegurança. Uma das capacidades que a IA tem, na medida em que é suportada em *machine learning* (aprendizagem automática), é a de identificar incidentes num sistema, tendo em conta aquilo que aprendeu recorrendo aos dados disponíveis. Esta capacidade permite, por exemplo, detetar intrusões com base nos dados que são fornecidos ao algoritmo de *machine learning*.

6 A longo prazo, há quem defenda que a IA pode trazer mais benefícios para a defesa do ciberespaço do que para o ataque, na medida em que permite substituir tarefas humanas que hoje não favorecem a segurança. As capacidades de efetuar atividades repetitivas em grande escala e analisar elevadas quantidades de dados permitem automatizar e melhorar a descoberta de vulnerabilidades, a reação a incidentes ou a identificação de tendências (Schneier, 2018).

PUBLICAÇÕES E NOTÍCIAS

No dia 20 de outubro, foi **aprovada a Estratégia Nacional de Ciberdefesa (ENC) pelo Conselho de Ministros**, documento articulado com a Estratégia Nacional de Segurança do Ciberespaço e as orientações do Conceito Estratégico de Defesa Nacional. A ENC define os seguintes objetivos: consolidar a capacidade de ciberdefesa; maximizar a resiliência e a coesão da ação nacional; promover a investigação, desenvolvimento e inovação; e garantir recursos qualificados.

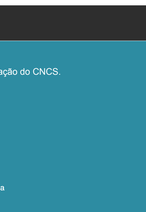
No dia 24 de outubro, foi **apresentada uma atualização** do *Referencial de Educação para a Segurança, Defesa e Paz*, utilizado na área de Educação para a Cidadania no ensino, contando agora com um tema dedicado à cibersegurança, desenvolvido pela Direção-Geral da Educação, o Instituto da Defesa Nacional e o Centro Nacional de Cibersegurança. Este referencial, embora facultativo, fica disponível para ser ministrado desde o ensino básico ao secundário.



No dia 27 de outubro, decorreu em Ponta Delgada **a primeira edição da conferência C-Days Acores**, onde se discutiram temas ligados à prevenção em cibersegurança e se lançou o calendário para os **primeiros cursos da C-Academy – Programa de Formação Avançada em Cibersegurança**, do CNCS. Já se encontram agendadas formações até ao final de 2023. Para interessados, as inscrições encontram-se disponíveis aqui.

A **ENISA – Agência da União Europeia para a Cibersegurança** publicou, no dia 3 de novembro, o *ENISA Threat Landscape 2022*, através do qual analisa as ameaças ao ciberespaço. O documento identifica como as principais ameaças, durante o segundo semestre de 2021 e o primeiro de 2022, o *ransomware*, o *malware*, a engenharia social, as ameaças aos dados, as ameaças à disponibilidade, a desinformação e os ataques às cadeias de fornecimento.

O **CNCS** organizou, no dia 3 de novembro, mais um Cibertema, desta feita com o título *Diferenças socioeconómicas: estará a cibersegurança ao alcance de todos?*, um debate com Rikke Jensen, do Royal Holloway, University of London, e Tiago Lapa, do CIES – Centro de Investigação e Estudos de Sociologia, do ISCTE-IUL. Para assistir à gravação deste e de outros Cibertemas basta aceder à seguinte página: ver.



O **CNCS** lançou, no dia 9 de novembro, mais um episódio do seu novo Podcast *Comunicar Cibersegurança*. O assunto tratado neste segundo episódio foram os resultados do *Relatório Cibersegurança em Portugal, tema Economia*, publicado este ano, e realizado por uma equipa da Universidade do Minho. Esta edição contou com os responsáveis que realizaram o estudo, Francisco Carballo-Cruz e João Cerejeira. Assista a todos os episódios na seguinte página: ver.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança