bilingue edition

ptsoc{news}

Desafios da IA na cibersegurança

3 perguntas a José Pedro Antunes

Referencial para uma abordagem pragmática por Inês Esteves

06

AI challenges in cybersecurity

3 questions to José Pedro Antunes

Referential for a pragmatic approach by Inês Esteves

.pt

DESAFIOS E OPORTUNIDADES DA ADOÇÃO DO SELO DE MATURIDADE DIGITAL – CIBERSEGURANÇA

11 de outubro • Edifício Barra Barra

16h30 | Abertura

Luisa Ribeiro Lopes, .PT

Mário Campolargo, Secretário de Estado da Digitalização e da Modernização Administrativa

16h45 | Tertúlia

Inês Esteves, .PT

Joana Lobo, APCER

Lino Santos, Centro Nacional de Cibersegurança

Raul Martins, Estrutura de Missão Portugal Digital

17h30 | Encerramento

Dora Moita, Imprensa Nacional-Casa da Moeda

Entrega de certificação "Selo de Maturidade Digital – Cibersegurança" pela Imprensa Nacional-Casa da Moeda ao .PT

PRÓXIMOS EVENTOS:

Inovação, Conhecimento e Cibersegurança Protocolo de Cooperação .PT e Cisco Systems

20 de outubro • Edifício Barra Barra

16h30 | Abertura

Cibersegurança: Tendências para 2023 Protocolo de Cooperação .PT e Women4Cyber

26 de outubro • Edifício Barra Barra

16h30 | Abertura

04 **Desafios da IA na cibersegurança.** AI challenges in cybersecurity

18 **Estatísticas** Statistics

Incongruências Inconsistencies

Crime sem deteção Undetected crime

O estado do ransomware industrial Industrial ransomware

Crescimento de 9% em cinco anos 9 % growth in five years

20 **3 perguntas a...** 3 questions to...

José Pedro Antunes

Coordenador Executivo do INCode.2030 Executive Coordinator of INCode.2030

27 **Referencial para uma abordagem pragmática** Referential for a pragmatic approach

Inês Esteves

Vogal Executiva do Conselho Diretivo do .PT Executive member of .PT's Board of Directors

32 **Documentos** Documents

KINDNS para segurança dos domínios KINDNS for domain security

Muitas horas perdidas Many lost hours

Cinco cursos universitários de cibersegurança Five cybersecurity university courses

IA ética e diplomática Ethical and diplomatic AI

Desafios da IA na cibersegurança

"Juntamente com os ciberataques 'tradicionais', o uso da inteligência artificial (IA) e da aprendizagem por máquina (ML) deixa os sistemas vulneráveis a novos tipos de ataque que exploram algoritmos e fluxos de trabalho de processamento de informações subjacentes. Todos os aspectos da segurança de um sistema de IA ou ML são potencialmente vulneráveis [e] sem entender e mitigar adequadamente essas vulnerabilidades, os responsáveis dos sistemas não podem garantir às partes interessadas e, em última análise, aos utilizadores, que um sistema de IA é seguro e protegido".

A explicação simples mas eficaz do National Cyber Security Centre do Reino Unido, que acompanha um recente guia de princípios para a segurança da ML, demonstra como novas tecnologias potenciam novos vetores para ciberataques. Isto ocorre quando os alertas de ataques informáticos "tradicionais" às organizações têm aumentado. Pode a IA ajudar neste domínio ou será apenas um enorme problema?

"A equipa de cibersegurança vê-se geralmente inundada com dados que precisa de classificar para gerir as suas ciberdefesas" e "a IA está a aparecer como uma ferramenta muito necessária no kit de ferramentas da cibersegurança",

AI challenges in cybersecurity

'Alongside "traditional" cyber attacks, the use of artificial intelligence (AI) and machine learning (ML) leaves systems vulnerable to new types of attack that exploit underlying information processing algorithms and workflows. All aspects of an AI or ML system's security are potentially vulnerable [and] without properly understanding and mitigating these vulnerabilities, system designers can't assure stakeholders, and ultimately users, that an AI system is safe and secure.'

The simple but effective explanation from the UK's National Cyber Security Centre, which accompanies a recent guide to principles for the security of machine learning, shows how new technologies leverage new vectors for cyber attacks. This occurs at a time when alerts of 'traditional' computer attacks on organisations have increased. Can AI help in this area or is it just an enormous problem?

'The cybersecurity team is generally flooded with data that they need to classify to manage their cyberdefenses,' and 'AI is emerging as a much-needed tool in the cybersecurity toolkit', states Sagar Samtani, a professor at the Indiana University (USA).

refere Sagar Samtani, professor na Universidade do Indiana (EUA).

Num ambiente de segurança confrontado com centenas ou mesmo milhares de alertas diários, "a IA é particularmente adequada para encontrar padrões em grandes quantidades de dados".

Ela pode ser usada em, pelo menos, duas situações. Primeiro, na automatização das tarefas normalmente atribuídas a analistas humanos, onde se "inclui a detecção automática de estações de trabalho, servidores, repositórios de código

In a security environment faced with hundreds or even thousands of daily alerts, 'AI is particularly well suited to finding patterns in huge amounts of data. '

There are at least two ways in which it can be used. First, it can help automate tasks often assigned to human analysts, which include 'automatically detecting unknown workstations, servers, code repositories and other unknown hardware and software on a network,' as well as '[to] allocate security defenses'.

e outro hardware e software desconhecido numa rede", assim como "alocar as defesas de segurança".

Por outro lado, "a IA pode ajudar a detectar padrões em grandes quantidades de dados que os analistas humanos não conseguem ver", como "padrões linguísticos de hackers que colocam ameaças emergentes na Dark Web e alertam os analistas", escreve Samtani, que alerta para uma vertente paralela da IA com impacto nas organizações: as pessoas.

"As empresas podem estar a pensar em substituir os seus analistas humanos por sistemas de IA, mas devem estar preocupadas com o quanto podem confiar em sistemas automatizados. Também não é claro se e como os problemas de IA bem documentados de enviesamento, equidade, transparência e ética surgirão em sistemas de cibersegurança baseados em IA".

Também a escassez de especialistas é um desafio: "é ainda mais difícil encontrar especialistas que conheçam ML e segurança" e que consigam falar a mesma "linguagem". "A colaboração entre esses dois grupos é a chave para aplicar com sucesso a ML à cibersegurança", escreve-se em "The Future of Machine Learning in Cybersecurity".

On the other hand, 'AI can help detect patterns within large quantities of data that human analysts can't see', such as 'key linguistic patterns of hackers posting emerging threats in the dark web and alert analysts', writes Samtani, who warns of a parallel element of AI impacting organisations: people.

'Companies might be thinking about replacing their human analysts with AI systems, but might be worried about how much they can trust automated systems. It's also not clear whether and how the well-documented AI problems of bias, fairness, transparency and ethics will emerge in AI-based cybersecurity systems.'

The shortage of specialists is also a challenge: 'it is even harder to find experts who know both ML and security' and how can speak the same 'language'. 'Collaboration between these two groups is the key to successfully applying ML to cybersecurity', is written in **'**The Future of Machine Learning in Cybersecurity**'**.

Credible solution or snake oil?

Another aspect of the use of these systems is the escalation of attacks and counter-attacks potentiated when both defenders and attackers use AI, namely generative adversarial networks (or GANs)

Solução credível ou "banha da cobra"?

Outra vertente do uso destes sistemas é a escalada de ataques e contra-ataques potenciada quando tanto defensores como atacantes usam a IA, nomeadamente redes adversárias generativas ("generative adversarial networks" ou GANs) que "lutam" entre si e se vão auto-melhorando em cada instância - criando melhor software de defesa mas também atacante, a partir de intermináveis batalhas.

A existência desta evolução da IA é consensual e, para usar o termo escolhido por Arvind Narayanan, professor na Universidade de Princeton (EUA), não se trata da "banha da cobra" que envolve estas disciplinas.

Dos anos 50-60 com os sistemas baseados em lógica aos baseados em conhecimento das décadas de 70-80 e em dados a partir deste século, as expetativas perante a IA têm evoluído por fases. A atual vive do sucesso relativo da "Machine Learning", de que fazem parte as GANs - cujo resultado mais visível têm sido as "deepfakes" (ver "Deepfakes: uma nova ciberameaça às organizações", na PTSOC {news} #3).

Narayanan concede que a IA é um termo que cobre "um conjunto de tecnologias relacionadas", algumas com um

that 'fight' each other and self-improve with each step they take - creating, from endless battles, a better defence software that also attacks.

The existence of this AI evolution is consensual and, to use the term chosen by Arvind Narayanan, a professor at Princeton University (USA), it is not the 'snake oil' that coats these subjects.

From logic-based systems from the 50-60s to knowledge-based ones from the 70-80s, also considering data from this century, the expectations towards AI have evolved in stages. The current one lives on the relative success of 'Machine Learning', of which GANs are part of - whose most visible result has been deepfakes (see 'Deepfakes: a new cyber threat to organizations', in PTSOC {news} #3).

For Narayanan, AI is an umbrella term for 'a set of related technologies', some with a 'genuine, remarkable, widely-publicized progress', also taken advantage of by companies that 'exploit public confusion, slap the "AI" label on whatever they're selling', presenting it to the 'credulous media' as a 'solution to all problems'.

He considers that we are 'far from perfect, but improving' in areas such as spam detection, detection of copyrighted material

"genuíno, notável, publicamente reconhecido progresso", mas aproveitado também por empresas que "exploram a confusão pública para colar a etiqueta IA no que vendem", apresentando-a aos "media crédulos" como uma "solução para todos os problemas".

Ele considera que se está "longe da perfeição mas a melhorar" em áreas como a deteção de spam ou de violação do direito de autor, ou na recomendação de conteúdos. A ML "nunca será perfeita nestas tarefas" mas evolui positivamente com a contribuição dos utilizadores humanos.

"Essencialmente dúbia" é a aplicação da IA na previsão, em ações como a análise das redes sociais para extrapolar potenciais ataques a empresas, por exemplo.

Em Março de 2021, Vânia Oliveira, autora da dissertação "Cibersegurança e Inteligência Artificial", listou as áreas da cibersegurança em que eram utilizados algoritmos de IA e de ML, e nelas incluiu a deteção de intrusão, malware, ransomware, DoS (Denial of Service) e phishing. Quanto às técnicas "promissoras", constam a ML, Natural Language Processing (NLP), automatização e robótica, "fuzzy logic" e "vision machine".

O uso de algoritmos de NLP ocorre na deteção de intrusões, ransomware e

or content recommendation. ML 'will never be perfect at these tasks' but evolves positively with the contribution of human users.

The use of AI is 'fundamentally dubious' when it comes to making predictions, such as when it analysis social media to extrapolate potential attacks on companies, for example.

In March 2021, Vânia Oliveira, author of the dissertation 'Cybersecurity and Artificial Intelligence', listed cybersecurity areas where AI and ML algorithms were used, and included intrusion detection, malware, ransomware, DoS (Denial of Service) and phishing. The 'promising' techniques include ML, Natural Language Processing (NLP), automation and robotics, fuzzy logic and machine vision.

NLP algorithms are used in intrusion detection, ransomware and phishing, while automation algorithms focus on malware. Fuzzy logic algorithms are more adapted to DoS attacks and phishing, and machine vision algorithms to intrusion detection.

Among this range of uses, it is clear that some of the doubts imposed on AI occur because a consensus definition of the concept has not yet been reached. In a document prepared by the European

phishing, enquanto os de automatização se focam no malware. Os algoritmos de lógica "fuzzy" são mais adaptados aos ataques por DoS e no phishing; os de visão por máquina na deteção de intrusões.

Nesta panóplia de utilizações, percebe-se que algumas das dúvidas impostas à IA ocorrem por não se chegar a uma definição consensual do conceito. Num documento preparado pelo European Parliamentary Research Service (EPRS) no início do ano, relativo à diretiva sobre a IA, salienta-se como a sua definição legal foi "muito criticada", pela falta de clareza e poder gerar incerteza legal nos programadores, operadores e utilizadores. Os autores da proposta de diretiva quiseram alargar o conceito de IA a sistemas computacionais usados em domínios de elevado risco. Segundo eles, "a vantagem estaria em tornar a aplicação das novas regras mais dependente do domínio em que a tecnologia é utilizada e dos riscos relacionados com os direitos fundamentais, e não de uma técnica computacional específica".

A IA, com "as suas características específicas (por exemplo, opacidade, complexidade, dependência de dados, comportamento autónomo), pode afetar negativamente vários direitos fundamentais e a segurança dos utilizadores", pelo que os autores da proposta de diretiva adotam uma abordagem baseada

Parliamentary Research Service (EPRS) at the beginning of the year on the AI directive, it is highlighted how its legal definition was 'heavily criticised' for lack of clarity, possibly leading to legal uncertainty with programmers, operators and users. The authors of the proposal for a directive wanted to extend the concept of AI to computer systems used in high-risk domains. According to them, 'the advantage would be in making application of the new rules more dependent on the domain in which the technology is used and the fundamental rights-related risks, rather than on a specific computational technique'.

AI, with 'its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour), can adversely affect a number of fundamental rights and users' which is why the authors of the proposal for a directive have followed an approach based on different risk levels: unacceptable, high, limited and low.

AI in Europe

The AI Act aims to be the first global-level legislation to regulate all sectors whether AI has an impact. In its current definition, an AI system is understood as a 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for

em diferentes escalões de risco: inaceitável, elevado, limitado e baixo.

IA na Europa

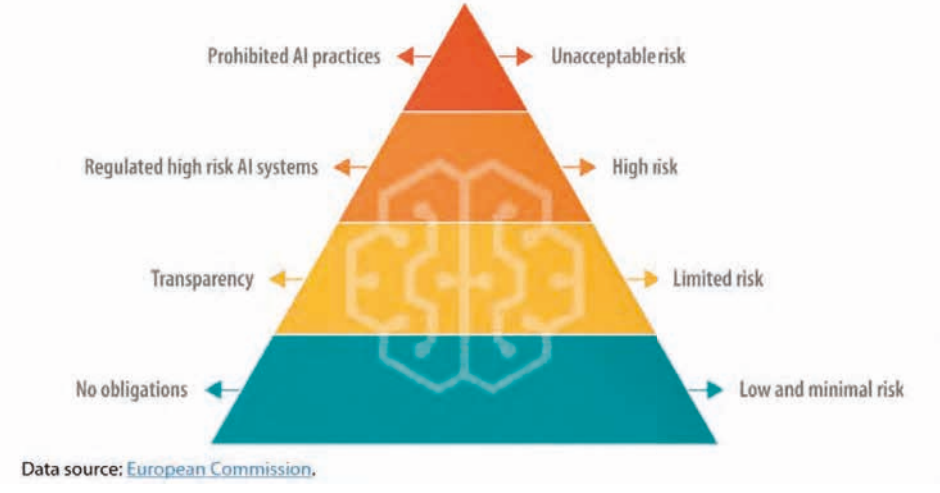
O AI Act pretende ser a primeira legislação a nível global a regular todos os setores on de a IA tenha impacto. Na sua definição atual, entende um sistema de IA como "um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage".

O referido anexo refere as abordagens de aprendizagem automática supervisionada, não supervisionada e por reforço,

a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.'

That abovementioned Annex refers to supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning. Others are logic- and knowledge-based, namely including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems. Finally, statistical approaches, Bayesian estimation, search and optimization methods.

The Council wants a less comprehensive definition, more focused on ML.



Data source: European Commission.

utilizando uma grande variedade de métodos, designadamente aprendizagem profunda. Outras são baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais. Por fim, as abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização.

O Conselho pretende uma definição menos abrangente e mais focada na ML.

Em Abril passado, os comités do PE para o Internal Market and Consumer Protection (IMCO) e o de Civil Liberties, Justice and Home Affairs (LIBE) apresentaram um relatório sobre o projeto de diretiva, com várias emendas.

Em Junho, num documento preparatório para a diretiva sobre IA, a Comissão realçou a importância desta na pandemia, com os sistemas usados no desenvolvimento de vacinas, na detecção de doenças por reconhecimento de padrões em imagens médicas ou em emergências com robôs a substituírem humanos. Mas acrescentava que os sistemas de IA podem "assegurar uma proteção mais eficiente contra os riscos da cibersegurança", como "tentativas maliciosas para explorar vulnerabilidades específicas da IA", incluindo:

Last April, the EP Committees on Internal Market and Consumer Protection (IMCO) and on Civil Liberties, Justice and Home Affairs (LIBE) presented a report on the draft directive**,** with several amendments.

In June, in a preliminary document on the AI act, the Commission stressed AI's importance during the pandemic, with the systems used in the quest for vaccines, in disease detection via pattern recognition using medical imagery or in emergency response with robots replacing humans. But it added that AI systems can 'ensure more efficient protection against cybersecurity risks' such as 'malicious attempts to exploit AI specific vulnerabilities', including:

Evasion - when an attacker modifies input data, sometimes in an imperceptible manner, so that the AI model cannot correctly identify the input and leads to wrong outputs.

Data poisoning - action aiming to modify the behaviour of the AI model by altering the training datasets, especially why web-scraped data, sourced from data exchanges or from open datasets.

Model extraction - attacks that aim to build a surrogate system that imitates the targeted AI model.

Evasão – quando um atacante modifica os dados de entrada ("input"), às vezes de maneira imperceptível, para que o modelo de IA não possa identificar corretamente os "inputs" e gere "outputs" errados.

Envenenamento de dados – ação para modificar o comportamento do modelo de IA alterando os conjuntos de dados de treino, especialmente quando extraídos da Web, provenientes de trocas de dados ou de conjuntos de dados abertos.

Extração de modelos – ataques para construir um sistema substituto que imita o modelo-alvo de IA.

"Backdoor" ou porta das traseiras – é um risco típico na programação, mas é mais difícil de detectar e evitar no caso da IA devido à sua opacidade.

Há também uma "falta de disposições claras de segurança que abranjam riscos específicos da IA", o que "pode ser altamente problemático para utilizadores e consumidores" destas aplicações.

Por fim, como a certificação na cibersegurança é voluntária, há um vazio de "normas estabelecidas de cibersegurança de IA de melhores práticas para programadores". Estas omissões prosseguem no processo paralelo de revisão da diretiva para a segurança dos sistemas

Backdoor - a typical risk in programming, which is more difficult to detect and avoid in the case of AI due to its opacity.

There is also a 'lack of clear safety provisions covering specific AI risks', which 'can be highly problematic for users and consumers' of these applications.

Finally, because cybersecurity certification is voluntary, there are no 'established AI cybersecurity standards of best practices for developers'. These omissions continue in the parallel review process of the Directive on Security of network and information systems - the NIS Directive, from 2016, transposed until 2018 and which had no mention of AI.

In January 2020, the European Commission (EC) announced its review. The public consultation ended in October 2020 and, in December, the EC announced a new cybersecurity strategy on the revised NIS 2.

The proposal was submitted to the European Parliament's (EP) Committee on Industry, Research and Energy (ITRE) in April of the following year, with an initial version released in May and the deadline for amendments to end in June.

The ITRE document was voted on in 2021 and adopted by the EP in November but the European Council amended it, nota-

em rede e de informação - a Diretiva NIS, de 2016, transposta até 2018 e que não tinha qualquer menção à IA.

Em Janeiro de 2020, a Comissão Europeia (CE) anunciou a sua revisão. A consulta pública terminou em Outubro de 2020 e, em Dezembro, a CE anunciou uma nova estratégia revista para a cibersegurança na NIS 2.

A proposta foi apresentada ao Comité para a Indústria, Investigação e Energia (ITRE) do Parlamento Europeu (PE) em Abril do ano seguinte, com uma versão inicial divulgada em Maio e o prazo para as emendas a terminar em Junho.

O documento do ITRE foi votado ainda em 2021 e adotado pelo PE em Novembro mas o Conselho Europeu alterou-o, nomeadamente com a exclusão de entidades de segurança nacional ou de defesa. O acordo político conseguido no início do Verão deve ser votado no PE antes do fim do ano. O período de transposição da diretiva foi fixado em 21 meses.

A NIS 2 já menciona a IA. O Conselho advoga que as entidades responsáveis no setor "devem avaliar as suas próprias capacidades de cibersegurança e, quando apropriado, procurar a integração de tecnologias de melhoramento da cibersegurança, como IA ou sistemas de ML para melhorarem as suas

bly excluding national security or defence entities. The political agreement reached at the beginning of the summer should be voted on in the EP before the end of the year. The period of transposition of the directive has been set at 21 months.

The NIS 2 already mentions AI. The Council advocates that the entities responsible in the sector 'must assess their own cybersecurity capabilities and, where appropriate, seek the integration of cybersecurity-enhancing technologies such as AI or ML systems to improve their capabilities and network protection'.

In addition, States should 'encourage the use of innovative technology, including AI, whose use can improve the detection and prevention of attacks against networks and information systems'. National research and development (R&D) strategies should also 'facilitate the use of such technologies, namely those related to (semi-)automated cybersecurity tools'.

With cybersecurity as one of its priorities in the current presidency of the European Council, the Czech Republic should not want to postpone the approval of the directives until 2023.

National ambition in innovation

Portugal follows Europe and AI's commitment to R&D to deal with an 'accel-

capacidades e a proteção de redes".

Além disso, os Estados devem "incentivar o uso de tecnologia inovadora, incluindo a IA, cujo uso pode melhorar a detecção e prevenção de ataques contra redes e sistemas de informação". As estratégias nacionais em investigação e desenvolvimento (I&D) devem igualmente "facilitar o uso de tais tecnologias, em particular as relacionadas com ferramentas (semi)automatizadas em cibersegurança".

Tendo a cibersegurança como uma das suas prioridades na atual presidência do Conselho Europeu, a Chéquia não deve querer adiar a aprovação das diretivas para 2023.

Ambição nacional na inovação

Portugal acompanha a Europa e o empenho na I&D da IA para lidar com a "acelerada concorrência no mercado global", refere-se em "AI Portugal 2030". O documento da estratégia nacional de IA, incluído no INCoDe.2030, apela ao uso da IA na saúde, clima, transportes, agricultura, indústria ou cibersegurança. A ambição é ter os setores mais inovadores portugueses "promovidos como 'living labs' para novas experimentações a nível global", nomeadamente na IA para redes de energia sustentável, para a condução autónoma ou na cibersegurança.

erated competition in the global market', refers the 'AI Portugal 2030' initiative. The national AI strategy document, included in INCoDe.2030, calls for the use of AI in health, climate, transport, agriculture, industry or cybersecurity. The ambition is to have the most innovative Portuguese sectors 'promoted as "living labs" for new experimentation at a global level', including in AI for sustainable energy networks, for autonomous driving or in cybersecurity.

This last one 'is increasingly important in a society with growing prevalence of information systems, many of which

Ela "é cada vez mais importante numa sociedade com crescente prevalência de sistemas de informação, muitos dos quais possuem IA. Um número crescente desses sistemas estará no controlo de instalações e infraestruturas críticas, que fornecem serviços essenciais a todos os cidadãos, como hospitais, fábricas, sistemas de purificação e abastecimento de água, transporte e sistemas integrados de gestão urbana. Outros serão ubíquos em unidades menores, como carros e outros veículos, robôs industriais e assistentes robóticos móveis. Os algoritmos de cibersegurança exigirão a capacidade de se adaptar a novos tipos de ataques e responder de maneira adequada e autónoma em tempo real".

Acresce que "a IA minimizará o tempo decorrido entre a detecção de um ataque e a reação correspondente do sistema. No entanto, os sistemas de IA podem estar sujeitos a ataques de segurança, dando origem a um novo e mais alto conjunto de práticas autónomas de gestão da cibersegurança". Foi isso que ocorreu em 2021, quando investigadores da Universidade de Zurique analisaram os processos de aprovação de 338 dispositivos médicos com IA ou ML nos EUA e na Europa. Eles detetaram falhas, nomeadamente enviesamentos na radiologia, com o treino de novos modelos e uma optimização para homens brancos. Isto afetava mulheres e pessoas de cor,

have AI. An increasing number of these systems will be in control of critical facilities and infrastructures, which provide essential services to all citizens, such as hospitals, power plants, water purification and provisioning systems, transport, and integrated urban management systems. Others will be ubiquitous in smaller units such as cars and other vehicles, industrial robots and mobile robotic assistants. Cybersecurity algorithms will require the ability to adapt to new kinds of attacks and respond accordingly and autonomously in real time.'

Moreover, 'AI will minimise the elapsed time between the detection of an attack and the system's corresponding reaction. However, AI systems may be subject to security attacks, giving rise to a new and higher set of autonomous cybersecurity management practices.' This is what happened in 2021, when researchers at the University of Zurich analysed the approval processes of 338 medical devices with AI or ML in the US and Europe. They detected flaws, namely biases in radiology, with the training of new models and an optimisation for white men. This affected women and people of colour, **'**amplifying existing inequalities.**'** It is in this model training that biases can be generated, synthesised in the expression 'garbage in, garbage out'. The problem can also occur in cybersecurity, with the absence of algorithm audits**.**

"amplificando desigualdades existentes". É neste treino dos modelos que se podem geram os enviesamentos, sintetizados na expressão "lixo que entra, é lixo que sai". O problema pode ocorrer igualmente na cibersegurança, com a ausência de auditorias aos algoritmos.

As ferramentas de ML para detetar e interromper ataques informáticos, sem intervenção humana, são rápidas a analisar incidentes e ganham mais experiência "aprendendo" com a ocorrência de mais eventos, acelerando a sua eficiência perante comportamentos anormais futuros.

Para tal, é necessário mostrar-lhes as mais recentes técnicas de hacking, algo difícil quando ainda não foram descobertas ou partilhadas. Isto serve igualmente na deteção e combate a botnets de DDoS ou para ransomware. No campo do malware, a tarefa é ainda mais difícil com o uso de vírus polimórficos.

De difícil deteção são também os "deepfakes". Em Agosto passado, um responsável da empresa Binance explicou como criminosos usaram um "holograma de IA" com a sua imagem para conseguirem reuniões com potenciais investidores com que ele próprio nunca tinha reunido. As imagens para criar o "deepfake" foram obtidas a partir de entrevistas televisivas.

Noutra vertente, estas imagens estão a

ML tools for detecting and stopping computer attacks, without human intervention, are quick to analyse incidents and gain more experience 'learning' from the occurrence of more events, accelerating their efficiency in the face of future abnormal behaviours.

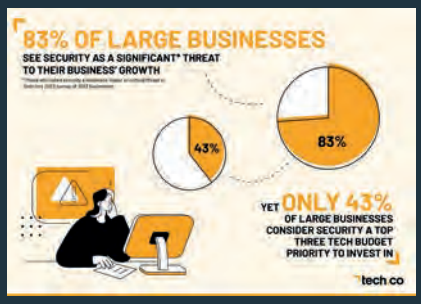
To do this, they need to be shown the latest hacking techniques, something difficult when they have not yet been discovered or shared. This can also be used when it comes to detecting and combating DDoS botnets or ransomware. In the field of malware, the task is even more difficult with the use of polymorphic viruses.

Deepfakes are also difficult to detect. Last August, a department head of Binance explained how criminals used an **'**AI hologram**'** with his image to get meetings with potential investors with whom he himself had never met. The images used to create the deepfake were obtained from television interviews. Elsewhere, these images are being used by impostors to respond to job offers. 'The main drivers appear to be money, espionage, access to company systems and unearned career advancement.' There is a lot of interest in the computer industry, namely in jobs with access to personal information from 'customers, financial data, corporate IT databases and/or proprietary information.'

ser usadas por impostores para responder a ofertas de emprego. "Os principais fatores parecem ser dinheiro, espionagem, acesso aos sistemas da empresa e progressão sem mérito na carreira". Há muito interesse no setor informático, nomeadamente em empregos com acesso a informação pessoal de "clientes, dados financeiros, bases de dados corporativas de TI e/ou informações proprietárias". Por enquanto, muitos destes esquemas têm falhado na deteção de imperfeições. Mas são tecnologias recentes que tenderão a melhorar e a criar novos problemas aos responsáveis da cibersegurança.

For now, many of these schemes have failed due to the detection of imperfections. But these are recent technologies that will tend to improve and create new problems for those responsible for cybersecurity.

Incongruências



As grandes empresas são as mais visadas pelos cibercriminosos mas embora 83% entenda a segurança como uma ameaça significativa ao seu negócio, apenas 43% a inclui como uma das três principais prioridades orçamentais de tecnologia. Entre as indústrias mais "cegas às ameaças" constam a hotelaria, distribuição e retalho. Nas PMEs, 63% vê a cibersegurança como uma ameaça ao negócio mas apenas 30% a terá como prioridade no investimento.

Inconsistencies

Large businesses are the most targeted by cybercriminals. Despite this, only 83 % of them perceive security as a significant threat to their business and 43 % include it as one of the top three technology budget priorities. Among the most 'threat-blind' industries are hospitality, wholesale and retail. When it comes to SMEs, 63 % of them see cybersecurity as a threat to their business but only 30 % will see it as an investment priority.

Crime sem deteção

Uma organização demora 197 dias a descobrir um ciberataque e 69 dias a corrigi-lo. Nos EUA, apenas 0,05% desses casos acaba por ser detetado ou leva a acusações na justiça. No entanto, o custo do cibercrime para as organizações em todo o mundo mais do que triplicou desde os 3.000 milhões de dólares registados em 2015. Os negócios mais vulneráveis são as instituições financeiras e bancárias, as de saúde, as empresas que lidam com dados pessoais e as instituições do ensino superior.

Undetected crime

It takes a company 197 days to discover a cyber attack and 69 days to fix it. In the US, only 0.05 % of these cases end up being detected or leading to court charges. However, the cost of cybercrime to organisations worldwide has more than tripled since the $3 billion recorded in 2015. The most vulnerable businesses are banks and financial institutions, healthcare institutions, corporations that deal with personal data, and higher education institutions.

O estado do ransomware industrial

No segundo trimestre deste ano, 23 grupos atacaram organizações industriais e fizeram 125 pedidos de ransomware, contra 158 nos primeiros três meses. A Europa sofreu 46 incidentes, seguida da América do Norte (36) e Ásia (32). Foi registada uma especialização de vários grupos em setores específicos de atividade ou geografias (como os Black Basta, Ransomhouse e Everest, que apenas atacaram nos EUA e na Europa). "O ransomware adaptou-se e evoluiu, está mais eficiente e provoca ataques mais devastadores", constatou também a ENISA neste "Threat Landscape for Ransomware Attacks", onde analisa 623 casos registados entre Maio de 2021 e Junho passado.

Crescimento de 9% em cinco anos

O mercado da cibersegurança deve crescer 8,9% até 2027. O valor estimado passará dos atuais 173,5 mil milhões de dólares para os 266,2 mil milhões de dólares. Nestes cinco anos, os fatores de crescimento são os ciberataques a empresas, a procura por soluções de segurança para a IoT, o aumento do número de violações de dados e as preocupações com as infraestruturas críticas.

Industrial ransomware

In the second quarter of 2022, 23 groups attacked industrial organisations and made 125 ransomware requests, up from 158 in the first three months. Europe as targeted in 46 incidents, followed by North America (36) and Asia (32). Several groups focused their activities in specific sectors of activity or geographies (such as Black Basta, Ransomhouse and Everest, which only attacked the USA and Europe). ENISA's 'Threat Landscape for Ransomware Attacks' report noted that 'ransomware has adapted and evolved, becoming more efficient and causing more devastating attacks', having analysed 623 reported cases between May 2021 and last June.

9 % growth in five years

The cybersecurity market is expected to grow by 8.9 % by 2027. The estimated value will go from the current $173.5 billion to $266.2 billion. In these five years, the growth factors are cyber attacks on enterprises, the demand for IoT security solutions, increased data breaches and growing concerns for cyber attacks on critical infrastructures.

3

José Pedro Antunes

Coordenador Executivo do INCoDe.2030
Executive Coordinator of INCoDe.2030

1. Quais os desafios para a cibersegurança na Inteligência Artificial (IA)?

São vários, mas irei abordar alguns que julgo serem mais prementes face à atualidade. Antes de mais, a exposição ao digital. O número de dispositivos ligados à Internet é, hoje, bastante elevado e com uma tendência de crescimento bastante acentuada. Este crescimento leva, não só, a um aumento dos riscos de segurança das organizações, mas também dos cidadãos. Veja-se, por exemplo, o que se passou no período do Covid-19. A maior permanência das pessoas em casa, levou a um aumento significativo de dispositivos ligados à Internet, em ambientes pouco preparados para lidar com questões de cibersegurança, o que teve como impacto o significativo aumento do número de ataques executados durante esse período.

Depois, a pouca literacia digital dos cidadãos no que respeita à segurança da informação. Sendo que esta é uma situação transversal a empresas e sociedade civil, revela-se sobretudo problemática entre os jovens que, pese a aptidão

1. What are cybersecurity's main challenges in the field of Artificial Intelligence (AI)?

There are several, but I'll address only a few that are more pressing right now. First of all, exposure to digital. Nowadays, the number of devices connected to the Internet is quite high and with a very strong growth trend. This growth leads not only to an increase in the security risks of organisations, but also of citizens. Take, for example, what happened during the COVID-19 period. The greater permanence of people at home led to a significant increase in Internet-connected devices, in environments poorly prepared to deal with cybersecurity issues, which resulted in a significantly increased number of attacks carried out during this period.

Then, there is citizens' lack of digital literacy in terms of information security. Since this is a cross-cutting situation for businesses and civil society, it is especially problematic among young people, despite their 'natural' aptitude for using digital devices, as they lack the knowledge about the risks and ethics associated with their use in Internet access. This is extremely concerning, because, combined with ignorance, there seems to be an exacerbated confidence that they will not be the target of attacks or that their personal data will not be misused.

Finally, the shortage of human resources with advanced skills in information security

"natural" para a utilização de dispositivos digitais, carecem de conhecimento sobre os riscos e ética associados à sua utilização no acesso à Internet. Um dado extremamente preocupante, pois, aliado ao desconhecimento, parece existir uma confiança exacerbada de que não serão alvo de ataques ou de que os seus dados pessoais não serão alvo de utilização indevida.

Por último, a escassez de recursos humanos com competências avançadas em segurança da informação e cibersegurança para fazer face às necessidades das organizações. Este é um problema de dimensão mundial. Para Portugal, considerando esta escassez de recursos humanos a nível global, a questão agudiza-se, já que os talentos formados nas nossas instituições são maioritariamente contratados para trabalhar fora do país.

Estes são os desafios que acho mais relevantes destacar e para os quais as tecnologias de IA podem ter um papel fundamental.

Gostaria de acrescentar, relativamente ao primeiro desafio, que a IA, ao analisar e interpretar grandes conjuntos de dados, vem contribuir para uma maior segurança face ao aumento de dados. Ao integrar tecnologias de IA com os sistemas de segurança, torna-se possível automatizar processos, identificar padrões de atuação, novos riscos e potenciais ataques, aumentar a eficiência na deteção de ameaças, e diminuir a carga de trabalho dos especialistas, ao mesmo tempo que aumenta a sua capacidade de processamento e entendimento

and cybersecurity to meet the organizations' needs. This is a worldwide problem. For Portugal, considering this shortage of human resources globally, the issue becomes even worse, since the talents trained in our institutions are mostly hired to work abroad.

These are, then, the challenges that I find most relevant to highlight and for which AI technologies can play a key role.

Still in relation to the first challenge, I would just like to add that AI, when analysing and interpreting large data sets, contributes to greater security in the face of increased data. By integrating AI technologies with security systems, it becomes possible to automate processes, identify performance patterns, new risks and potential attacks, to increase efficiency in detecting threats, and to reduce the workload of experts, while increasing its processing capacity and understanding of the information collected. Algorithms developed in AI, complemented with automation (RPA), enable the automatic correction of vulnerabilities and the configuration or reconfiguration of equipment, immediately responding to potential attacks.

We are aware that AI will not mitigate all the risks associated with human behaviour - the major risk factor of organisations and people themselves - but it will surely help in the detection, identification and implementation of measures to mitigate these risks by protecting organisations' security.

> "As tecnologias de IA não são diferentes e os hackers, normalmente indivíduos com elevadas competências tecnológicas e tempo para a preparação de soluções de ataque, têm consciência desse potencial."

sobre a informação recolhida. Os algoritmos desenvolvidos em IA, complementados com a automação (RPA), possibilitam a correção automática de vulnerabilidades e a configuração ou reconfiguração dos equipamentos, respondendo de forma imediata a potenciais ataques.

Temos consciência de que a IA não irá mitigar todos os riscos associados ao comportamento humano, o grande fator de risco das organizações e das próprias pessoas, mas seguramente irá ajudar na deteção, identificação e implementação de medidas que mitiguem esses riscos protegendo a segurança das organizações.

Qualquer tecnologia pode ser utilizada para o bem ou para o mal. As tecnologias de IA não são diferentes e os hackers, normalmente indivíduos com elevadas competências tecnológicas e tempo para a preparação de soluções de ataque, têm consciência desse potencial. Nesse sentido, se é verdade que a IA pode trazer benefícios na defesa das organizações, é igualmente verdade que pode ser utilizada para ataques mais sofisticados. Ataques que podem ser tão variados como a produção de notícias falsas ou a manipulação de imagens.

Concluindo, a utilização de IA em cibersegurança é fundamental para uma melhor proteção de bens e pessoas. É uma incerteza quem conseguirá ser mais eficiente e eficaz, se quem

Any technology can be used for good or for evil. AI technologies are no different and hackers, usually individuals with high technological skills and time to prepare attack solutions, are aware of this potential. Thus, if it's true that AI can bring benefits to the defence of organisations, it is equally true that it can be used for more sophisticated attacks - which can be as varied as the production of fake news or manipulating images.

> "AI technologies are no different and hackers, usually individuals with high technological skills and time to prepare attacks, are aware of this potential."

In conclusion, the use of AI in cybersecurity is critical to better protect assets and people. It's uncertain who will be able to be more efficient and effective, who defends, who attacks. The only certainty is that organisations must be prepared and seek, within their means, to invest in the training and awareness of employees regarding the technologies of the present, but also of the future.

2. Is Portugal well prepared to deal with these challenges?

No country is fully prepared to deal with all challenges. But in Portugal, as in Europe, measures are being taken and financial support is being provided that can help. Europe aims to achieve digital sovereignty. For this, its work plan foresees the provision of financial support for training,

defende, se quem ataca. A única certeza é a de que as organizações devem estar preparadas e procurar, naquelas que são as suas capacidades, investir na capacitação e sensibilização dos colaboradores para aquelas que são as tecnologias do presente, mas também do futuro.

2. Portugal está bem preparado para lidar com estes desafios?

Nenhum país está totalmente preparado para lidar com todos os desafios. Mas em Portugal, e na Europa, estão a ser tomadas medidas e disponibilizados apoios financeiros que podem ajudar. A Europa tem como objetivo alcançar a soberania digital, e para tal tem previsto no seu plano de trabalhos a disponibilização de apoios financeiros para a formação, investigação e inovação, desenvolvimento e implementação de soluções. Ações que visam suprir as necessidades das organizações e das pessoas no que respeita à capacitação e à digitalização da economia e da sociedade.

Destas medidas, podem elencar-se o apoio às instituições do ensino superior para a criação de mais cursos em competências digitais avançadas e apoio à investigação. Como?
- através do financiamento de projetos inovadores potenciados pelas tecnologias consideradas emergentes;
- financiamento à implementação de "hubs" de inovação digitais ligados aos diferentes sectores de atividade e que se espera tenham um forte impacto nas PMEs;
- zonas livres tecnológicas que permitem a

research and innovation, development and implementation of solutions. Actions aimed at meeting the needs of organisations and people with regard to the empowerment and digitalisation of the economy and society.

These measures may include supporting higher education institutions to create more courses in advanced digital skills and support research. How?
- By financing innovative projects powered by emerging technologies.
- By financing the implementation of digital innovation hubs linked to the different sectors of activity, expected to have a strong impact on SMEs.
- By creating technology-free zones allowing the experimentation of these technologies in a controlled and regulated manner.
- By creating regulation on the development and use of these technologies in accordance with the fundamental rights defended by the EU.

In Portugal, in addition to its alignment with the European strategy and the use of European funds, own funding has been made available, namely under the PRR [Portuguese Recovery and Resilience Plan], in order to further enable companies and public administration in its modernisation and transformation to this increasingly digital world. In terms of digital training, INCoDe.2030 plays a key role in its mission. The five axes of INCoDe.2030 present initiatives aimed at students up to year 12, at those who are active and need to acquire

experimentação destas tecnologias, de forma controlada e regulada;
- criação de regulação no desenvolvimento e utilização destas tecnologias de acordo com os direitos fundamentais defendidos pela EU.

Em Portugal, além do alinhamento com a estratégia europeia e utilização dos fundos europeus, tem sido disponibilizado financiamento próprio, nomeadamente ao abrigo do PRR, de forma a potenciar, ainda mais, empresas e administração pública na modernização e transformação para este mundo, cada vez mais digital. Ao nível da capacitação digital, o INCoDe.2030 tem, no âmbito da sua missão, um papel fundamental. Nos seus cinco eixos tem iniciativas dirigidas a alunos até ao 12° ano, aos que estando no ativo necessitam de adquirir novas competências para se manterem no mercado de trabalho, aos que, por diferentes motivos, se encontram numa situação de exclusão, até aos que, tendo competências digitais, necessitam de adquirir competências avançadas. Tod@s devem ser incluídos digitalmente.

A este papel acrescenta-se, ainda, a responsabilidade do INCoDe.2030 na coordenação de algumas das principais estratégias nacionais de tecnologias emergentes, como é o caso da Estratégia Nacional de IA.

No que respeita à resposta aos desafios na utilização de IA na área da cibersegurança, algumas organizações, públicas e privadas, já tomaram a dianteira e adotaram algumas iniciativas na sua utilização e integração com di-

new skills to remain in the labour market, at those who, for different reasons, are in a situation of exclusion, and even at those who, despite already having digital skills, need to acquire advanced skills. All must be included digitally.

In addition to this role, INCoDe.2030 is responsible for coordinating some of the main national strategies for emerging technologies, such as the National AI Strategy.

Regarding the response to challenges in the use of AI in cybersecurity, some public and private companies have already taken the lead and adopted some initiatives in their use and integration with different tools. However, there is still a long way to go. Companies that can develop a technological roadmap and hire specialised resources, whether cybersecurity or AI technologies, are still a minority.

It's important to highlight that more than 95% of our business fabric comprises micro-, small- and medium-sized companies, and that they need specialised support in skills as well as in tools. Under the PRR, some initiatives are being prepared, namely in the area of cybersecurity, which are expected to support SMEs in the preparation and implementation of information security and training processes. Although important and necessary, these initiatives are only a small part of the solution.

ferentes ferramentas. No entanto, ainda existe um longo caminho a percorrer. Ainda são uma minoria as empresas que conseguem desenvolver um "roadmap" tecnológico e contratar recursos especializados, seja de cibersegurança ou de tecnologias de IA.

É importante realçar que mais de 95% do nosso tecido empresarial é composto por micro e PMEs, e que estas necessitam de apoio especializado em competências e em ferramentas. Ao abrigo do PRR estão a ser preparadas algumas iniciativas, nomeadamente na cibersegurança, que se espera virem a apoiar as PMEs na preparação e implementação de processos de segurança de informação e formação. Apesar de importantes e necessárias, estas iniciativas são apenas uma pequena parte da solução.

Muito tem sido feito ao longo destes últimos anos. Não podemos esquecer-nos que este é um processo contínuo e que há muito mais a fazer. A velocidade de inovação e transformação tecnológica é cada vez maior, novos desafios vão surgir e só com uma constante atualização, de tecnologias e competências, por parte das organizações e dos cidadãos, podemos preparar-nos para responder a novos riscos e vulnerabilidades.

3. O AI Portugal 2030 acompanha a visão europeia de apostar em áreas de maior potencial - saúde, clima, transportes, agricultura, indústria ou cibersegurança. Houve capacidade interna e recursos humanos desde o lançamento

Much has been done over the last few years. However, we must not forget that this is an ongoing process and that there is much more to be done. The speed of innovation and technological transformation is increasing, new challenges will arise and only with a constant update of technologies and skills, by organisations and citizens, can we prepare ourselves to respond to new risks and vulnerabilities.

3. At AI Portugal 2030, we follow the European vision of investing in areas of greater potential - health, climate, transport, agriculture, industry or cybersecurity. Did we have internal capacities and human resources since the launch of the national strategy in 2019?

As I've mentioned earlier, the shortage of human resources with advanced skills in the STEM areas [science, technology, engineering and mathematics] is a worldwide problem. One of the main objectives of the European Commission is to train up to 20 million specialists by 2030.

At a national level, a great effort has been made to train professionals specialised in these areas. The training offer in digital skills has been growing, both in different levels of education and in training by public and private entities. INCoDe.2030, in its different axes, has continuously supported the development of initiatives that include

dessa estratégia em 2019?

A escassez de recursos humanos com competências avançadas nas áreas STEM ["science, technology, engineering and mathematics"] é um problema mundial. Um dos grandes objetivos da Comissão Europeia é conseguir formar cerca de 20 milhões de especialistas até 2030.

A nível nacional, tem sido feito um grande esforço no sentido de formar profissionais especializados nestas áreas. A oferta formativa em competências digitais tem vindo a crescer, quer nos diferentes graus de ensino, quer na formação por parte de entidades públicas e privadas. O INCoDe.2030 tem apoiado de forma contínua o desenvolvimento de iniciativas que incluem todos na capacitação digital. Por exemplo, o Centro Nacional de CiberSegurança, prevê o desenvolvimento de uma academia com cursos online de formação básica em cibersegurança, na plataforma NAU. Esta oferta também tem aumentado em áreas como a computação avançada, blockchain, ciência dos dados, robótica e IA.

Acredito, por isso, que a Estratégia Nacional serviu de bússola para as diferentes organizações, incluindo do ensino superior. Em 2019, já se assistia a projetos de investigação, produtos e oferta comercial e formativa, mas a mensagem nela inserida confirmou a necessidade das organizações olharem para as tecnologias de IA como ferramentas de apoio ao desenvolvimento da sua atividade, na otimização de processos internos, conhecimento de clientes ou de inovar e criar novos modelos de negócio.

digital training for everyone. As an example, the Portuguese National Cybersecurity Center (CNCS) has planned the creation of an academy. Meanwhile, it made a set of online basic cybersecurity training courses available through the NAU platform. In addition to this, it has also been increasing its offer in areas such as advanced computing, blockchain, data science, robotics and AI.

I therefore believe that the National AI Strategy served as a compass for different organisations, including those of higher education. In 2019, when it was first published, there were already research projects, products and commercial and training offers but the message it contained confirmed the need for organisations to look at AI technologies as tools to support the development of their activity, whether in the optimisation of internal processes, customer knowledge or to innovate and create new business models.

Inês Esteves

Vogal Executiva do Conselho Diretivo do .PT
Executive member of .PT's Board of Directors

Referencial para uma abordagem pragmática

Numa sociedade mais digital, num mundo cada vez mais interconectado e dependente da tecnologia, é muito elevada a exposição a ataques cibernéticos de diferentes níveis de maturidade e a capacitação desta para os temas da cibersegurança.

A par do mediatismo e significativo impacto dos ataques recentes perpetrados a setores relevantes como a saúde, defesa, comunicação social, telecomunicações ou banca, 48% de PMEs portuguesas sofreram, pelo menos, um tipo de crime cibernético em 2021, segundo os dados do Eurobarómetro "SMEs and Cybercrime", publicado pela Comissão Europeia em maio de 2022.

É urgente e absolutamente fundamental que o tecido empresarial português, constituído maioritariamente por PMEs, enderece práticas claras e integradas de cibersegurança e de gestão do risco na sua gestão, sendo este um dos grandes desafios da liderança num contexto de acelerada transformação digital.

Referential for a pragmatic approach

In an increasingly digital society, in a progressively interconnected and technology-dependent world, exposure to cyber attacks with different maturity levels is very high, as is its capacity for cybersecurity issues.

Alongside the media coverage and significant impact of recent attacks on relevant sectors such as health, defence, media, telecommunications or banking, 48% of Portuguese SMEs suffered at least one type of cybercrime in 2021, according to Eurobarometer 'SMEs and Cybercrime' data, published by the European Commission in May 2022.

It is urgent and absolutely essential for Portuguese businesses, made up mainly of SMEs, to include clear and integrated cybersecurity and risk management practices in their management. This is one of the great leadership challenges in a world of accelerated digital transformation.

It is true that the financial capacity for

É certo que a capacidade financeira de investimento e capacitação em cibersegurança desempenham um papel relevante nos níveis de maturidade das organizações, mas não podem constituir-se como impedimento ou desresponsabilização na sua adoção. A liderança tem aqui o papel essencial na definição da estratégia e integração clara destes temas nas organizações que dirigem, a qual deve assentar num posicionamento colaborativo, alinhado com boas práticas e "standards" de segurança reconhecidos, que contribuam para a diminuição da sua exposição ao risco e para uma maior ciber-resiliência.

Procurando desconstruir a excessiva complexidade que muitas vezes é impressa a este tema, pretende-se identificar uma abordagem pragmática dirigida às organizações que querem endereçar a cibersegurança, mas que não sabem por onde começar.

O referencial DNP TS 4475-1:2021, o primeiro normativo a ser concretizado no contexto do Sistema Nacional de Certificação de Maturidade Digital, que endereça o pilar da cibersegurança (tema que aprofundámos na PTSOC News #5) é um excelente ponto de partida, podendo constituir-se como um guião para a adoção de boas práticas de cibersegurança.

investment and training in cybersecurity play a relevant role in the maturity levels of organisations, but they cannot be seen as an impediment or accountability when it comes to their implementation. Leadership plays a key role in defining the strategy and the clear integration of these issues in the organisations it directs; its direction must be based on a collaborative positioning, aligned with good practices and recognised security standards that contribute to a reduced risk exposure and a greater cyber-resilience.

Seeking to deconstruct the excessive complexity that is often imprinted on these issues, we intend to identify a pragmatic approach aimed at organisations that want to address cybersecurity, but do not know where to start.

The DNP TS 4475-1:2021 referential is the first normative to be implemented by the National Digital Maturity Certification System. It addresses the cybersecurity pillar (an issue we have deepened in PTSOC News #5), an excellent starting point, and can be a guide for the adoption of good cybersecurity practices.

With three requirement levels (bronze, silver and gold), it has a progressive adoption structure that allows any type of company or organisation to select the

Com três níveis de exigência (bronze, prata e ouro), tem uma base de adoção progressiva que permite que qualquer tipo de empresa ou organização selecione o nível mais adequado às suas capacidades, dimensão, estrutura e objetivos.

Não se trata de um sistema de gestão, como preconizado pela família das normas ISO. Segue antes uma abordagem mais pragmática, ágil e menos formal das boas práticas de cibersegurança a incorporar, e cujo primeiro nível, bronze, estabelece os requisitos mínimos, de simples adoção, mas de elevado impacto na mitigação dos riscos de cibersegurança mais comuns, que qualquer organização que utiliza a tecnologia e o digital tem de endereçar para minimizar a sua exposição ao cibercrime.

Vamos por pontos:

Conhecer a norma: começar por adquirir a norma DNP TS 4475-1:2021, disponível na versão portuguesa, junto do Instituto Português da Qualidade;

Criar uma cultura de segurança: os requisitos da norma focam-se em três áreas essenciais - organizacional, humana e técnica. Constituir uma equipa multidisciplinar, com uma visão holística da organização, com

level best suited to its capacities, size, structure and objectives.

This is not a management system, as advocated by the ISO family of standards. Rather, it follows a more pragmatic, agile and less formal approach to good cybersecurity practices to be incorporated. The first level, bronze, establishes the minimum requirements; these are easy to implement but have a high impact in mitigating the most common cybersecurity risks that any organisation that uses technology and digital tools must address to minimise their exposure to cybercrime.

Let's take it one step at a time:

Get to know the standard: Start by acquiring the DNP TS 4475-1:2021 standard, available in Portuguese from Instituto Português da Qualidade;

Create a culture of safety: The standard's requirements focus on three key areas - organisational, human and technical. Building a multidisciplinary team, with a holistic view of the organisation, with the ability to influence and facilitate the adoption of safe practices and behaviours will be a strategic factor for the creation of a true cybersecurity culture.

Assess: Carry out a gap analysis, which is

capacidade de influenciar e facilitar a adoção de práticas e comportamentos seguros serão um fator estratégico para a criação de uma verdadeira cultura de cibersegurança.

Avaliar: realizar um "gap analysis", que mais não é do que uma verificação entre o estado da arte da organização face aos requisitos elencados na norma para cada um dos níveis de exigência. Utilize um "template" que permita documentar e espelhar os resultados obtidos, identificando possíveis abordagens para responder adequadamente aos "gaps" identificados.

Estabelecer laços de cooperação: há um conjunto de entidades com responsabilidades em matéria de cibersegurança, onde o .PT se inclui, que podem colaborar na adoção de boas práticas e na capacitação para estas matérias, constituindo-se como parceiros de implementação.

Definir um plano de ações: claro, exequível, com metas temporais realistas, o qual deve ser permanentemente acompanhado, garantindo a implementação das ações definidas.

Comunicar e capacitar: a cibersegurança é uma responsabilidade partilhada. Colaboradores informados e sensibilizados para estas matérias são o primeiro

nothing more than a check between the organisation's state of the art in view of the requirements listed in the standard for each of the requirement levels. Use a template to document and mirror the results obtained, identifying possible approaches to adequately respond to the identified gaps.

Establish cooperation ties: There is a set of entities with cybersecurity responsibilities, where .PT is included, which can collaborate in the adoption of good practices and training for these issues, becoming implementation partners.

Set an action plan: Clear, feasible, with realistic time targets, it must be permanently monitored, ensuring the implementation of the defined actions.

Communicate and empower: Cybersecurity is a shared responsibility. Employees who are informed and made aware of these issues are the first pillar of the organisation's protection.

Internal audit: Promote an independent check of the level of compliance of the organisation with the standard's requirements. This will allow for greater security and confidence in the implementation process.

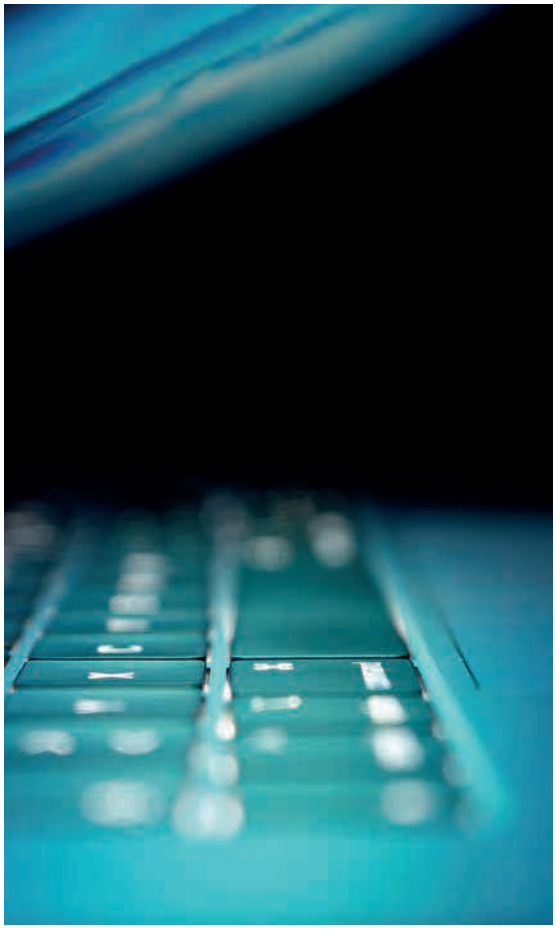
pilar da proteção da organização.

Auditoria interna: promover uma verificação independente do nível de conformidade da organização face aos requisitos da norma, a qual permitirá uma maior segurança e confiança do processo de implementação.

Certificação: porque não? Sendo certo que a adoção da norma DNP TS 4475-1:2021 não exige a sua certificação, o objetivo central é o efetivo alinhamento com boas práticas de segurança que contribuam para a diminuição da exposição ao risco e para uma maior ciber-resiliência. A certificação confere às organizações a garantia da sua maturidade digital, o que se traduz num posicionamento de maior diferenciação, competitividade e visibilidade no seu contexto de atuação.

Fotos: Philipp Katzenberger_ unsplash

Certification: Why not? While the adoption of the DNP TS 4475-1:2021 standard does not require its certification, its main objective is the effective alignment with good security practices that can contribute to reduce the risk of exposure and to greater cyber-resilience. Certification ensures organisations their digital maturity, which translates into a positioning of greater differentiation, competitiveness and visibility in their operations.



KINDNS para segurança dos domínios

A ICANN lançou a iniciativa Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS), para promover boas práticas operacionais e normas de segurança do sistema de nomes de domínio (DNS). A ICANN pretende encorajar essas medidas junto dos operadores, antecipando que assim "contribuirá para a segurança, estabilidade e resiliência da infraestrutura que suporta a Internet".

KINDNS for domain security

ICANN has launched the Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS) initiative to promote good operational practices and domain name system (DNS) security standards. ICANN intends to have these measures implemented with operators, anticipating that it will 'contribute to the security, stability and resilience of the infrastructure that supports the Internet.'

Muitas horas perdidas

Um total de 5.106 horas perdidas a gerir 168 incidentes, dos quais 91% atribuído a erro humano. Os dados de 2021 relativos aos operadores de telecomunicações foram revelados pela ENISA no "Telecom Security Incidents", tendo mostrado no relatório "Trust Services Security Incidents" que foram as falhas de sistema as principais causas (47%) desses incidentes.

Many lost hours

A total of 5 106 hours where lost managing 168 incidents, of which 91 % were attributed to human error. ENISA's 'Telecom Security Incidents' revealed 2021 data on telecommunications operators; their 'Trust Services Security Incidents' report showed that system failures were the main causes (47 %) of these incidents.

Cinco cursos universitários de cibersegurança

Com a escassez de recursos humanos na cibersegurança, a formação tende a acelerar para (re)qualificar pessoas neste setor. Nos EUA, algumas universidades estão a fazê-lo, como sucede com a New York University (curso "Introduction to Cyber Attacks"), Stanford University ("Cryptography I"), University of Maryland ("Hardware Security"), University of Michigan ("Internet History, Technology, and Security") e Western Governors University, com o curso "Network and Security Foundations".

IA ética e diplomática

A Europa quer liderar os avanços tecnológicos na inteligência artificial, fazendo-os acompanhar de uma proteção ética, onde inclui a privacidade e os dados pessoais. O AI Act pode ser uma diretiva pioneira, pela sua classificação setorial e gradual de riscos associados, mas também pela potencial aplicação em quase 30 países. Por isso, pode também ser uma ferramenta na geopolítica e na diplomacia externa - não só útil mas também necessária, como explica este documento do Parlamento Europeu, "AI diplomacy".

Five cybersecurity university courses

With the shortage of human resources in cybersecurity, training tends to happen at a faster pace in order to (re)qualify people in this sector. This is what some US universities are doing, as is the case with New York University ('Introduction to Cyber Attacks'), Stanford University ('Cryptography I'), University of Maryland ('Hardware Security'), University of Michigan ('Internet History, Technology, and Security') and Western Governors University, with the 'Network and Security Foundations' course.

Ethical and diplomatic AI

Europe wants to lead technological advances in AI, pairing them with ethical protection, including privacy and personal data. The AI Act may be a pioneering directive, for its sectoral and gradual classification of associated risks, but also for its potential application in nearly 30 countries. It can thus also be used as a geopolitical and foreign diplomacy tool - not only useful but also necessary, as this 'AI diplomacy' document explains.

Directora | Director
Inês Esteves

Edição | Editor
Pedro Fonseca

Design Gráfico | Graphic Design
Sara Dias
Maria Cristóvão

Tradução | Translation
Sara Pereira

Fotografia (capa e índice) | Photography (cover & index)
Joakim Honkasalo | Unsplash
Pawel Czerwinski | Unsplash

Publicação trimestral | Quarterly publication
Setembro 2022 | September 2022