Editorial

Cibersegurança: da prevenção do risco à gestão de incidentes

Cybersecurity: from risk prevention to incident management

João Emílio de Almeida[1],[2]

joaoalmeoda@my.istec.pt

[1] ISTEC Porto, Centro de Investigação em Tecnologias Avançadas (CITECA), Rua Dr. Lopo de Carvalho, 70, 4350-162 Porto, Portugal.

[2] Universidade do Porto, Laboratório de Inteligência Artificial e Ciência da Computação (LIACC), Rua Dr. Roberto Frias, s/n 4200-465 Porto, Portugal.

DOI: 10.17013/risti.43.1-4

1. Introdução

Não é de hoje a preocupação com a segurança dos sistemas informáticos. Com a criação dos primeiros computadores surgiram os ataques cibernéticos mais variados. Desde os anos 80, pelo menos, que os vírus informáticos são transmitidos de computador para computador. No início eram as disquetes. Depois vieram os CDs, DVDs e as "pendrives". Com o advento da internet e do e-mail, a sua difusão aumentou e expandiu-se a todo o mundo. Ainda antes da terrível pandemia provocada pelo vírus SARS-CoV-2, que a todos nos afeta, já os vírus informáticos nos andavam a complicar a vida: aos utilizadores, administradores de sistemas, responsáveis e gestores em todos os níveis hierárquicos das mais diversas organizações.

Como acontece com todos os riscos que não podem ser eliminados, resta a prevenção e a mitigação. Os ataques informáticos são cada vez mais sofisticados, difíceis de detetar e combater. No livro "Big Breaches", recentemente publicado, Neil Daswani (co-diretor do Advanced Cyber Security Program de Standford) e Moudy Elbayadi (consultor de segurança em empresas multinacionais) alertam para os custos astronómicos que as falhas e ataques de segurança têm atingido. Os alvos já não são apenas as empresas ou particulares, mas organizações governamentais e até países. O famoso caso das eleições

presidenciais de 2016 eleva os incidentes cibernéticos à categoria de ciberterrorismo e ataque militar, conduzidos de forma discreta e sub-reptícia por países contra outros países.

O uso da informação como arma já vem de longe, não é novidade. Os incríveis avanços tecnológicos têm trazido, como consequência, um crescente aumento do valor da informação e da importância da detenção das técnicas mais avançadas para o seu controlo. Os EUA, líderes neste domínio, já há décadas que se dedicam a espiar e a registar todas as comunicações e transferências de dados digitais a que conseguem aceder. A agência responsável pela espionagem das telecomunicações, a NSA (National Security Agency), durante muitos anos teve a sua existência negada pelas próprias entidades oficiais. Chegou a ser ironicamente denominada por No Such Agency.

Nas várias guerras do Golfo, a utilização de técnicas cibernéticas para anular os sistemas informáticos do inimigo, por exemplo, os sistemas de defesa anti-aéreos, foram fundamentais para o sucesso das forças aliadas. Hoje, a dimensão da guerra cibernética atinge um patamar muito mais elevado, com a destruição de satélites, interferências em sistemas vitais (distribuição de eletricidade e água, centrais nucleares, etc.). Não é segredo que países como a Coreia do Norte e a China, a par da Rússia, têm efetuado ataques cibernéticos a redes norte-americanas. Embora não o confirmem oficialmente, há um grande investimento em tecnologias para ataque e defesa das instalações cibernéticas.

Também ao nível das empresas, os ataques consistem no roubo de informação, ou então no seu sequestro, como é o caso do "*ransomware*". É praticamente impossível ficar imune a estes ataques. Resta aumentar as defesas, antecipar os ataques e gerir as crises o melhor possível.

A Inteligência Artificial é uma arma que tem sido utilizada na prevenção e na defesa aos ataques cibernéticos. Antecipando possíveis falhas, colmatando vulnerabilidades e tentando ultrapassar os danos causados, de forma automática, para que as interrupções de comunicações, a recuperação dos dados e o restabelecimento de serviços sejam feitos o mais rapidamente possível, minimizando prejuízos e reduzindo os tempos de inatividade. Como se diz no mundo do espetáculo "*the show must go on!*".

Cabe a cada um de nós, como utilizador, desenvolvedor ou administrador de sistema (possivelmente desempenhando estas três funções cumulativamente), adotar as medidas preventivas, as boas práticas recomendadas, estar atento às vulnerabilidades que vão aparecendo e atuar imediatamente sempre que alguma brecha ou ataque sejam detetados.

Para esta edição foram selecionados seis artigos para publicação nesta edição da RISTI, depois de devidamente escrutinados pelos membros do comité científico.

Foram submetidos pelos autores um total de 146 artigos, sob a temática dos sistemas e tecnologias de informação, o que corresponde a uma apertadíssima e exigentíssima taxa de aceitação de 4,1%.

2. Estrutura

O primeiro artigo, com o título "*Aplicação das Redes Neuronais Artificiais para classificação das operações de perfuração: O caso de poços deepwater de Exploração e Produção*" apresenta dois procedimentos independentes para identificar o melhor modelo de NPT (Non-Productive Time) e PT (Productive Time) aplicados aos processos de perfuração de poços de petróleo localizados a grande profundidade. As conclusões apontam o modelo Multi-layer Perceptron (MLP) como o melhor modelo. O sistema de classificação pode ser utilizado para produzir um relatório preciso e detalhado sobre as atividades realizadas durante a perfuração de um poço. Os resultados apresentados permitem concluir que os relatórios diários de perfuração representam uma fonte rica de informação e podem ser utilizados para melhorar o processo de construção de poços de petróleo.

O segundo artigo, com o título "*Rendimiento académico y patrones de uso del campus virtual: Un estudio de caso controlado*" apresenta a análise de dados recolhidos a partir de plataformas de ensino recorrendo a tecnologias digitais, para apoio ao professor. O objetivo deste estudo consistiu em utilizar os registos das ferramentas digitais para apoio ao ensino, num caso controlado, com o mesmo professor, mesma área de conhecimento e metodologia docente, mas cursos diferentes, se existem diferenças no comportamento dos estudantes, no que se refere a rendimento académico, consoante o género, ano do curso e acesso aos recursos digitais. Os resultados obtidos apontam para que os alunos do primeiro ano tenham um comportamento mais polarizado e com maiores diferenças; as estudantes são mais ativas digitalmente, havendo uma relação mais positiva entre qualificações e atividade digital nos estudantes do quarto ano. A análise dos dados agrupados confirma as diferenças dos alunos nos diferentes cursos, condicionado ao uso e desempenho digital.

O terceiro artigo, cujo título é "*Análisis para la implementación de la tecnología 5g basados en el modelo GSMA y su interacción con el internet de las cosas en Ecuador*". Neste estudo, foi analisada a opção de implantação a ser seguida pelas operadoras móveis do Equador para a implantação da tecnologia 5G baseada no modelo GSMA e sua interação com a Internet das Coisas (IoT). Apresenta uma pesquisa sistemática da literatura, em que foram utilizadas quatro perguntas com o objetivo de analisar a implementação da tecnologia 5G e a sua interação com a IoT. As conclusões apontam que ainda existe um caminho a percorrer no Equador para as operadoras procederem à transição para a tecnologia 5G e a implementação da IoT ligada às cidades inteligentes (smart cities).

O quarto artigo, com o título "*Facilitadores, barreras y recomendaciones sobre el uso de las Tecnologías Digitales de la Información y la Comunicación por adultos con parálisis cerebral en Brasil*" aborda o tema do uso das tecnologias de informação e comunicação (TIC) para melhorar a qualidade de vida dos adultos com limitações físicas, em particular com paralisia cerebral. A partir de doze entrevistas a pessoas do sul do estado de São Paulo, Brasil, são indicadas as facilidades e benefícios que as TIC

apresentam para as pessoas com paralisia cerebral, concluindo com recomendações para melhorias a introduzir em futuros desenvolvimentos da TIC que facilita ainda mais a o dia a dia destas pessoas.

O quinto artigo, com o título "*Aceitação do Aviso de cookies e criação de publicidade direcionada: uma decisão consciente ou falta de informação?*" enquadra-se plenamente nas preocupações expressas no editorial desta revista: aborda o tema da segurança na navegação na Internet, associado à recolha de dados personalizados dos utilizadores, através de "cookies". Apesar do Regulamento Geral sobre a Proteção de Dados (RGPD) que foi aprovado pelo Parlamento Europeu, ainda existe falta de informação e de formação dos utilizadores em relação a este assunto. O artigo publica os resultados obtidos através de um inquérito a 242 utilizadores em Portugal.

O sexto artigo, com o título "*Sistema de Visão Computacional para Identificação Automática de Potenciais Focos do Mosquito Aedes aegypti Usando Drones*" apresenta um sistema de visão computacional (SVC), através de imagens recolhidas a partir de um drone, para identificação de potenciais focos do mosquito *Aedes aegypti* que se encontra associado à transmissão de doenças como o dengue, chikungunya e zika. Através de uma rede neuronal do tipo CNN, são apresentados resultados mais precisos quando comparados com outros encontrados na literatura. Este sistema poderá trazer melhorias aos programas de prevenção e combate de fontes de reprodução de mosquitos, com a utilização de drones e SVC, ao providenciar dados mais fidedignos com uma maior taxa de acerto. Trata-se também de uma área importante da segurança, neste caso, associada à saúde pública.

3. Agradecimentos

Esta introdução termina agradecendo a todos os autores e membros do conselho científico e editorial que participaram no processo de revisão dos artigos que compõem esta edição, desejando que este número de RISTI seja mais um contributo para a transição digital, em que a tecnologia é colocada ao serviço da humanidade e da paz, para o progresso e desenvolvimento harmonioso da sociedade.

Um agradecimento especial às Bases de Dados de Revistas Académicas como CiteFactor, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, ISI Web of Knowledge, Latindex, ProQuest, QUALIS, SciELO, SCImago y Scopus, entidades que contribuem para que a RISTI seja uma revista científica de referência.