

# Use of AI in Computer Networks

Ana Filipa Pereira, Carolina Santejo, and Raquel Costa

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal

e-mail: {a89500,a89589,a89464}@alunos.uminho.pt

**Resumo** Cada vez mais a Inteligência Artificial (AI) tem uma presença mais notável no nosso quotidiano, seja, por exemplo, na automatização de tarefas ou no gerenciamento de grandes volumes de dados. Com a evolução desta área nasceram dois conceitos muito importantes: Machine Learning e Deep Learning. Quando falamos em redes de computadores é necessário realçar o papel da AI na capacidade de as gerir, processar e principalmente proteger de possíveis vulnerabilidades, uma vez que, dado o crescente volume de dados e uso de tecnologias diariamente, é preciso recorrer a ferramentas para lidar com toda esta complexidade. O desenvolvimento contínuo desta área torna-a cada vez mais suscetível a ataques cibernéticos. Assim, foram concebidos algoritmos que ajudam a detetar e eliminar potenciais ameaças. A AI tem vantagens em domínios específicos mas, no que toca a conceitos mais abstratos é requerida a nossa capacidade intelectual.

## 1 Introdução

“We are changing the world with technology”

Se há algo que podemos afirmar sobre as redes de computadores é que estas revolucionaram a atualidade. Seja uma *local area network* que permite a partilha de ficheiros entre dois computadores relativamente próximos, ou a própria internet, a verdade é que as networks se tornaram indispensáveis. Quebraram as barreiras geográficas da comunicação e da partilha de informação tornando-as praticamente instantâneas. Atualmente, as redes de computadores são peças fundamentais, por exemplo, em qualquer empresa ou negócio. No entanto, com a constante evolução e aumento da complexidade das networks, torna-se necessário encontrar formas eficazes de as gerir e de as manter seguras. Neste trabalho iremos abordar o papel da Inteligência Artificial na gestão e segurança de redes.

## 2 INTELIGÊNCIA ARTIFICIAL

### 2.1 Tecnologia AI

Quando falamos de tecnologia AI não podemos deixar de mencionar o matemático Alan Turing, pai da computação e pioneiro da Inteligência Artificial. Um dos seus artigos foi uma das primeiras reflexões sobre as

possibilidades de as máquinas simularem comportamentos inteligentes. Atualmente, apercebemo-nos que cada vez mais estamos rodeados por este tipo de tecnologia, como por exemplo o reconhecimento facial, funcionalidade esta que integra as mais recentes especificações dos smartphones. A Inteligência Artificial é um conceito abrangente dentro da área da computação, sendo que o seu principal objetivo é desempenhar tarefas que tipicamente requerem a inteligência humana. Assim sendo, trata-se de uma grande ajuda na análise de grandes volumes de dados e na automatização das tarefas quotidianas.

## 2.2 Machine Learning vs Deep Learning

Machine Learning e Deep Learning são dois subdomínios da Inteligência Artificial, sendo que o conceito de Deep Learning é visto como uma evolução de Machine Learning que usa *neural networks* de modo a conseguir tomar decisões mais exatas sem a intervenção do ser humano.

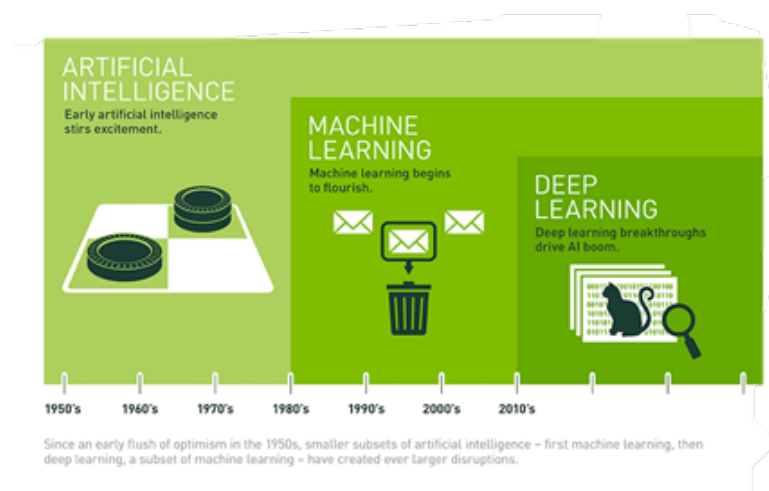


Figura 1. Evolução AI

- **Machine Learning:** De uma forma geral, podemos dizer que se baseia em algoritmos que analisam e filtram certos dados, de forma a aprender com eles para depois determinar ou prever algo sem alguma ajuda explícita. Os algoritmos de ML baseiam-se em dados estruturados e são construídos para irem aprendendo através desses mesmos dados. À medida que o tempo passa, a máquina começa a prever situações cada vez melhor, pois vai recebendo mais informações e com estas aprende cada vez mais. É importante também salientar que a diversidade de perspetivas e de dados melhora também a sua eficácia e performance.

- **Deep Learning:** Estes algoritmos funcionam de uma forma bastante similar aos de Machine Learning, a diferença é que existem diversas camadas organizadas hierarquicamente e cada uma delas tem a sua interpretação e definição de certos aspetos. A isto damos o nome de *artificial neural networks*, uma vez que

o seu funcionamento é parecido com o do cérebro humano. Estas redes não precisam de dados estruturados como acontece em Machine Learning, uma vez que elas recebem o input e processam-no de forma a obter o resultado correspondente.

É importante referir que estas tecnologias são aplicadas dependendo do contexto de cada caso, uma vez que, há certas características de Machine Learning que se “encaixam” melhor num tipo de situação, tal como há situações onde a abordagem mais eficiente a ser feita é através de Deep Learning. Portanto, se estivermos a tratar de dados de menor escala e volume, e que sejam facilmente classificados, tal como o reconhecimento e classificação de imagens, optamos por Machine Learning. Por exemplo, se queremos que a nossa máquina tenha a capacidade de distinguir um cão de um gato, então mostramos-lhe uma série de imagens devidamente classificadas e especificando as características de cada um. Após isso, a máquina irá conseguir distinguir ambos os animais. Neste caso, a abordagem mais eficiente será a de Machine Learning, pois, tal como vimos, os seus algoritmos são feitos para aprender com dados devidamente classificados e estruturados, para depois aplicar esses mesmos critérios de classificação que lhe foram instruídos. Já a aplicação das neural networks de deep learning acontece num maior volume de dados, uma vez que a sua organização de camadas hierárquicas adequa-se a uma maior complexidade de problemas, ao contrário dos algoritmos de Machine Learning. Tal como é de prever quanto melhor for a qualidade e diversidade da informação passada, melhor será o resultado final.

## **2.3 AI no gerenciamento de redes**

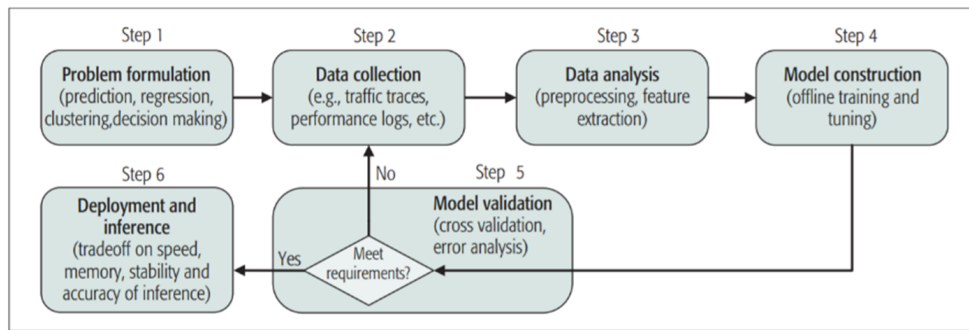
### **□ Porque é que recorremos a AI quando falamos de redes de computadores?**

Com as grandes evoluções tecnológicas no mundo ao nosso redor e o constante aumento de dados e dispositivos nas redes, é impossível depender apenas do ser humano para analisar, processar e agir. Portanto, é necessário um método que permita gerenciar esta crescente complexidade de uma forma rentável e eficaz. Para tal, recorre-se à inteligência artificial, uma tecnologia que revela ser uma grande ajuda quando falamos do processamento de grandes volumes de dados no menor tempo possível.

### **□ Qual a estratégia para ajudar no gerenciamento de redes?**

Primeiramente, é importante salientar que as capacidades de ML tais como a classificação e previsão desempenham um papel fulcral para resolver problemas como a deteção de intrusões e a previsão do desempenho nas redes de computadores, uma vez que estamos a lidar com comportamentos imprevisíveis e padrões variáveis característicos de cada rede. Podemos caracterizar o fluxo de trabalho de ML aplicado nas redes em vários passos [figura 2].

Há certos elementos que são indispensáveis quando falamos de uma abordagem AI num problema. Seja qual for essa solução, é importante que, garantidamente, se baseie em grandes volumes de informação de qualidade e diversificada, uma vez que, é através desses dados obtidos e da sua consequente análise que a máquina consegue aprender e construir a sua inteligência ao longo do tempo. “The more diverse the data



**Figura 2.** Funcionamento de ML nas redes de computadores

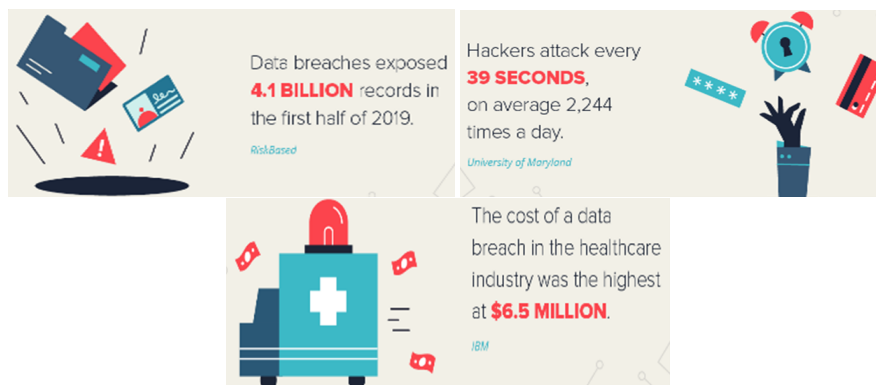
collected, the smarter the AI solution becomes”. Dispositivos móveis ou até routers, não só precisam de recolher dados rapidamente como também processá-los, de modo a manter a rede o mais adaptável possível. Além disso, é necessário dados devidamente classificados entre todos os domínios específicos envolvidos no problema, pois assim a máquina consegue dividir o problema em vários segmentos, de modo a facilitar a sua resolução. Posteriormente, é feita a implementação de algoritmos de ML ou de *neural networks* que depois da análise dos dados irão encontrar a resolução mais adequada. Finalmente, umas das técnicas também usadas neste campo é a *Virtual Network Assistant*, que muitos de nós podemos experienciar no nosso dia a dia quando, por exemplo, em plataformas como a *Netflix*, recebemos recomendações de filmes ou séries com base no que temos visto e nas preferências que vamos revelando à medida que escolhemos o que assistir. Este método é aplicado em grandes volumes de dados de modo a identificá-los e a relacioná-los através de similaridades para solucionar um problema.

Com a aplicação desta tecnologia aos domínios das redes de computadores, surgem imensos benefícios e aplicações. Entre estes podemos destacar as práticas de *cybersecurity*.

### 3 AI e cybersecurity

“Quanto mais inteligente a ameaça, mais inteligente precisa de ser a proteção”

Como foi referido anteriormente, a constante evolução das redes de computadores faz com que estas se tornem mais complexas e inovadoras, mas também mais vulneráveis. Estas vulnerabilidades podem ser tanto a nível de hardware como de software e são, por exemplo: a má gestão da rede, o controlo de acesso às redes não é aplicado, um sistema que não possui a atualização mais recente ou simplesmente um router de wi-fi com uma fraca password. Todas estas falhas são “pontos de entrada” na rede, tornando possíveis ataques informáticos (estes cada vez mais diversificados e sofisticados) que põem em risco a segurança dos dados e informação de utilizadores e empresas.

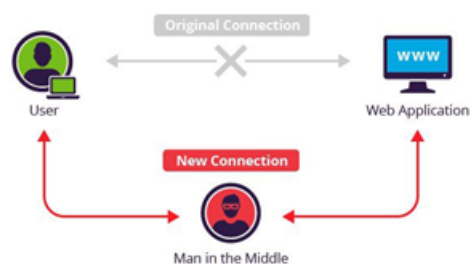


**Figura 3.** Dados e estatísticas sobre cybersecurity

### 3.1 Exemplos de CyberAttacks

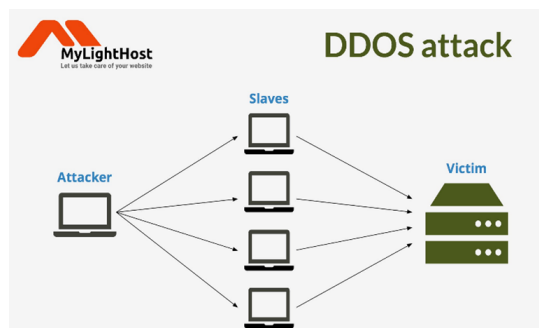
Seguem-se dois exemplos de “Cyber Attacks” que achamos pertinentes referir:

- **Man-in-the-Middle (MITM):** MITM é bastante comum quando acessamos, por exemplo, redes WiFi públicas. Neste tipo de ataque cibernético, o “hacker” interceta a comunicação entre duas entidades. Usando um método conhecido como “IP spoofing” ele altera o seu IP de forma a fazer-se passar por ambas as partes em questão (por exemplo um utilizador e um website ou um router). Desta forma o “hacker” passa a ter acesso a todo o tráfego gerado e conseqüentemente toda a informação partilhada entre as entidades, sem que estas se apercebam.



**Figura 4.** Man-in-the-middle

- **Denial-of-service attack (DoS):** Este ataque tem como objetivo impedir o bom funcionamento de algum sistema, servidor ou rede. Isto consiste em sobrecarregar com tráfego o alvo, de forma a que este não seja capaz de o gerir (devido ao esgotamento dos recursos e da largura de banda). Desta forma o sistema acaba “por crashar”.



**Figura 5.** Denial-of-service attack

### 3.2 Utilização da AI em CyberSecurity

“A Inteligência Artificial é capaz de detetar 85% dos ciberataques”

Sistemas que apliquem os princípios da inteligência artificial permitem, com a informação que possui e que vai adquirindo, criar e consolidar um padrão, ou seja, definir aquilo que é “aceitável”. Se os algoritmos de AI perceberem atividades incomuns ou qualquer comportamento que esteja fora do padrão, eles sinalizam como sendo anomalia, podendo mesmo bloqueá-la. No entanto, isto leva-nos àquele que é um dos problemas da AI: a probabilidade de falsos positivos, uma vez que nem sempre uma atividade fora do padrão é uma ameaça. Mas é de realçar que esta probabilidade apesar de existir, vai diminuindo com cada nova “interação”, dado que o sistema está constantemente a aprender com os erros e a evoluir. Alguns tipos de comportamentos suspeitos são, por exemplo: aumento drástico de download de ficheiros ou da velocidade de digitação, ou ainda a efetuação de compras online anormalmente grandes. A deteção destas possíveis ameaças pode ser feita através de vários métodos como por exemplo: a deteção de endereços IP, URLs (etc...) suspeitos, padrões de digitação ou a análise de tráfego de rede através da utilização de firewalls tradicionais ou complementadas com AI. Estas “smart firewalls” são mais eficazes que as tradicionais uma vez que permitem uma análise mais profunda dos pacotes de rede, detetar tráfego criptografado.

**Huawei Launches the Industry’s First AI-Based Firewall, Enabling Intelligent Enterprise Border Protection**

Oct 17, 2018

**Figura 6.** Huawei: Adoção da tecnologia AI para segurança nas redes

- **Gmail uses machine learning to block 100 million spams in a day.** It has developed a system to filter out emails and offer a spam-free environment efficiently.
- IBM's Watson cognitive training uses machine learning to detect cyber threats and other cybersecurity solutions.
- **Google is using Deep Learning AI on its Cloud Video Intelligence platform.** On this platform, the videos stored on the server are analyzed based on its content and context. The AI algorithms send security alerts whenever something suspicious is found.
- Balbix platform uses AI-powered risk predictions to protect the IT infrastructure against data and security breaches.

**Figura 7.** Google: Aplicações de ML e DL

Acabamos de referir métodos para detetar ameaças usando a inteligência artificial. No entanto, surge a questão: como é que os sistemas a partir de uma ameaça conseguem alargar o seu conhecimento, e detetar outras que possam vir a surgir? Existem vários meios para o fazer, mas falaremos apenas de um conhecido como “Campaign Hunting”. “Campaign Hunting” consiste em detetar possíveis novas ameaças, usando semelhanças encontradas em ameaças já detetadas. Segue-se um exemplo para melhor exemplificar: Imagine-se que foi encontrado um URL malicioso. O que o algoritmo baseado nos princípios de AI faz é encontrar novos URLs semelhantes àquele que foi encontrado. E que semelhanças são estas? Podem ser várias, nomeadamente semelhanças lexicográficas, os URLs serem registados pela mesma pessoa ou no mesmo período, entre outras. A partir destas novas ameaças descobertas aplica-se o mesmo processo, descobrindo, assim, anomalias que de outra maneira poderiam passar despercebidas.

“In fact, more than 10 percent of the cyberattacks we block today are based on intelligence gained solely through Campaign Hunting.”

## **4 AI vs Inteligência humana**

### **4.1 Inteligência humana**


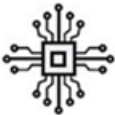
Inteligência humana é a capacidade intelectual que nos permite pensar, aprender através de diferentes experiências, entender conceitos complexos, aplicar a lógica e a razão, resolver problemas matemáticos, reconhecer padrões, tomar decisões, reter informação e comunicar com outros seres.

## 4.2 Balanço tecnologia-humanidade

Cada vez mais, a humanidade se vê obrigada a utilizar a tecnologia nas mais diversas áreas visto que seria impossível executar certas tarefas por muito simples que elas sejam, por exemplo o processamento de grandes quantidades de dados num curto período de tempo. No entanto há funções que requerem as nossas capacidades tais como a tomada de decisões, de facto, mesmo as maquinas mais avançadas estão ao nível de uma criança de 6 anos no que respeita a esta categoria, por causa da nossa capacidade de aprender através das experiencias. Por estas razoes, é necessário retirar o melhor de cada uma e encontrar um balanço.

## 4.3 Qual é a melhor?

Apesar da grande evolução tecnológica, como se pode fundamentar através da tabela abaixo [Figura 8], a AI ainda está longe de superar a mente humana nos mais diversos aspetos, por isso é que o ser humano, nos tempos que correm, nunca poderão ser totalmente substituídos por máquinas.

	Weight	Space	Processor Speed	Energy Efficiency
	3 pounds (1.4 kg)	1/6 basketball (80 cubic inches or 1,300 cm <sup>3</sup> )	Up to 1,000,000 trillion operations per second	20 watts
	150 tons	Basketball court (cabinets over 4,350 square feet, or 400 m <sup>2</sup> )	93,000 trillion operations per second	10 million watts

**Figura 8.** AI vs Inteligência Humana

## 5 Conclusão

Neste trabalho, não só refletimos sobre a importância da inteligência artificial e a sua presença cada vez mais marcante no nosso dia a dia, como também aprofundamos o nosso conhecimento na área, nomeadamente a diferença entre *Machine Learning* e *Deep Learning*. Além disto, abordamos o papel da AI enquanto aliada no combate ao cibercrime e sua importância na gestão de redes.



## Referências

1. Alpaydin, E.: Machine Learning: The New AI (2016)
2. Paul R. Daugherty, H. James Wilson: Human + Machine: Reimagining Work in the Age of AI (2018)
3. Mowei Wang, Yong Cui, Xin Wang, Shihan Xiao, and Junchen Jiang Machine Learning for Networking: Workflow, Advances and Opportunities (2015)
4. Raouf Boutaba, Mohammad A. Salahuddin, Noura Limam, Sara Ayoubi, Nashid Shahriar, Felipe Estrada-Solano, and Oscar M. Caicedo: *Journal of Internet Services and Applications: A comprehensive survey on machine learning for networking: evolution, applications and research opportunities* (2018)
5. Apostolopoulos, J.: (2019, June 5) Cisco Blogs. *Improving Networks with Artificial Intelligence*. Retrieved from: <https://blogs.cisco.com/networking/improving-networks-with-ai>
6. Kevin Skapinetz. *Overcome cybersecurity limitations with artificial intelligence* [Video file]. Retrieved from: <https://www.ibm.com/security/artificial-intelligence>
7. Orli Gan. "Artificial Intelligence: a Silver Bullet in Cyber Security? CPX 360 Keynote". *YouTube*, uploaded by: Check Point Software Technologies, Ltd. , 21 March 2018 , <https://www.youtube.com/watch?v=ggje-L0ViFM&list=LL&index=3&t=972s>