# O RECURSO E CONTRIBUIÇÃO POTENCIAL DA INTELIGÊNCIA ARTIFICIAL PARA A CIBERSEGURANÇA EM AMBIENTES DIGITAIS


Autor:
Raúl C. Morgado
Doutorando

Orientador:
Luís B. Gouveia
Professor Associado


Universidade Fernando Pessoa
11 de março de 2016
Porto

# AGENDA

- Introdução
- Cibersegurança
- Inteligência Artificial
- Inteligência Artificial na Cibersegurança
- Comentários Finais

# INTRODUÇÃO

Porque é que necessitamos da Inteligência Artificial (IA) na área da cibersegurança?

- ✓ Número de ataques;
- ✓ Elevada frequência de ataques;
- ✓ Grande quantidade de informação para ser processada;
- ✓ Resposta em tempo oportuno;
- ✓ Mais dispositivos digitais;
- ✓ Ameaças mais inteligentes.

# CIBERSEGURANÇA

## O que é cibersegurança?

Conjunto de atividades, técnicas ou não-técnicas, meios e tecnologias que visam proteger computadores, redes de computadores, hardware e software contra danos e intrusão ilícita.

# CIBERSEGURANÇA

## Pilares da Cibersegurança

- Confidencialidade;
- Integridade;
- Disponibilidade.

# CIBERSEGURANÇA

## Principais tipos de ataques

- Negação de Serviço;
- *Malwares*;
- Ataques em redes sociais;
- *Botnets* e *Zombies*;
- *Scarewares*.

# INTELIGÊNCIA ARTIFICIAL

## O que é Inteligência Artificial?

"estudo e construção de entidades artificiais com capacidades cognitivas semelhantes às dos seres humanos".

(Ernesto, 2008)

# INTELIGÊNCIA ARTIFICIAL

**As abordagens para o estudo de IA dividem-se em 4 categorias:**

| | Desempenho Humano | Racionalidade |
|---|---|---|
| Pensamento e raciocínio | Sistemas que pensam como os humanos | Sistemas que pensam racionalmente |
| Comportamento | Sistemas que agem como os humanos | Sistemas que agem racionalmente |

(Russell e Norvig, 2009)

# INTELIGÊNCIA ARTIFICIAL

## Paradigmas da IA

- Biológico (Holland – 1975)
  - ✓ Aplicação da teoria da seleção natural de Darwin e Mendel a problemas complexos (computação evolutiva).
- Computacional (Allen Newell e Herbert Simon – 1976)
  - ✓ "Os Sistemas Físicos de Símbolos têm os meios necessários e suficientes para a ação inteligente geral."
- Conexionista (Rumelhart e McClelland – 1986)
  - ✓ Olha para a inteligência como sendo uma "propriedade emergente das interações de um número elevado de unidades elementares de processamento."

# INTELIGÊNCIA ARTIFICIAL

## Correntes da IA

- Tese da IA forte
  - ✓ É viável o aparecimento de máquinas que são inteligentes.
- Tese da IA fraca
  - ✓ Apenas é possível construir de artefactos que imitam o homem na sua ação inteligente.

# INTELIGÊNCIA ARTIFICIAL

## Escolas de Pensamento (IA Fraca)

- IA Convencional
  - ✓ Inspirada nas ciências sociais, foca-se na observação do comportamento humano individual, representação do conhecimento e em métodos de inferência.
- Inteligência Computacional
  - ✓ Inspirada nos processos naturais e biológicos através da imitação de sistemas biológicos.

# INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

## Métodos mais utilizados:

- Sistema Especialista
  - ✓ Desenvolvimento de um conjunto de regras que analisam a informação sobre um dado problema e recomendam uma modalidade de ação para a sua solução.

- Redes Neuronais
  - ✓ Baseiam-se num processo de aprendizagem de soluções de problemas conhecidos de modo a criar generalizações para posteriormente resolver novos problemas.

# INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

## Métodos mais utilizados:

- Agentes Inteligentes
  - ✓ Entidades computacionais, com caraterísticas muito próprias, que atuam como intermediários com objetivos específicos.
- Sistemas Imunológicos Artificiais
  - ✓ Baseado no funcionamento do sistema imunitário humano.

# INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

Aplicações usando IA mais comuns:

- Planeamento em questões de segurança;
- Deteção de fraudes com cartões de crédito;
- Deteção de *spam* e *worm*;
- Deteção de vírus;
- Sistemas de prevenção de intrusões;
- Sistemas de deteção de intrusões;
- Sistemas de deteção de ataques de negação de serviço;
- Sistemas de classificação de *malware*.

# INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

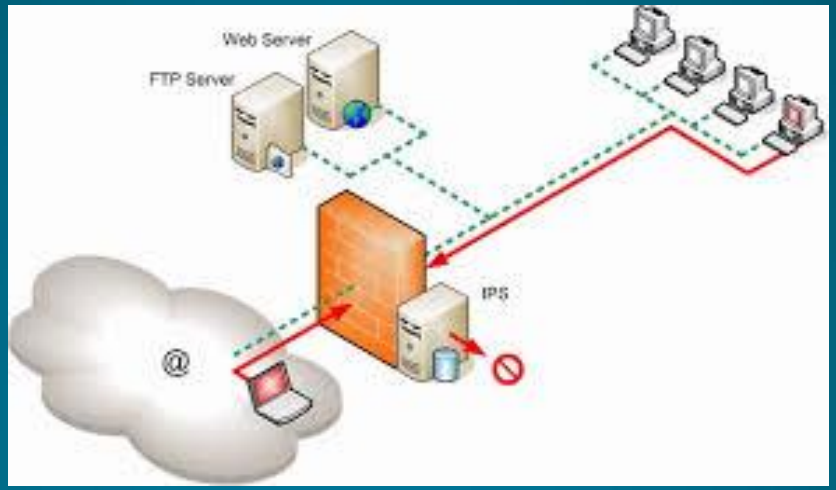
## Exemplos – Deteção de *Spam*

- Como saber se uma mensagem é lixo ou se interessa?

# INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

## Exemplos – Deteção de Intrusões

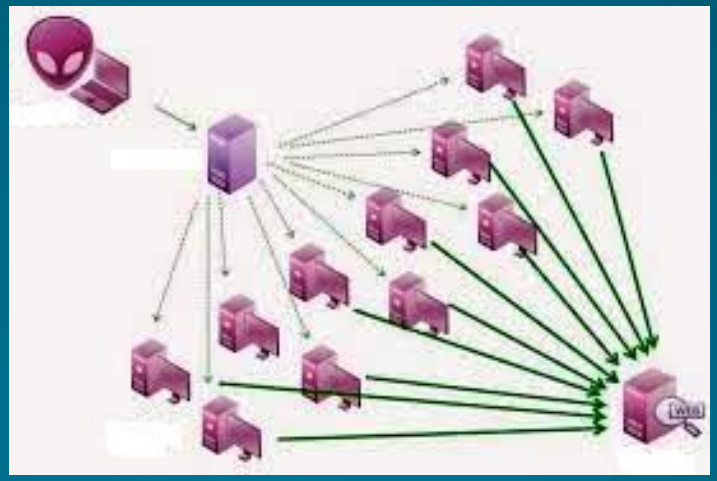
- Como saber se determinado comportamento de utilizadores é suspeito e como lidar com a situação?



# INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

## Exemplos – Deteção de ataques de negação de serviço

- Como saber se determinado sistema está a ser atacado e como solucionar a situação?



# COMENTÁRIOS FINAIS

Vantagens

- Maior segurança e proteção;
- Sistemas com capacidade de adaptação;
- Sistemas com capacidade de aprender e de evoluir.

# COMENTÁRIOS FINAIS

Desafios

- Questões Comerciais;
- Questões Legais;
- Sistemas IA maliciosos.

# REFERÊNCIAS BIBLIOGRÁFICAS


- Costa, H. e Simões, A. (2008). Inteligência Artificial. Fundamentos e Aplicações. FCA – Editora de Informática, 3ª edição;

- Dilek, S.; Çakir, H. and Aydin, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, Nº 1;

- Hurst, J. (w/d). Overview and Tutorial on Artificial Intelligence Systems, SANS Institute;

- Kumbhar, S. (2014). An Overview on Use of Artificial Intelligence Techniques in Effective Security Management", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 9;

# REFERÊNCIAS BIBLIOGRÁFICAS


- Reddy, Y. and Thirupathaiah, A. (2014). Artificial Intelligence in Cyber Defense. International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3, Nº 5;

- Russel, S. and Norvig P. (2009). Artificial Intelligence. A Modern Approach. Prentice-Hall, Inc, 3th edition;

- Tyugu, E. (2011). Artificial Intelligence in Cyber Defense. 3rd International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn;

- Wood, B.; Saydjari, O. and Stavridou, V. (w/d). A Proactive Holistic Approach to Strategic Cyber Defense. Cyber Defense Research Center, Systems Development Laboratory.