

# Javier Carnerero Cano

## Work Experience

- Oct. 2019 – present **Teaching Assistant**, Dept of Computing, Imperial College London. Courses: **Deep Learning**, **Introduction to Machine Learning** and **Mathematics for Machine Learning**.
- May 2018 – present **Machine Learning & Security Research Assistant**, Dept of Computing, Imperial College London.
- Nov. 2017 – Feb. 2018 **Data Engineer**, Area of Big Data & Business Intelligence Solutions, Santander Global Tech.
- Feb. 2016 – Oct. 2017 **RF, Antennas & Passive Sensors Research Assistant**, Dept of Signal Theory & Communications, Universidad Carlos III de Madrid.

## Education

- 2016 – 2017 **MRes in Multimedia and Communications**, Universidad Carlos III de Madrid.
- 2015 – 2017 **MEng in Telecommunications Engineering**, Universidad Carlos III de Madrid.
- 2011 – 2015 **BEng in Telecommunications Engineering**, Universidad Carlos III de Madrid.

## Languages

- Spanish **native**  
English **full professional proficiency**

## R&D Interests

- Machine Learning (ML) & Adversarial ML
- ML for Security
- Bilevel Optimisation & GANs

## Computer Skills

- **OS**: Windows & Linux
- **Prog lang.**: Python, MATLAB, Java & C
- **ML & DL Frameworks**: PyTorch & TensorFlow
- **Databases**: SQL
- **Office suite**: Microsoft Office &  $\text{\LaTeX}$

## Participation in R&D Projects

- May 2018 – present **Evaluating the Robustness of Machine Learning Algorithms in Adversarial Settings**, funded by Defence Science and Technology Laboratory (Dstl), in collaboration with Imperial College London. PI: Prof E. C. Lupu.
- Apr. 2017 – Aug. 2017 **Development of a Multiband Feeder with Autotracking Capability**, funded by Prodetel, S.A., in collaboration with Universidad Carlos III de Madrid. PI: Dr F. J. Herraiz-Martínez.

## Selected Publications

### Conference Papers

- Feb. 2020 **J. Carnerero-Cano**, L. Muñoz-González, P. Spencer, and E. C. Lupu, “Regularisation Can Mitigate Poisoning Attacks: A Novel Analysis Based on Multiobjective Bilevel Optimisation” (under review) [[Link](#)].

- Sep. 2019 L. Muñoz-González, B. Pfitzner, M. Russo, **J. Carnerero-Cano**, and E. C. Lupu, "Poisoning Attacks with Generative Adversarial Nets", in *arXiv preprint arXiv:1906.07773* (under review). [\[Link\]](#).

### Book Chapters

- Dec. 2019 L. Muñoz-González, **J. Carnerero-Cano**, K. T. Co, and E. C. Lupu, "Challenges and Advances in Adversarial Machine Learning", *NATO Science for Peace and Security Series - D: Information and Communication Security*, Vol. 55: Resilience and Hybrid Threats - Security and Integrity for the Digital World, pp. 102–120. IOS Press. [\[Link\]](#).

### Journal Papers

- Apr. 2020 G. Galindo-Romera, **J. Carnerero-Cano**, J. J. Martínez-Martínez, A. Rivera-Lavado, and F. J. Herraiz-Martínez, "A Contactless System for the Dielectric Characterization of Liquid Drops" (under review).
- June 2018 **J. Carnerero-Cano**, G. Galindo-Romera, J. J. Martínez-Martínez, and F. J. Herraiz-Martínez, "A Contactless Dielectric Constant Sensing System Based on a Split-Ring Resonator-Loaded Monopole", *IEEE Sensors Journal*, vol. 18, no. 11, pp. 4491–4502. JCR impact factor: **3.076 - Q1** (2018). [\[Link\]](#).
- Apr. 2017 G. Galindo-Romera, **J. Carnerero-Cano**, J. J. Martínez-Martínez, and F. J. Herraiz-Martínez, "An IoT Reader for Wireless Passive Electromagnetic Sensors", *Sensors*, vol. 17, no. 4, pp. 693–1–693–19. JCR impact factor: **3.031 - Q1** (2018). [\[Link\]](#).

---

## Peer Reviewing

### Conferences and Workshops

- 2019 – present **ACM Workshop on Artificial Intelligence and Security (AISec)**, **Workshop on Machine Learning for Cybersecurity (MLCS)**.

### Journals

- 2019 – present **EURASIP Journal on Information Security**.

---

## Assistance in the Supervision of Students

- 2018 **G. Collinge**, "Analysis of Causative Attacks against Machine Learning Algorithms", MSc in Computing Science, Imperial College London. Master's Thesis supervised by Dr. L. Muñoz-González. **Distinguished Project**.

---

## Awards and Grants

- May 2018 **PhD Scholarship**, Defence Science and Technology Laboratory (Dstl), Ministry of Defence, United Kingdom.
- Mar. 2016 **MEng Research Scholarship**, Dept of Signal Theory & Communications, Universidad Carlos III de Madrid.

---

## Organisations

- 2020 – present **IEEE & IEEE Computer Society**, Student Member.
- 2020 – present **ACM**, Student Member.
- 2019 – present **Imperial College London ACM Student Chapter**, Member.