

# Javier Carnerero Cano

ML & Sec. Researcher and Telecom Engineer

✉ [j\(dot\)cano\(at\)imperial\(dot\)ac\(dot\)uk](mailto:j(dot)cano(at)imperial(dot)ac(dot)uk)

📄 [javiccانو.github.io](https://javiccانو.github.io)

in [linkedin.com/in/ccano-javi](https://linkedin.com/in/ccano-javi)

🐙 [github.com/javiccانو](https://github.com/javiccانو)

## Work Experience

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

## Education

- 2016 – 2017 **MRes in Multimedia and Communications**, Universidad Carlos III de Madrid. [[Link](#)].
- 2015 – 2017 **MEng in Telecommunications Engineering**, Universidad Carlos III de Madrid. [[Link](#)].
- 2011 – 2015 **BEng in Telecommunications Engineering**, Universidad Carlos III de Madrid. [[Link](#)].

## Languages

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

## R&D Interests

- ML, Deep Learning and Adversarial ML
- Data Poisoning, Bilevel Optimization and GANs
- ML for Security

## Computer Skills

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

## 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

### Papers under Review or in Preparation

- (preprint) **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”, in *arXiv preprint arXiv:2003.00040*. [[Link](#)].
- (preprint) 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*. [[Link](#)].

## Book Chapters

- 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

- 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", *Progress In Electromagnetics Research M*, vol. 94, pp. 201–208. [\[Link\]](#).
- 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. [\[Link\]](#).
- 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. [\[Link\]](#).

---

## Peer Reviewing

### Conferences and Workshops

Workshop on Machine Learning for Cybersecurity, ACM Workshop on Artificial Intelligence and Security, Joint Workshop on CPS & IoT Security and Privacy, Neural Information Processing Systems.

### Journals

EURASIP Journal on Information Security, IEEE Transactions on Information Forensics and 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

- 2020 **Best Poster Award**, Machine Learning Summer School, Indonesia.
- 2018 **PhD Scholarship**, Defence Science and Technology Laboratory (Dstl), Ministry of Defence, United Kingdom.
- 2016 **MEng Research Scholarship**, Dept of Signal Theory and Communications, Universidad Carlos III de Madrid.

---

## Organizations

- 2020 – present **IEEE and IEEE Computer Society**, Student Member.
- 2020 – present **ACM**, Student Member.