

José **Jair** Cardoso de **Santanna**

Researcher Principal, Assistant Professor, Threat Intelligence Enthusiast, and Energetic Public Speaker

Contact

Oosterstraat 5
7514DX Enschede
The Netherlands

jairsantanna@gmail.com
+31 6 82508224


Links


/jcsantanna 

/jjsantanna 

/jcsantanna 

/TxcQNxUAAAAJ 

/0...2-8361-6729 

/K-2169-2016 

Languages

Dutch★★★★☆

English★★★★★

Portuguese★★★★★

Mission Statement

I am passionate about leveraging my expertise in the cybercriminal domain and phenomena to create a safer digital world. With advanced skills in big data analysis, a problem-solving mindset, and a can-do attitude, I am dedicated to addressing complex challenges in cybersecurity. My experience collaborating with Law Enforcement and my enthusiasm for using innovative technologies empower me to make meaningful, data-driven contributions to combat cyber-crime effectively.

Relevant mentions

I am currently a Principal Researcher and Innovator at Northwave Security, a Dutch managed security service provider. In this role, I lead small and medium-sized teams in several projects aimed at improving the accuracy and efficiency of processes using data mining, machine learning, and the latest artificial intelligence models & technologies. Three publicly disclosed projects include: (1) automation of phishing email analysis and escalation, (2) adaptive anomaly detection of identity-related attacks, and (3) automation of the analysis of leaked datasets & information from cybercriminals.

In addition to Northwave, I am a one-day-a-week assistant professor at the University of Twente (sponsored by Northwave), where I work to bridge academia and industry while teaching and supervising students. One of my courses is Digital Forensics for Cybercrime,” where I provide (1) in-depth knowledge of cybercriminal activities and emerging cyber threats (e.g., Cybercrime-as-a-Service, ransomware, DDoS attacks, business email compromise, cyber fraud and scams, illicit online marketplaces, among others). The lectures in this course are highly hands-on and designed to provoke critical thinking about investigating the modus operandi of cybercriminals. Students complete three assignments in which I guide them to perform big data analysis using Python, machine learning techniques, and the latest AI large language models to test predefined hypotheses.

Over the last seven years, I have frequently collaborated with the Dutch Police, initially with the Team High Tech Crime and currently with Politie Midden Nederland, focusing on ‘Booters’ — DDoS-as-a-service providers. I conducted my PhD (2013–2017) on investigating the entire Booters ecosystem. My PhD thesis and several publicly available scripts have been used by various law enforcement agencies worldwide during multiple successful *Operation PowerOff* campaigns (2018, 2022, and 2023). I was actively involved in these operations, helping to mine data and providing strategic and actionable advice.

Finally, it is worth mentioning that during the final years of my PhD, I developed (1) the concept of ‘DDoS fingerprints’ to facilitate the attribution, detection, and mitigation of attacks; (2) a database to store these specific fingerprints (called DDoSDB); and (3) several converters for transforming fingerprints into formats compatible with network appliances to mitigate attacks. These three elements formed the foundation of what is known as the DDoS Clearing House,” which has been implemented in several European countries and was selected as a ‘key innovation’ by the European Commission in 2021. In the Netherlands, the DDoS Clearing House serves as a key technical component of the Anti-DDoS-Coalitie, of which I am one of the founding members.

Education

- 2013–2017 **Doctor** in Computer Science University of Twente, The Netherlands
“DDoS-as-a-Service–Investigating Booter Websites”.
Link: https://research.utwente.nl/files/18494043/jjsantanna_thesis.pdf
- 2010–2012 **Master** in Computer Science Federal University of Rio Grande do Sul, Brazil
“A BPM-based Solution for Inter-domain Circuit Management”.
- 2005–2010 **Bachelor** in Computer Engineer Federal University of Pará, Brazil
“A Comparative Evaluation of DCCP Protocol in Mesh Networks.”

Experience

Principal Researcher and Innovator

- 2024–Now **Northwave BV** Utrecht, The Netherlands
Tasks & Responsibilities: (1) Drive the exploration and application of cutting-edge technologies such as Machine Learning, Artificial Intelligence, Cloud Computing, and Quantum Computing to enhance and automate cybersecurity processes; (2) Conceptualize and deploy advanced solutions to address critical challenges, focusing on efficiency, scalability, and resilience; (3) By collaborating with multidisciplinary teams and engaging with stakeholders, I align innovative approaches with organizational goals and industry needs; (4) Lead research initiatives to evaluate emerging technologies, integrate them into cybersecurity frameworks, and share knowledge through thought leadership and mentorship; and (5) Streamline processes and leverage data-driven insights to proactively mitigate threats.

Cloud Security Leader

- 2019–2023 **Northwave BV** Utrecht, The Netherlands
Tasks & Responsibilities: (1) Think strategically and support the development of Cloud Security innovation, and industry experience together with the newest technologies to help clients innovate at scale and transform large businesses; (2) Turn innovative ideas into business differentiation by crafting customized automated Cloud Security solutions; (3) Deliver projects for clients using the latest technology and automation to achieve speed and scale; (4) Collaborate with security colleagues and use technology to innovate and pioneer security solutions to help clients build resilience and social impact; and (5) Interact with confidence with highly positioned stakeholders internal and external, with clients and the ecosystem of technology solutions.

Assistant Professor

- 2017–now **University of Twente** Enschede, The Netherlands
Tasks & Responsibilities: teach, supervise students, lead projects, submit project proposals, review academic papers and journals, and perform own research.
Current Offered Courses: (1) Digital Forensics for Cybercrime; (2) Secure Cloud Computing
Last concluded supervision titles:
 - Automating the Cybersecurity Triage Process using LLMs.
Link: <https://essay.utwente.nl/100966>.
 - Evaluating Large Language Models for Automated Cyber Security Analysis Processes. Link: <https://essay.utwente.nl/100846>

Technical Advisor

2024–2024	To the board of <i>Northwave Cyber Security</i> On: European Artificial Intelligence (AI) act	The Netherlands
2017–now	To the <i>Team High Tech Crime (THTC)</i> police unit On: “DDoS attacks” and “Booters, Stressers, and DDoS-for-hire”	The Netherlands
2019–2019	To <i>Logius</i>, the digital government service of the Netherlands Ministry of the Interior and Kingdom Relations (BZK) Report on: “Assessing Logius’ Quality Peering Platform (KPP) Against DDoS Attacks”	The Netherlands
2019–2019	To the <i>Nationale Beheersorganisatie Internet Providers (NBIP)</i> and the <i>Stichting Internet Domeinregistratie Nederland (SIDN)</i> Report on: “The impact of DDoS attacks on Dutch enterprises.”	The Netherlands
2016–2016	To the Yokohama National University For the production of a report on “Reflection & Amplification DDoS attacks” requested by the <i>Japanese Ministry of Internal Affairs and Communications</i> .	Japan
2016–2016	To the Dutch National Cyber Security Center and the Scientific Research & Documentation Center For the production of a report on “Cyber metrics 2016: DDoS and Malware” requested by the <i>Dutch Ministry of Security and Justice</i> .	The Netherlands

Academic Project/Task Leader

2019–2023*	Cybersecurity Competence for Research and Innovation (CONCORDIA) Funded by: the European Framework Programme for Research and Innovation Responsible to lead from 2019–2020 the pilot DDoS Clearing House with 42 partners.	
2017–2019	Collecting, Transforming, Applying, and Disseminating DDoS Attack Knowledge Funded by: SIDN fonds	
2018–2019	Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands Funded by: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)	

Lecturer

2012–2013	University of Santa Cruz do Sul (UNISC) Tasks & Responsibilities: Supervise students and teach (integrally) the courses: <ul style="list-style-type: none">• Digital Systems;• Computer Networks; and• Network Management.	Santa Cruz do Sul, Brazil
-----------	--	---------------------------

Guest Lecturer

2015–2019	Cybercrime & Cybersecurity (minor) Course: Introduction to Network Forensics	University of Twente, The Netherlands
2016–2019	Network Management Lectures: (1) “SNMPv1, v2, v3 and Beyond” and (2) “Network management based on WebServices”	University of Twente, The Netherlands
2015–2019	Network Security Lecture: “DDoS attacks into the Matrix”	University of Twente, The Netherlands
2015 & 2016	Product Design to Online Business Lectures: (1) “Booters: the DDoS-as-a-Service phenomenon” and (2) “Product Design to Online Business”	University of Twente, The Netherlands

Presentations

**Last 5 public presentations.*

Invited	Revisiting more than a Decade of DDoS Attacks Venue: Anti-DDoS-Coalition plenary	Nov/2024
Invited	The Double-Edged Sword: Risks of AI Language Models Venue: ISACA Risk Event	Nov/2024
Invited	AI in Action: Automating Large-Scale Data Analysis Venue: Europol Cybercrime Conference	Oct/2024
Invited	Training on The EU AI Act Venue: Northwave Cyber Security Conference	Oct/2024
Invited	Using AI LLM for in-depth Dataset Analysis Venue: ONE Conference	Oct/2024

Rewards & Awards

2021	Great EU-funded Innovations	European Union
2018	Best Science Communicator of the Netherlands	FAMELab
2018	Among the top Young Talented Engineers of the Netherlands	Het Koninklijk Instituut Van Ingenieurs