

# ICICN2026 Track 8

## Basic Information:

### 专栏题目 Title

中文：网络欺骗防御：理论、方法与系统  
英文：Cyber Deception Defense: Theory, Methods, and Systems

### 专栏介绍和征稿主题 Introduction and topics

#### 中文：

网络欺骗防御是一类面向主动防御的安全技术与方法，其核心思想是通过构造、伪装、诱导和动态编排等手段，有意识地影响攻击者对网络资产、服务、身份、拓扑和攻击面的感知与判断，从而达到误导、拖延、暴露、溯源、牵制和遏制攻击的目的。与传统以阻断和检测为主的被动防御不同，网络欺骗防御强调在对抗过程中主动塑造攻击者所见的信息环境，使防守方能够在更早阶段发现威胁、获取对手行为情报，并提升整体网络韧性。

随着高级持续性威胁、自动化攻击工具链以及人工智能驱动攻击能力的快速发展，网络欺骗技术正在从单点蜜罐部署，逐步演进为面向复杂网络环境的体系化、动态化与智能化防御机制。其研究内容涉及攻击认知建模、博弈论与决策优化、强化学习与多智能体协同、蜜罐与诱饵系统设计、移动目标防御、威胁情报提取、攻防评测与安全治理等多个方向。

本专题面向网络欺骗防御的前沿理论、关键技术、系统实现与行业应用，旨在汇聚网络安全、人工智能、博弈论、控制与决策、网络与系统、安全运营等领域的研究者与实践者，推动网络欺骗防御在模型、算法、平台和实战应用等层面的深入发展。投稿可涉及理论分析、算法设计、系统实现、原型验证、实验评测以及真实应用案例。

本专题关注但不限于以下研究方向：

1. 网络欺骗防御的概念体系、体系架构与形式化建模。
2. 面向网络欺骗的博弈论方法、序贯决策方法与优化理论。
3. 基于强化学习、多智能体学习与策略演化的智能欺骗防御。
4. 蜜罐、蜜点、蜜标、诱饵身份与伪装服务的设计、部署与协同。
5. 移动目标防御、动态攻击面变换与欺骗资源编排优化。
6. 面向高级持续性威胁的诱捕、拖延、溯源与对手画像分析。
7. 面向云原生、边缘计算、物联网、工业互联网、车联网与数字孪生环境的欺骗防御。
8. 生成式人工智能、大语言模型与自动内容生成在网络欺骗中的应用。
9. 网络欺骗与威胁情报提取、态势感知、安全运营和自动化响应的联动机制。
10. 网络欺骗防御的实验平台、仿真环境、数据集、基准测试与效能评估指标。
11. 攻击者认知建模、反欺骗识别、对抗性适应与鲁棒防御机制。
12. 网络欺骗防御中的可解释性、安全性、隐私保护、伦理与合规问题。

#### 英文：

Cyber deception defense is an active-defense paradigm that intentionally influences an adversary's perception, reasoning, and decision-making by constructing, disguising, and dynamically orchestrating deceptive assets, services, identities, network views, and attack surfaces. Rather than relying solely on passive detection and post-incident response, cyber deception aims to mislead, delay, expose, attribute, constrain, and contain attackers, thereby improving defenders' visibility, increasing adversarial cost, and enhancing overall cyber resilience.


Driven by the rapid evolution of advanced persistent threats, automated attack toolchains, and AI-enabled offensive capabilities, cyber deception is moving beyond isolated honeypots toward integrated, adaptive, and intelligent defense ecosystems. The field now spans a broad spectrum of topics, including adversarial cognition modeling, game-theoretic analysis, sequential decision-making, reinforcement learning, deceptive system design, moving target defense, threat intelligence extraction, security evaluation, and trustworthy deployment.

This special session aims to bring together researchers and practitioners from cybersecurity, artificial intelligence, game theory, control and decision, networking, systems, and security operations to discuss the latest advances in the theories, methods, platforms, and applications of cyber deception defense. Submissions may include theoretical analysis, algorithm design, system development, prototype implementation, empirical evaluation, and practical deployment studies.

Topics of interest include, but are not limited to:

1. Concepts, architectures, and formal models for cyber deception defense.
2. Game-theoretic, sequential decision-making, and optimization methods for deceptive defense.
3. Intelligent deception defense based on reinforcement learning, multi-agent learning, and strategy evolution.
4. Design, deployment, and coordination of honeypots, honeypoints, honeytokens, deceptive identities, and decoy services.
5. Moving target defense, dynamic attack surface mutation, and deception resource orchestration.
6. Luring, delaying, attribution, and adversary profiling against advanced persistent threats.
7. Cyber deception for cloud-native systems, edge computing, Internet of Things, industrial Internet, vehicular networks, and digital twin environments.
8. Applications of generative artificial intelligence, large language models, and automated content generation in cyber deception.
9. Integration of cyber deception with threat intelligence extraction, situational awareness, security operations, and automated response.
10. Testbeds, simulation environments, datasets, benchmarks, and evaluation metrics for cyber deception defense.
11. Adversary cognition modeling, anti-deception detection, adaptive attacks, and robust defense mechanisms.
12. Interpretability, security, privacy, ethics, and compliance issues in cyber deception defense.

## Track Chair(s):

	姓名 <b>Name</b>	谭晶磊 Jinglei Tan
	称谓 <b>Prefix</b>	特聘副研究员
	部门 <b>Department</b>	网络空间安全学院
	单位 <b>Organization</b>	广州大学
	城市/地区 <b>City/Region</b>	广州

## Organizer's Brief Biography

中文:

入选省级高层次青年人才、国家资助博士后研究人员计划、中国新锐科技人物，获国际发明展览会铜奖、省教育厅优秀论文一等奖（序1）、全军军事理论成果三等奖。近五年发表第一/通信作者学术论文30余篇（3篇ESI论文，10篇中科院一区/CCF A期刊）。主持省自然青B、国自然青C、博后面上项目，授权专利/软著9项。担任多个中文高质量科技期刊优秀青年编委和EI国际会议研讨会主席，IEEE TIFS、IEEE TDSC等TOP期刊审稿人，核心期刊专题发起人，受邀在公安部学术研讨会报告。

英文:

Selected as a provincial-level high-level young talent, a national-funded postdoctoral researcher program participant, a Chinese emerging technological figure, won the bronze award at the International Invention Exhibition, the first prize of the Provincial Education Department's excellent thesis (ranked 1st), and the third prize of the military theory achievements of the entire army. In the past five years, published over 30 first/lead author academic papers (3 ESI papers, 10 papers in the first zone of the Chinese Academy of Sciences/CCF A journals). Hosted provincial natural science youth B, national natural science youth C, and postdoctoral face-to-face projects, obtained 9 patents/soft copyrights. Served as an excellent young editor for several high-quality Chinese scientific and technological journals and the chairperson of EI international conferences and seminars, served as a reviewer for TOP journals such as IEEE TIFS and IEEE TDSC, initiated special issues for core journals, and was invited to give a report at the academic symposium of the Ministry of Public Security.

	姓名 <b>Name</b>	蔡肖 Xiao Cai
	称谓 <b>Prefix</b>	副研究员
	部门 <b>Department</b>	网络空间安全学院
	单位 <b>Organization</b>	广州大学
	城市/地区 <b>City/Region</b>	广州

### Organizer's Brief Biography

中文：

近五年申请人发表 SCI 论文 80 余篇，其中第一作者论文 37 篇（含通讯作者 7 篇），中科院一区 TOP 30 篇，覆盖 TIFS、TFS、TC 等旗舰期刊；7 篇入选科睿唯安（ESI）高被引论文，总被引 1000+。申请人入选 2024 年博士后创新人才支持计划 A 类（“博新计划”），主持国家自然科学基金青年项目、广东省自然科学基金面上项目、中国博士后科学基金项目等，申请发明专利 10 余项，获得国际发明展览会铜奖，广东省计算机学会优秀论文一等奖，川渝优秀论文三等奖两项等。申请人也担任多个著名国际期刊审稿人，并担任中科院一区期刊客座编辑。

英文：

Over the past five years, the applicant has published more than 80 SCI papers, including 37 as the first author (7 of which were as the corresponding author). Thirty of these papers appeared in top-tier journals within the Chinese Academy of Sciences (CAS) Zone 1 —including flagship journals such as \*TIFS\*, \*TFS\*, and \*TC\*—and seven were recognized by Clarivate Analytics (ESI) as Highly Cited Papers, accumulating a total citation count exceeding 1,000. The applicant was selected for the 2024 Class A of the Postdoctoral Innovative Talent Support Program (the "Boxin Program") and has led various research projects, including a Young Scientists Fund project under the National Natural Science Foundation of China (NSFC), a General Program under the Natural Science Foundation of Guangdong Province, and a project funded by the China Postdoctoral Science Foundation. Furthermore, the applicant has applied for over 10 invention patents and has received numerous accolades, including a Bronze Medal at an International Invention Exhibition, a First Prize for Outstanding Paper from the Guangdong Computer Society, and two Third Prizes for Outstanding Papers in the Sichuan-Chongqing region. The applicant also serves as a reviewer for several renowned international journals and as a Guest Editor for a CAS Zone 1 journal.

	姓名 <b>Name</b>	张晓彪 Xiaobiao Zhang
	称谓 <b>Prefix</b>	博士
	部门 <b>Department</b>	信息工程学院
	单位 <b>Organization</b>	西北农林科技大学
	城市/地区 <b>City/Region</b>	咸阳杨凌

### Organizer's Brief Biography

中文：

长期从事图像处理、人脸分析和深度学习等领域的研究工作，主要研究的课题包括生理信号提取、目标检测与识别、对抗学习和安全评估等，在相关高水平期刊与国际会议上发表论文 20 余篇，掌握国际研究动态，并建立了一定的国际国内学术交流联系。曾经多次作为科研骨干力量参与过省级和国家级项目，先后参与并完成陕西省科技计划重点产业创新链项目“智能医护协助陪伴机器人”、深圳市科技计划国际合作研究项目“智能养老陪护机器人研究”和国防项目。多项成果发表在 TIM、TCSVT、SPL、PRL 等国际期刊。曾被西北工业大学研究生院报道，链接如下：  
<https://mp.weixin.qq.com/s/qJNmSVN7VBnZCpRbWO6woA>。

英文：

Long-term engagement in research in the fields of image processing, face analysis, and deep learning, with primary focus

on physiological signal extraction, object detection and recognition, adversarial learning, and security evaluation. More than 20 papers have been published in high-level journals and international conferences, demonstrating familiarity with global research trends and establishing academic collaborations both domestically and internationally. Served as a key research member in multiple provincial- and national-level projects, including the Shaanxi Provincial Key Industry Innovation Chain Project “Intelligent Medical Assistance and Companion Robot,” the Shenzhen Science and Technology Program International Cooperation Project “Research on Intelligent Elderly Care Companion Robots,” as well as national defense projects. Several research results have been published in prestigious international journals such as TIM, TCSVT, SPL, and PRL. Featured by the Graduate School of Northwestern Polytechnical University.