

Research Topics & Ideas: Cybersecurity

About this document

This PDF contains 50 **cybersecurity research topics** for dissertations and theses, organized into 10 areas of cybersecurity, from adversarial machine learning and AI security to trustworthy systems and secure computation. Each topic is written as a researchable question and linked to a completed dissertation (2022–2026, 21 universities), so you can see how it was studied in practice. Use it to shortlist cybersecurity dissertation topics and thesis ideas, then narrow one down to your own population, setting and timeframe.

By [Derek Jansen](#) (MBA) · Reviewed by [Eunice Rautenbach](#) (DTech) · Grad Coach · October 2026

Online version: gradcoach.com/research-topics-cybersecurity/

© 2026 Grad Coach. Free to share and adapt under [CC BY 4.0](#) with credit to Grad Coach and a link to gradcoach.com/research-topics-cybersecurity/. Research questions and thesis titles quoted here remain their authors'; each dissertation keeps its own license.

Contents

Adversarial machine learning and AI security · 5 topics	2
Critical infrastructure and cyber warfare · 5 topics	2
Cryptography and secure implementations · 5 topics	3
Hardware, embedded and device security · 5 topics	3
Malware and threat detection · 5 topics	3
Network security and intrusion detection · 5 topics	4
Phishing, fraud and identity · 5 topics	4
Privacy and data protection · 5 topics	5
Security governance, policy and workforce · 5 topics	5
Trustworthy systems and secure computation · 5 topics	6
How to turn a topic into your research question	7

Adversarial machine learning and AI security

1. Which adversarial attacks still work on a large language model that has been aligned?

See it in a real dissertation: [Large Language Model's Vulnerabilities Under Adversarial Attacks](#) · Gwonwoo Lee · Purdue University · 2026

2. How does a deep network fail once it leaves the benchmark it was tested on?

See it in a real dissertation: [Identifying and Mitigating Vulnerabilities of Deep Neural Networks in the Wild](#) · Hui Li · University of Chicago · 2023

3. Could a signal classifier be made robust without losing the accuracy it was built for?

See it in a real dissertation: [Adversarial Robustness in Signal Classification Through Vector Quantized Information Bottleneck](#) · Attanasia Garuso · Rowan University · 2026

4. Should a security team trust a model whose decisions nobody can interpret?

See it in a real dissertation: [Interpretation and Robustness of Black-Box ML Models for Secure Cyber Space](#) · Qudrat E Alahy Ratul · Boise State University · 2024

5. How much compute does privacy cost when several parties train one network together?

See it in a real dissertation: [Privacy-Preserving and Resource-Efficient Learning Frameworks for Collaborative Deep Neural Networks](#) · Shiwei Ding · Michigan Technological University · 2026

Critical infrastructure and cyber warfare

6. How ready is a power utility for ransomware, measured rather than self-reported?

See it in a real dissertation: [Adopting Critical Power Grid Infrastructure Technologies: An Organizational Cybersecurity Assessment against Ransomware](#) · Fayez Alsoubaie · Portland State University · 2026

7. Can overlapping cybersecurity standards be reconciled automatically rather than by committee?

See it in a real dissertation: [A Neuro-symbolic Semantic Analysis Approach to the Harmonization of Cybersecurity Standards in the Energy Domain](#) · Schroeder, William · Purdue University · 2025

8. How did the internet become a place where states fight one another?

See it in a real dissertation: [The Origins of Cyber Warfare: How the Internet Became Weaponized](#) · Ada Sonia Peter Nee Obanua · Harvard University · 2024

9. How does a state claim sovereignty over a domain it cannot physically hold?

See it in a real dissertation: [Virtually inconceivable: Geopolitics, capacity, and sovereignty claims in the digital domain](#) · Carver, Julia · University of Oxford · 2025

10. What regulation actually changes a firm's security spending rather than its paperwork?

See it in a real dissertation: [Strategic incentives and regulation in cyber security](#) · Manos Perdikakis · University of Oxford · 2025

Cryptography and secure implementations

11. How much leakage does an encrypted database give up through the queries run against it?

See it in a real dissertation: [A Combinatorial Approach to Leakage Abuse Attacks and Their Mitigation](#) · Francesca Marie Falzon · University of Chicago · 2023

12. What can an attacker infer from order-preserving encryption, and can that be closed off?

See it in a real dissertation: [Improving Security of Order-Preserving Encryption and Its Applications in Data Outsourcing](#) · Shen Ning · Boise State University · 2023

13. Could a quantum scheme lease out a decryption key and reliably take it back?

See it in a real dissertation: [Collusion-Resistant Quantum Key Leasing](#) · Nikhil Pappu · Portland State University · 2026

14. Does the charging-line side channel on a smartphone survive an attempt to reproduce it?

See it in a real dissertation: [Reproducing and Evaluating Charger Surfing: Robustness of Smartphone Charging-Line Side-Channels](#) · Colby M Watts · California Polytechnic State University · 2026

15. What does an attacker gain by trading memory for time against a cryptographic primitive?

See it in a real dissertation: [Time-Space Trade-Offs in Cryptographic Primitives](#) · Akshima · University of Chicago · 2022

Hardware, embedded and device security

16. How would you detect a trojan in a sensor your organization did not manufacture?

See it in a real dissertation: [Trojans in Wireless Sensor Networks](#) · Maryamsadat Jalalitabar · Georgia State University · 2022

17. What would a computer look like if it were designed to make a backdoor impossible?

See it in a real dissertation: [A Solder-Defined Computer Architecture for Backdoor and Malware Resistance](#) · Marc W. Abel · Wright State University · 2023

18. Which countermeasures against power side channels introduce vulnerabilities of their own?

See it in a real dissertation: [Systematic Characterization of Power Side Channel Attacks for Residual and Added Vulnerabilities](#) · Aurelien T Mozipo · Portland State University · 2023

19. Will a vehicle ever run its own intrusion detection on the hardware already inside it?

See it in a real dissertation: [Lightweight FPGA-based machine learning models for vehicle security](#) · Auangkun Rangsikunpum · Loughborough University · 2026

20. How much location privacy can an app give a user that the platform underneath does not?

See it in a real dissertation: [Achieving Location Privacy in iOS Platform Using Location Privacy Framework](#) · Anna Systaliuk · San Jose State University · 2022

Malware and threat detection

21. How do you find malware that exists only in memory, on a platform the usual tools cannot image?

See it in a real dissertation: [Malware and Memory Forensics on M1 Macs](#) · Charles A. Glass · Louisiana State University · 2022

22. How fast does an Android malware classifier go stale, and can it notice on its own?

See it in a real dissertation: [Concept Drift Detection in Android Malware](#) · Inderpreet Singh · San Jose State University · 2023

23. Can you tell an attack from ordinary administration when both use the same built-in binaries?

See it in a real dissertation: [Common Pattern Generation for the Detection of LOLBin Attacks](#) · Alaa AbuShqeir · San Jose State University · 2023

24. Can a small language model run a useful penetration test on consumer hardware?

See it in a real dissertation: [Comparing PPO and GRPO for Automated Penetration Testing with Compact Language Models on Consumer-Grade Hardware](#) · Junhao Dong · Purdue University · 2026

25. What does internet-wide scanning tell a defender that their own logs cannot?

See it in a real dissertation: [Internet-wide Threat Intelligence and Enterprise Lateral Movement Detection](#) · Joseph Khoury · Louisiana State University · 2025

Network security and intrusion detection

26. Is zero trust network access measurably safer than a VPN, or only newer?

See it in a real dissertation: [Zero Trust Network Access vs. Traditional VPNs: A Comparative Analysis of Security Posture and Performance in Hybrid Network Environments](#) · Anurag Choudary Putti · Purdue University · 2026

27. Can a detector trained on known attacks classify one it has never seen on a medical device?

See it in a real dissertation: [Evaluating Machine Learning Models on Classification of Novel Cyber Attacks in the Healthcare Domain](#) · Promise Ehimen · Minnesota State University Moorhead · 2026

28. Can synthetic network traffic stand in for the real thing when the real thing cannot be shared?

See it in a real dissertation: [Generative Modeling for Packet-Level Network Traffic Synthesis](#) · Xi Jiang · University of Chicago · 2026

29. What forensic trace does an attack on a software-defined control plane leave behind?

See it in a real dissertation: [Software-Defined Networking Security Techniques and the Digital Forensics of the SDN Control Plane](#) · Abdullah Alshaya · Louisiana State University · 2023

30. Can an agent learn to defend a network by repeatedly attacking itself?

See it in a real dissertation: [Autonomous Network Defence Using Multi-Agent Reinforcement Learning and Self-Play](#) · Roberto G. Campbell · San Jose State University · 2022

Phishing, fraud and identity

31. Will a phishing detector's explanation ever be good enough for an analyst to act on?

See it in a real dissertation: [From Feature-Enhanced Url Phishing Detection to Explainable Multi-Agent Email Phishing Detection Using Large Language Models](#) · Tanya Yadav · San Jose State University · 2026

32. Which nudge actually stops someone tapping a link in a text message?

See it in a real dissertation: [Exploring Automatic and Reflective Nudges for Smishing](#) · Morgan E. Edwards · Old Dominion University · 2026

33. What should an organization do in the hour after a phishing email is detected?

See it in a real dissertation: [Developing a Framework to Improve Phishing Response After Detection](#) · Kevin Umba · Marquette University · 2026

34. Can anomalies in a voter registration file be told apart from ordinary data entry error?

See it in a real dissertation: [Leveraging Machine Learning and Deep Learning Techniques for Voter Registration Fraud Detection](#) · Nahid Anwar · Boise State University · 2025

35. Is the way you move a mouse distinctive enough to authenticate you?

See it in a real dissertation: [ML-Based User Authentication Through Mouse Dynamics](#) · Sai Kiran Davuluri · San Jose State University · 2023

Privacy and data protection

36. Does a differentially private system leak through how long it takes to answer?

See it in a real dissertation: [Foundations of Differential Privacy Against Timing Attacks](#) · Zachary Ben Ratliff · Harvard University · 2026

37. Do people judge the same data collection differently in a room and on a screen?

See it in a real dissertation: [Context Matters: Privacy Perceptions and Data Sharing Behaviors Across Physical and Virtual Environments](#) · Beatrice Li · University of Virginia · 2026

38. Why do students say they care about privacy and then hand it over anyway?

See it in a real dissertation: [Examining the Privacy Paradox Among Undergraduate Students](#) · Karen Elizabeth Bumbaugh · Purdue University · 2026

39. How would you estimate what a system gives away when you cannot model it exactly?

See it in a real dissertation: [A general framework of estimating information leakage for privacy and forensics problems with imperfect statistical information](#) · Shahnewaz Karim Sakib · Iowa State University · 2023

40. What does a privacy-preserving pipeline cost a language model in accuracy?

See it in a real dissertation: [Privacy preserving methods for Natural Language Processing](#) · Plant, Richard · Edinburgh Napier University · 2025

Security governance, policy and workforce

41. Which cybersecurity model actually fits a school district with no budget for one?

See it in a real dissertation: [A Comparative Analysis of Models of Cybersecurity in Louisiana Public School Systems](#) · Bonnie Chelette · Louisiana State University · 2023

42. Do staff-facing policies say the same thing across the campuses of one university?

See it in a real dissertation: [Selected California State University Cybersecurity Readiness Policies and Related Guidance for Staff](#) · Andrew Hung-Nguyen · San Jose State University · 2026

43. What would actually close the cybersecurity workforce gap, and who has to move first?

See it in a real dissertation: [Strengthening the U.S. Cybersecurity Workforce: A Strategic Collaboration of the U.S. Government, Academia, and Private Sector](#) · Chelene Reyes Yardumian · Harvard University · 2026

44. Does the way cybersecurity education is delivered explain who ends up in the field?

See it in a real dissertation: [Cybersecurity education praxis and broadening participation in cybersecurity: Pieces of the same puzzle.](#) · Cynthia Thomas · University of Louisville · 2024

45. How should an organization govern the risk of an AI system it did not build?

See it in a real dissertation: [Navigating AI's Security and Risk Management Maze: Using the CRSPi Framework and Platform to Strengthen AI Resilience](#) · David Haddad · Purdue University · 2026

Trustworthy systems and secure computation

46. Where are the real gaps in a software supply chain, as opposed to the ones tools check?

See it in a real dissertation: [Identifying Gaps in Software Supply Chain Security Systems Using the AStRA Model](#) · Eman Abdul-Muhd Abu Ishgair · Purdue University · 2026

47. Does a multiparty computation stay fair when one participant walks away halfway through?

See it in a real dissertation: [Secure Multiparty Protocols on Blockchain with Fairness and Scalability](#) · Joshua Holmes · Boise State University · 2024

48. How do you let a voter spoil a ballot without making the choice traceable?

See it in a real dissertation: [Toward Privacy-Preserving Electronic Voting with Ballot-Spoiling Using Blockchain](#) · Yoonsu Ra · Boise State University · 2023

49. Could a person carry a device that defends their privacy from the sensors around them?

See it in a real dissertation: [Machine-Augmented Humans As a Privacy Armor](#) · Yuxin Chen · University of Chicago · 2022

50. Which privacy attacks become practical only once the attacker has a model to work with?

See it in a real dissertation: [Identifying and Mitigating AI-Enhanced Privacy Attacks](#) · Zhuolin Yang · University of Chicago · 2025

How to turn a topic into your research question

A topic is a starting point, not something you can research yet. These four steps take you from a topic on this list to a focused question you can actually answer.

- 1. Shortlist three, not one.** Pick three topics from this list that genuinely interest you and fit the access you have to people and data.

Recommended reading: [How to find and choose a dissertation topic](#)

- 2. Read the dissertation behind each one.** Its literature review and its "recommendations for future research" section show you what is already known and what is still open.

Recommended reading: [How to find a research gap](#)

- 3. Narrow it to your setting.** Name one population, one setting and one thing you will measure or explore. That turns a broad topic into a question you can finish.

Recommended reading: [How to write a research question](#)

- 4. Line up your aims, objectives and questions.** Your committee will check that they agree.

Recommended reading: [Research aims, objectives and questions](#)

Work through these once and you will have a focused question rather than a broad topic, which is what the rest of your proposal is built on.