

Cybersecurity and International Conflict, Minor

The Minor in Cybersecurity and International Conflict

Audrey Kurth Cronin, *Director, and Trustees Professor of Security and Technology*
 acronin (acronin@andrew.cmu.edu)@andrew.cmu.edu
 (acronin@andrew.cmu.edu), Posner Hall 385A

Emily Half, *Deputy Director for Academic Affairs*
 ehalf@andrew.cmu.edu, Posner Hall 391, 412-268-7082

<https://www.cmu.edu/cmist/>

Overview

Sponsored by the Carnegie Mellon Institute for Strategy and Technology (CMIST) (<https://www.cmu.edu/cmist/>), the minor in cybersecurity and international conflict focuses on the existing gaps in our understanding of cybersecurity and international conflict. The minor exposes students to basic technology concepts, methods of attack and defense, potential strategy and goals for cyber-engagement, and response and forensics for cyber-engagements.

Alongside conventional methods of warfare, cybersecurity has rapidly developed into a centerpiece of a state's ability to protect and project power. In the shifting landscape of cyber capabilities, how will laws, authorities, and policies keep pace? What are the implications and consequences of actions that may be considered "short of war" by some countries but "above the threshold" of conflict by others? Will a more aggressive defensive posture with respect to cybersecurity inadvertently increase the risk of conflict with states that sponsor malicious hacking groups? What is the proper balance between offense and defense in cybersecurity and how are cyber operations best integrated into a country's overall military strategy?

Unlike some other kinds of tactics, attribution of cyber attacks presents significant challenges. If the aggressor's identity cannot be quickly confirmed, how can a counterattack be launched? Some attackers may seek to mount "false flag" attacks and deception, for example, that misdirect defenders to counter-attack in the wrong direction. What are the appropriate rules of engagement for attacks on national systems, infrastructural systems, businesses, and individuals? When, for example, is a counterattack or a "kinetic" response permissible?

These questions have major implications for the study of war and peace. Those who seek to start a war may be harder to find and their motives more difficult to discern. The cybersecurity and international conflict minor tackles the social-scientific dimensions of cybersecurity with a focus on the implications of the cyber age for modern statecraft, warfare, elections (local, state, and national), and domestic and international politics.

Curriculum

Students are permitted to double count a maximum of two courses between the minor in Cybersecurity and International Conflict and another major or minor. Unlimited double counting is permitted with general education requirements.

Minor in Cybersecurity and International Conflict 63 units

Foundational Course 9 units

Students must take one of the following foundational courses:

	Units
84-101 Introduction to Political Science	9
84-104 Decision Processes in American Political Institutions	9
84-226 International Relations	9
84-275 Comparative Politics	9

Core Courses 27 units

Students must take all of the following core courses:

84-363 Click. Hack. Rule: Understanding the Power & Peril of Cyber Conflict	9
---	---

84-387 Remote Systems and the Cyber Domain in Conflict	9
84-405 The Future of Warfare	9

Elective Courses 27 units

Students must take three courses from the following list of elective courses (27 units). At least one course (9 units) must be taken from the Carnegie Mellon Institute for Strategy & Technology (CMIST) and have an 84-number:

84-110 The Economics of Politics and Technology	9
84-200 Security War Game Simulation	3
84-274 An Introduction to Technology and War	9
84-280 Popcorn and Politics: American Foreign Policy at the Movies	12
84-304 Analysis of Current US National Security Priorities	6
84-312 Terrorism in Sub-Saharan Africa	6
84-314 Politics, Technological Change, and Economic Growth	9
84-319 Civil-Military Relations	9
84-323 War and Peace in the Contemporary Middle East	9
84-325 Contemporary American Foreign Policy	9
84-328 Military Strategy and Doctrine	9
84-329 Asian Strategies	6
84-330 Race for the Future: US-China Tech Competition	6
84-331 Technology, Law, and Democracy	6
84-341 Transnational Criminal Networks & International Security	6
84-343 Offensive Cyber: Law & Policy	6
84-345 Hackers, the Law, & Policy Responses	6
84-347 Congress & National Security	9
84-349 Digital Diplomacy: Cybersecurity Challenges and Global Governance	9
84-350 A Strategist's Introduction to Artificial Intelligence	9
84-353 US-China Strategic Stability	6
84-356 Applied Political Data Analytics	9
84-365 The Politics of Fake News and Misinformation	9
84-368 Technology Ethics	9
84-370 Nuclear Security & Arms Control	9
84-371 International Governance of Artificial Intelligence	9
84-373 International Law	9
84-375 Geopolitics of Innovation	9
84-380 US Grand Strategy	9
84-383 National Cyber Policy & Strategy	6
84-386 The Privatization of Force	9
84-389 Terrorism and Insurgency	9
16-735 Ethics and Robotics	12
17-200 Ethics and Policy Issues in Computing	9
17-303 Cryptocurrencies, Blockchains and Applications	Var.
17-331 Information Security, Privacy and Policy in the Age of AI	12
17-333 Privacy Policy, Law, and Technology	9
17-334 Usable Privacy and Security	9
17-702 Current Topics in Privacy Seminar	3
79-302 Killer Robots? The Ethics, Law, and Politics of Drones and A.I. in War	9
80-249 AI, Society, and Humanity	9
95-444 Cybersecurity Policy and Governance II	6