**BHA-Cybersecurity & International Conflict**  
**Bachelor of Humanities and Arts (BHA)**

<table>
<thead>
<tr>
<th>Dietrich College (DC) Concentration in Cybersecurity &amp; International Conflict</th>
<th>81 units (minimum)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advisor:</strong> Emily Half, Posner Hall 391, 412-268-7082, <a href="mailto:ehalf@andrew.cmu.edu">ehalf@andrew.cmu.edu</a></td>
<td></td>
</tr>
</tbody>
</table>

The BHA concentration in cybersecurity and international conflict analyzes the past, present, and future role of cyber conflict and cybersecurity in international politics. Cyber attacks by nation-states and their proxies have an important impact upon conflict. The complexity and policy challenges of cyber-engagements is immense. This minor addresses the role of deterrence, dissuasion, and attribution in cyber conflict, while also studying the nuances of key components of modern warfare—from the security dilemma to escalation management.

Courses in this minor focus on the existing gaps in our understanding of cybersecurity and international conflict, such as whether cyberspace is offense or defense dominant (or over time fluid between the two), and which factors are important in determining the answer to this. Other relevant questions include how nation-states, their primary adversaries, and a bevy of nonstate actors engage online and in the virtual and information environments. Accordingly, 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 project power. As the United States and other emerging cyber powers craft and implement doctrine in this domain, there is likely to be a rapid increase in activity, from efforts to disrupt the online activities of global terrorist networks, to cybersecurity offense and defense in the Russia-Ukraine war, to near daily raids on foreign networks designed to cripple states’ cyberweapons before they can be deployed. In addition, the impact of cyberattacks on critical infrastructure, theft of intellectual property, pervasive identity theft, and hacking of sensitive databases have accumulated, gradually wearing down civilian networks and achieving strategic effects over time.

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 other kinds of conflicts, attribution of attacks presents significant challenges. Indeed, in many cases, it can be difficult to determine whether the attacker is a nation-state, a nonstate actor, a criminal gang, or a lone hacktivist. Investigators must combine technical and traditional methods to identify potentially responsible parties and to understand their intent. If the aggressor’s identity cannot be 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.

Additionally, what are appropriate responses to attacks made on civil infrastructure and private business operations, such as in the areas of financial services, transportation, energy, entertainment, and health care? In other words, what are the appropriate rules of engagement for 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.

BHA students take at least 9 courses in their DC concentration, for a minimum of 81 units. A completed DC Concentration Declaration Sheet must be approved by the concentration advisor and submitted to the BXA office by spring mid-semester break of the student’s sophomore year. BHA students who are admitted through internal transfer must have chosen a DC concentration at the time of their application, which serves as declaration.

**Foundational Courses**

(2 courses, 18 units)

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>84-104</td>
<td>Decision Processes in American Political Institutions</td>
</tr>
<tr>
<td>84-226</td>
<td>International Relations</td>
</tr>
<tr>
<td>84-275</td>
<td>Comparative Politics</td>
</tr>
</tbody>
</table>

**Core Courses**

(3 courses, 24 units)

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>84-387</td>
<td>Remote Systems and the Cyber Domain in Conflict</td>
</tr>
<tr>
<td>84-388</td>
<td>Concepts of War and Cyber War</td>
</tr>
<tr>
<td>84-405</td>
<td>The Future of Warfare</td>
</tr>
</tbody>
</table>

**Electives**

(4-5 courses, 39 units minimum)

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>84-200</td>
<td>Security War Game Simulation</td>
</tr>
<tr>
<td>84-312</td>
<td>Terrorism in Sub-Saharan Africa</td>
</tr>
</tbody>
</table>

At least two courses (18 units) must be taken from CMIST and have an 84-number.
BHA-Cybersecurity & International Conflict  
Fall 2023

84-319  Civil-Military Relations  9
84-323  War and Peace in the Contemporary Middle East  9
84-325  Contemporary American Foreign Policy  9
84-327  Repression and Control in Dictatorships  9
84-328  Military Strategy and Doctrine  9
84-329  Asian Strategies  6
84-365  The Politics of Fake News and Misinformation  9
84-370  Nuclear Security & Arms Control  9
84-372  Space and National Security  9
84-373  Emerging Technologies and International Law  9
84-374  Technology, Weapons, and International Conflict  9
84-380  US Grand Strategy  9
84-383  Cyber Policy as National Policy  6
84-386  The Privatization of Force  9
84-389  Terrorism and Insurgency  9
84-390  Social Media, Technology, and Conflict  9
16-735  Ethics and Robotics  12
17-200  Ethics and Policy Issues in Computing  9
17-303  Cryptocurrencies, Blockchains and Applications  9
17-331  Information Security, Privacy, and Policy  12
17-333  Privacy Policy, Law, and Technology  9
17-334  Usable Privacy and Security  9
17-702  Current Topics in Privacy Seminar  3
79-301  History of Surveillance: From the Plantation to Data Capitalism  6
80-249  AI, Society, and Humanity  9
95-444  Cybersecurity Policy and Governance  12