CYBER CASE:\STUDY

CALL FOR ABSTRACTS

SPONSORED BY:

AIR FORCE RESEARCH LABORATORY

TA PÁNTA REÎ · AIR FORCE CYBER COLLEGE

MGMWERX

CALL FOR ABSTRACTS

Funding to eligible participants for completed cyber case studies

The Air Force Cyber College announces a call for abstracts for teaching cases on topics related to Cyber Strategy, Policy, and Leadership. Teaching cases or table-top exercises identify dilemmas, or lead students to do so. In contrast to traditional academic cases studies, teaching cases do not "solve problems" in the text of the case – they enable active learning for students to work them out.

Successful abstract entrants will be invited to work on their draft cyber teaching case in the Air Force Cyber College Cyber Case Study Workshop – three (3) sessions of eight (8) hours held in November 2021. Cyber College will review and award eligible participants for cases successfully completed by November 23, 2021. Successful finished case studies will earn $500; a total of $2,000 will be paid for the Most Important case study, $1,500 for one Extremely Important case study, and $1,250 for one Important case study. Case studies will be published by the Air Force Cyber College Case Study Program. Unclassified cases will be published online on the AFCC Case Study page.

DEADLINE: TUESDAY, OCT 12, 2021

HOW TO APPLY:

1. Review the Call for Abstracts

2. Prepare your abstract

3. Attach a curriculum vitae for all case study authors

4. Email your proposal and curriculum vitae to:
AWC.cybercollege.org@us.af.mil

TOPICS OF INTEREST

- Cyber Strategy & Policy
- Deep Fakes
- Artificial Intelligence
- Digital Propaganda
- Trick Bots
- Agency and Inter-agency coordination
- Law of War in Cyberspace

Please see the full Call for Abstracts for more specific information on topics.

FUNDING:

Selected case study authors will be compensated.

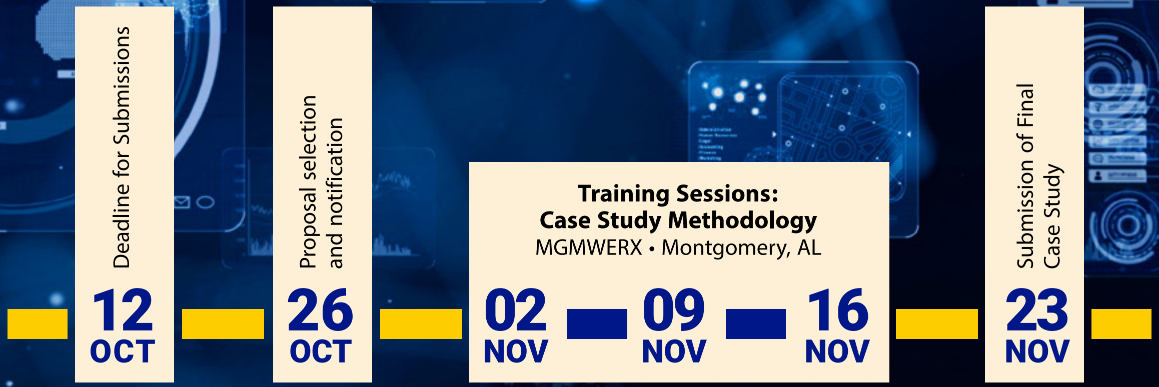
$500 for completing a case study accepted by Air Force Cyber College

$1250 for one (1) Important Case

$1500 for one (1) Extremely Important Case

$2000 for the Most Important Case

Please see Call for Abstracts for specific details on case study judgment criteria.



Deadline for Submissions
12 OCT

Proposal selection and notification
26 OCT

Training Sessions:
Case Study Methodology
MGMWERX • Montgomery, AL
02 NOV — 09 NOV — 16 NOV

Submission of Final Case Study
23 NOV

CYBER CASE:\STUDY
CALL FOR ABSTRACTS

SPONSORED BY:

CYBER CASE STUDY PROJECT: CALL FOR ABSTRACTS

Funding to eligible participants for completed cyber case studies

The Air Force Cyber College announces a call for abstracts for teaching cases on topics related to Cyber Strategy, Policy, and Leadership. Teaching cases or table-top exercises identify dilemmas, or lead students to do so. In contrast to traditional academic cases studies, teaching cases do not "solve problems" in the text of the case – they enable active learning for students to work them out.

Successful abstract entrants will be invited to work on their draft cyber teaching case in the Air Force Cyber College Cyber Case Study Workshop – three (3) sessions of eight (8) hours held in November 2021. Abstracts are due by **October 12, 2021.** Cyber College will review and award eligible participants for cases successfully completed by **November 23, 2021.**[1] Successful finished case studies will earn $500; a total of $2,000 will be paid for the Most Important case study, $1,500 for one Extremely Important case study, and $1,250 for one Important case study. Case studies will be published by the Air Force Cyber College Case Study Program. Unclassified cases will be published online on the AFCC Case Study page.

Proposals are especially welcome for, but not limited to, the following specific topics:

- Any cyber strategy or policy topic that incorporates quantitative risk estimation and/or analysis especially associated with military missions
- Protecting senior leaders (and perhaps the entire force) from the reputational damage of Deep Fakes
- Coordination among allies with different rules for cyberwarfare
- Artificial intelligence – what are the leadership knowledge, skills, and abilities needed for leading organizations composed of humans and autonomous AI systems? What will need to change for humans to be led by autonomous AI systems?
- Artificial intelligence – what legal, ethical, and organizational issues arise in military use of AI
- Deterring Chinese lawfare in Hong Kong, the Nine-dash region, and elsewhere
- Digital propaganda and influence operations, including dilemmas of authorities and ethics
- Trick Bot and military-industry factors in response to cyber-attack
- Dilemmas of Department of Defense reliance on commercial off the shelf technology
- Agency authorities and interagency coordination in cyber operations
- Defense/reconstruction of critical infrastructure in countries in and beyond US borders
- The Law of War in cyberspace; exploring the competing visions of what constitutes a cyber-attack under international law

The primary objective of this call is to solicit abstracts for the development of case studies that provide teaching tools for instructors at the graduate level, especially those teaching in professional military education (PME) institutions or civilian graduate programs in peace and security studies with a focus on cyber security. Case studies that provide practice in the application of strategy, policy, or leadership concepts to scenarios involving cyber dilemmas will prove invaluable in helping to prepare students to grapple with complex real-world cyber issues.

DEADLINE: Abstracts will be accepted until **October 12, 2021.** We will announce successful submissions by **October 26, 2021.**

HOW TO APPLY

1. **Review the Call for Abstracts**

2. **Prepare your abstract.** The abstract should be no longer than one page and be written in English. The proposal should include the following elements and not exceed 300 words:

   i. Case title
   ii. Corresponding author and affiliation, including email address and telephone number
   iii. Name(s) of co-authors, if applicable with affiliations, email addresses, and telephone numbers

[Continued on next page]

[1] US Government personnel, please consult your organization for rules regarding payment – work completed on government time and/or equipment cannot be paid twice by the government.

- iv. Abstract detailing the story and dilemma(s) illustrated by the case
- v. Key cyber strategy, policy, or leadership issues illustrated by the case

3. **Attach a curriculum vitae for all case study authors**

4. **Email your proposal and curriculum vitae to: AWC.cybercollege.org@us.af.mil.**

PROPOSAL SELECTION

Abstracts will be selected from the submitted proposals based on the following selection criteria: (a) Relevance of the topic, (b) the appropriateness of the topic, problems, dilemma(s) and concepts for inclusion in a graduate cyber curriculum, and (c) the academic and professional qualifications of the authors.

TIMELINE

1. **October 12, 2021:** Deadline for submission of proposals

2. **October 26, 2021:** Proposal selection and notification

3. **November 2, 9, & 16, 2021:** Training, through active participation during all three sessions, on the case study methodology. The objective of the online/in-person training sessions is to provide in-depth instruction on the methodology and process of developing successful case studies. Sessions will be conducted in-person at MGMWERx in Montgomery, Alabama, and live online access will be available for those unable to attend in-person. As part of the training, participants will develop and present a detailed outline for their case including teaching notes and learning objectives. Case study authors will be expected to produce a publishable case study following completion of training (see timeline). All case manuscripts are subject to editorial and peer review. **Only those manuscripts that meet all publication criteria by the deadlines indicated below are eligible for remuneration.**

4. **November 23, 2021:** Submission of the final version of the case study

FUNDING

Selected case study authors will be compensated. The structure of the compensation will be as follows:

1. $500 for completing a case study accepted by Air Force Cyber College or compensation as listed below

2. A total of $2,000 will be paid for the Most Important case study, $1,500 for one Extremely Important case study, and $1,250 for one Important case study. Importance will be judged by a three-member faculty panel based on: (1) usefulness of the case study in a graduate cyber policy and strategy curriculum and (2) quality of the completed case study.