



## Writing Competition for Cyber Conflict Case Studies

**The Project:** The Armed Forces Communications and Electronics Association is partnering with the Cyber Conflict Studies Association (CCSA) and the Atlantic Council for a competition for case studies in the history of cyber conflict. There are a total of six possible prizes of up to \$1000 each for the best submissions. If determined to be of sufficient quality, winning studies will also be published in an upcoming journal or book. Additionally, winners will be automatically considered for internship or employment at the Atlantic Council or CCSA.

**The Importance of Cyber History:** Former Deputy Secretary of Defense William Lynn emphasized the importance of developing a “cyber cadre” for national defense. In other areas of national security, one way newly hired people learn the field is through the experience of those that have gone before. Understanding history is the main way to turn the experience of past generations into cumulative knowledge for the future, which is why we teach military officers the implications of Gettysburg, Inchon, Trafalgar or MIG Alley. Even though major conflicts have occurred in cyberspace since the mid-1980s, these events are largely unknown and untaught; making it far more likely we will continue repeating the same mistakes. This cyber conflict history writing competition will mine cyber conflict history to develop this experience and create a narrative of “cyber mindedness” to connect past, present and future cyber cadres.

**Deadline:** Papers are due by midnight (EST), June 1, 2012.

**Eligibility:** The contest has three categories. Each will have separate prizes, and authors must specify which they are applying for when submitting their paper:

1. University students (full- or part-time undergraduate or graduate)
2. Military (active or reserve)
3. Professional (not university or military)

**Prizes:** Each of the above categories will have a prize amount of:

**First place: \$1,000      Second place: \$500**

In addition to the core prizes, **an additional \$500 prize** has been established for international applicants, including students, military, or professionals, to encourage additional perspectives and participation. Please contact the project manager with any questions of eligibility.

Case studies of particular quality may be considered for publication in future CCSA journals, an upcoming *Comprehensive History of Cyber Conflict*, or selected for presentation at a future cyber conflict history conference. Professors are encouraged to allow papers to be used for course credit.

**Notification:** Winners will be notified in writing no later than July 20, 2012.



## Paper Requirements

Papers must be between 7,500 and 8,500 words in length, double-spaced, and typed with a 12-point font. To ensure anonymity of the author during judging, the document must not include the author's name on any page. Each page of the submission must show the exact title of the paper as the header.

**Evaluation Criteria:** Submissions will be evaluated based on originality, strength of argument and recommendations, adherence to the norms of spelling, grammar, and syntax, and clarity.

- **Originality:** Has the author identified and defined the central issue? Is this issue of major importance to the intelligence community or of major concern to users of intelligence? Has the author revisited a known issue and proposed a new approach or solution, or has the author defined an issue or approach from a new perspective? **Weight: 35 Percent**
- **Research and Analysis:** Has the author done original research, such as interviews or use of primary material, to bolster their paper? Are the facts and opinions from this research analyzed to make a coherent case on how and why this incident is historically relevant? **Weight: 35 Percent**
- **Clarity:** Is the author's product clearly presented and well organized? Is the issue clearly described and documented with the recommendations and proposed outcomes precisely laid out? Is the writing clear and lucid? **Weight: 20 Percent**
- **Spelling, Grammar, and Syntax:** Has the author prepared a grammatically correct and properly edited entry? **Weight: 10 Percent**

**Judging Process:** Submissions will be divided into two rounds of evaluation: a panel developed by CCSA will judge the first round, and cyber professionals from the AFCEA Cyber Committee will judge the second, making the final selection. Entries will be judged without knowledge of the author's identity.

**Important Dates:** Participants should email [the project manager](#) (contact info listed below) by April 15, 2012 with your name, choice of case study, and eligibility (student, military or professional participant). If an author would like to cover a case study not listed here or to change topics after April 15<sup>th</sup>, they should contact the project manager. Final papers are due by midnight EST on June 1, 2012.

**Additional Information:** Authors are welcome and encouraged to coauthor papers, however prize money will be split equally amongst the participants. Authors may also submit more than one paper for the contest and potential publication. Appropriate graphics or illustrations are permissible, but not required. Graphics may be embedded in the entry or a placeholder inserted to mark the location of the graphic. In either case, please email the graphic (photos or illustration in JPEG format; others (table/spreadsheet) in native format) to the project manager as a separate attachment to enable proper viewing and formatting for possible publication. Image sources must be properly identified.



## Case Studies

Participants may choose from the case studies below:

- Russian Patriot Hacking, such as during NATO's operation ALLIED FORCE (1999)
- Chinese Patriot Hacking, such as after the NATO bombing of the Chinese Embassy in Belgrade (1999), the Hainan Island Incident (2001), and in reaction to the 2010 Nobel Peace Prize
- Other Patriot Hacking: Indian and Pakistani (1999-2001) or Israeli and Palestinian (1999-2001)
- Evolution of U.S. Use of Cyber Power: DESERT STORM (1990), ALLIED FORCE (1999), Global War on Terrorism (2001-), UNIFIED PROTECTOR (2011)
- Espionage, such as TITAN RAIN, DIB intrusions (2000s-present), Espionage into German, French and Canadian ministries (2007-)
- Cuckoo's Egg (~1986)
- Morris Worm (1988)
- ELIGIBLE RECEIVER (1997)
- SOLAR SUNRISE (1998)
- MOONLIGHT MAZE (1999)
- Cyber conflict in Estonia (2007)
- Cyber conflict in Georgia (2008)
- Operation Buckshot Yankee (2008)

As each of these studies is an important incident in cyber conflict history, the best written case study for each topic will be considered for publication, regardless of whether it has won a prize. In the event that your paper is selected for publication or presentation, CCSA will ask that you submit a signed release form certifying that the submitted paper is original to you, the author, and that the submitted paper is previously unpublished.

## About Us

**About CCSA:** Founded in 2003 by cyber war theorists and practitioners from military, the US Intelligence Community, the White House, and academia, CCSA is a non-profit entity organized to promote and lead a diversified research and intellectual development agenda to advance the field of cyber conflict.

**About AFCEA:** Established in 1946, the Armed Forces Communications and Electronics Association (AFCEA) is a non-profit membership association serving the military, government, industry, and academia as an ethical forum for advancing professional knowledge and relationships in the fields of communications, IT, intelligence, and global security.

**About Atlantic Council:** The *Atlantic Council* has been Washington, DC's leading think tank for transatlantic and NATO national security issues for fifty years, and its new Brent Scowcroft Center on International Security will continue to extend this legacy. The Cyber Statecraft Initiative extends this focus to better understand conflict, cooperation, and competition in cyberspace.

## To Contact Us

Participants with any questions should contact the project manager, Karl Grindal, at [karl@cyberconflict.org](mailto:karl@cyberconflict.org)