



# The Cyber 9/12 Student Challenge

## Competition Instructions for Written Submission

The Cyber 9/12 Student Challenge requires student teams to respond to a simulated cyber incident that escalates and evolves over the course of the competition. Competition teams will write a cyber policy brief and have the opportunity to deliver an oral presentation to a panel of expert judges. The final score of the Qualifying Round will be determined by combining the score of a written cyber policy brief submitted before the competition and the score from an oral presentation based on the prepared cyber policy brief.

For the brief and presentation, teams must produce policy response options that respond, counteract, mitigate, and/or disrupt the damage and continued threat of the current cyberattack. When planning responses, teams should keep in mind that policy response alternatives should go beyond purely technical solutions, and may include legal, political, and diplomatic response alternatives. Teams should consider a variety of offensive and defensive response alternatives that take into account the roles of state, private sector, and international actors. In particular, teams should consider the role of cooperation between different actors necessary to achieve desired policy outcomes.

### **Written Policy Brief (maximum five single-sided pages)**

Your team must prepare a detailed written document that analyzes the implications of the cyber attack for various actors (such as government agencies, private sector stakeholders, and average citizens) and its relation to national cybersecurity policy. Each team must propose policy response options that address the cyber attack and briefly discuss the advantages and disadvantages associated with each policy response alternative. The competition is not meant to test a team's ability to spot issues, but rather to analyze and explain the reasons supporting the best cyber policy recommendation.

There are no format restrictions on font, size, margins, or style, but teams will be graded on professionalism of the presentation. Graphs, images, tables, and other graphics are permitted, but count towards the five single-sided page limit. Submissions that exceed the maximum page will be penalized.





**Decision Document** (template provided)

Teams will also be required to submit a “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision document” will be a prepared form, two single-sided pages (one double-sided page) in length, outlining the team’s policy response alternatives, decision process, and recommendations. This document will allow the judges to familiarize themselves with the proposed policy responses in an efficient manner.

The following outline is strongly suggested for structuring the prepared policy brief.

I. Cyber Policy Question Presented

Identify and clearly explain the cyber policy question facing the European leaders called to address the evolving cyber crisis.

II. Proposed Policy Response Alternatives

Identify and clearly explain the policy response options that the team has formulated to answer the cyber policy question facing the European leaders. It may be helpful for teams to clearly list their alternatives (E.g., Alternative 1, Alternative 2, Alternative 3).

III. Analysis and Impact of Policy Response Alternatives

Analyze the strengths, weaknesses, opportunities, and threats of each of the policy response alternatives. Each policy response alternative should describe the purpose of the proposed policy action, the expected outcomes, and the theoretical justification.

IV. Justification for Recommended Policy Response Alternative

Select one policy response alternative to recommend to European leaders. Compare and contrast the selected alternative and provide an explanation that justifies your selection.

Teams will have until **12:00 pm EST, April 15, 2015** to submit their written cyber policy brief via e-mail to competition directors:

KTothovaJordan@atlanticcouncil.org **and** a.cederberg@gcsp.ch

Late submission will be penalized.

