The Cyber 9/12 Strategy Challenge

Description and Rules

Updated March 4, 2025

Competition Mission

The Cyber 9/12 Strategy Challenge is designed to offer students, across a wide range of academic disciplines, a better understanding of the policy challenges associated with cyber conflict. Part interactive learning experience and part competitive scenario exercise, the Cyber 9/12 Strategy Challenge gives students interested in cyber conflict and policy an opportunity to interact with expert mentors, judges, and cyber professionals while developing valuable skills in policy analysis and presentation.

Student teams will be challenged to respond to an evolving scenario involving a major cyber-attack and analyze the threat it poses to state, military, and private sector interests. Teams will be judged based on the quality of their policy responses, their decision-making processes, and their oral presentation to a panel of judges. Along the way, teams will work with coaches at their home institution to develop their policy skills and receive feedback from expert panels of judges to ensure that all participants have the opportunity to improve their skills, as well as networking opportunities during the competition.

Importance of the Rules

All participants must be familiar with the rules before participating in the event. Teams will be evaluated based on a combination of written and oral tasks, in which a thorough understanding of the rules is important to succeed.

Competition Contact

For any questions about the competition, please contact the staff at the Geneva Centre for Security Policy responsible for the Geneva Cyber 9/12 Strategy Challenge.

Mr Gazmend Huskaj, Competition Director, Head of Cyber Security,
Geneva Centre for Security Policy, g.huskaj@gcsp.ch

Ms Alice Jorda, Competition Coordinator,
Geneva Centre for Security Policy, cyber-competition@gcsp.ch / a.jorda@gcsp.ch

Competition Rules

Rule 1. Format

The Cyber 9/12 Strategy Challenge consists of a cyber-incident scenario that evolves over the course of the exercise, prompting teams to modify their policy priorities and recommendations as part of successive oral presentations.

Qualifying Round — REPORT
Before the competition, teams will write a brief exploring and analyzing the key issues and implications related to the cyber incident described in the scenario materials. The length of the brief is limited to 500 words. Further detailed instructions, can be found in the document "Written Brief Instructions," which will accompany Intelligence Report I.

The qualifying round, held on day one, consists of 10-minute oral presentations, followed by 10 minutes to answer direct questions from a panel of judges. At the end of the round, teams will receive feedback from the judges who will score students based on their oral presentations. The judges' score on the oral presentation will be combined with the team score from the written brief submitted in advance of the competition (see Rule 7 below). Scores from the Qualifying Round will not carry over to the Semi-Final Round.

Semi-Final Round — RESPOND
The semi-final round, held in the morning on Day Two, will give advancing teams the opportunity to respond to a new intelligence report that alters the original scenario. Teams will receive the new intelligence report when advancing teams are announced at the conclusion of Day One. The semi-final round consists of one 10-minute oral presentation, followed by 10 minutes to answer direct questions from a panel of judges. Teams will have only little time to prepare and modify their policy priorities and recommendations. Advancing teams to the Final will be decided based on the judges' score on the oral presentation.

Final Round — REACT
The final round, held in the afternoon of Day Two, will involve a spontaneous reaction to an intelligence report that further alters the original scenario. Teams will have to respond to questions from the panel of judges with only little preparation, testing their ability to analyze information as a team and synthesize a response on the spot. Judges will deliver a final evaluation, and winners will be selected based on the final round scores.

Rule 2. Registration

To be considered for the competition, interested teams must submit all registration materials and all team information by the registration deadline. After all registration materials have been received, teams selected to compete will receive invitations and competition materials. Teams registering late may be considered at the discretion of the Competition Director, space permitting.

Rule 3. Eligibility

All students currently enrolled in an undergraduate, graduate, doctoral, professional, or law program on the date of the registration deadline are eligible to compete. There is no explicit major, coursework, or prior experience in cyber security necessary to compete, but successful applicants will have a strong link between cyber security and policy and their current academic interest.

Students with an interest in cyber security and policy from around the world are invited to apply to compete. However, the Cyber 9/12 Strategy Challenge cannot guarantee any funds to support any potential team expenses. Applicants are encouraged to inquire about funding from their home institutions.

Rule 4. Team Composition

Each team must include four students. Teams that register with less than four competitors may be considered at the discretion of the Competition Director, space permitting. There are no requirements for team composition based on the majors or education level of team members. Each team must also recruit a faculty member to act as their team coach and mentor. Whilst coaches are not required to take part in the competition event, their participation is necessary to ensure that all teams have support in crafting their responses.

Rule 5. Team Selection and Notification

Teams will be selected based on registration materials submitted in accordance with Rule 3. Selected teams will be notified via e-mail of their invitation to the competition. Teams selected to participate will complete a supplementary information packet in advance of the competition.

Rule 6. Pre-competition Preparation

Background information on the competition scenario for the Qualifying Round will be distributed before the competition. This information will be distributed to all teams after participants have completed registration and selected teams have been notified. For the Qualifying Round of the Competition (see Rule 7), teams will prepare both a written and oral policy brief based on a response to the first Intelligence Report. The oral policy brief will be presented at the competition as part of the Qualifying Round and must be accompanied by a "decision document" handed to the judges at the beginning of the competition round (see Rule 8 below).

Rule 7. The Scenario Exercise

The competition will focus on a single cyber incident scenario described through three intelligence reports, one for each round. The exercise encompasses tasks, both written and oral, that challenge students to respond to the political, economic, and security challenges created by the evolving cyber incident scenario. At all stages of the competition, scenario information and tasks will be distributed in a manner that ensures all teams have an equal chance to prepare.

Rule 8. Structure

Qualifying Round

Teams will be provided with a detailed scenario background packet that sets the scene for the fictional cyber incident scenario. Below are the tasks which will need to be completed for the qualifying rounds.

- *Written Cyber Policy Brief*
    - Two weeks before the competition, teams will submit a policy brief exploring the challenges faced by different actors related to the cyber incident described in the scenario materials. The brief is limited to 500 words in length.

- *Oral Cyber Policy Brief*
    - Teams will be given 10 minutes to present their response, followed by 10 minutes to answer direct questions from a panel of judges.

- *Decision Document*
    - 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 maximum of one single-sided page in length, outlining the team's policy response alternatives, decision process, and recommendations.

Semi-Final Round

After the advancing teams are announced, participants will receive the second intelligence report. This intelligence report will describe some change in, or escalation of, the original scenario and entail new problems for the actors involved.

- *Oral Cyber Policy Brief*
    - Teams will be given 10 minutes to present their response regarding further changes to their policy recommendations, followed by 10 minutes to answer direct questions from a panel of judges.

- *Decision Document*
    - Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the semi-final competition round. The "decision document" will be a maximum of one single-sided page in length, outlining the team's policy response alternatives, decision process and recommendations.

Final Round

After the advancing teams are announced, participants will receive the final intelligence report detailing further changes to the scenario and will be provided with a very short amount of time to use the new information to revise their policy responses.

- *Oral Cyber Policy Brief*
    - One at a time, each team will meet with a panel of judges. The teams will present a 10-minute presentation of their reaction regarding further changes to the scenario and their policy recommendations, followed by 10 minutes to answer direct questions from a panel of judges.

Rule 9. Permissible Assistance and Cheating

9.1. Before the competition, teams are encouraged to seek outside help to develop their policy briefs. Teams are expected to rely on their coaches, in particular to help develop and revise their policy ideas for the competition.

9.2. During the competition, NO OUTSIDE ASSISTANCE IS ALLOWED FOR TEAMS. Teams may confer with their coach ONLY and only during the breaks between rounds.

9.3. During the competition rounds, teams are not permitted any outside assistance. Teams are also not allowed to use electronic devices, apart from the device they are using for video teleconferencing during a digital competition. However, teams may use electronic devices such as cellular phones and computers during the breaks between rounds. Paper notes are highly encouraged at all times during the competition.

9.4. Cheating during the competition will not be tolerated and will result in the immediate disqualification of a team. All teams are expected to comply by the rigorous standards of academic honesty in place at their home institutions. Any team suspected of cheating may be subject to immediate disqualification. The home institutions of disqualified teams will also be notified of the disqualification. For clarification, the use of outside assistance during the competition – except from a team coach – is not permitted and will be considered cheating.

Rule 10. Judges

Each round of the competition will be judged by a panel of cyber policy experts. To standardize scoring and encourage consensus, all judges will score the teams based on a common grading scorecard in accordance with Rule 13. Judges may vary between sessions and rounds subject to their availability.

Rule 11. Observers, Media, and Broadcasting

11.1. During the digital event this year teams and external observers will not be able to observe other rounds they themselves are not competing in. However, side events during the two days will be provided for all team members and coaches to engage in. All participants and observers in the event are expected to conduct themselves in a responsible and professional manner.

11.2. Coaches will be allowed to attend their team's presentations but must remain silent. Any sign that coaches are assisting their team during a presentation may lead to disqualification.

11.3. The Cyber 9/12 Strategy Challenge reserves the right to partner with the media to provide live coverage of the event via broadcast or internet livestream. Additionally, members of the press may be present to cover the event. Every effort will be taken to ensure that they do not disturb or assist any of the participating teams in the competition.

Rule 12. Timekeeping

Competition staff will manage a clock to keep track of time limits for the presentations. Teams will be kept advised of the time using a "green-yellow-red" system of cards. At the five-minute mark a staff member will display a green card to the team; at the one-minute mark a staff member will display a yellow card; and at the expiration of time, a staff member will display a red card. A penalty will be assessed for teams exceeding the time limit.

Rule 13. Team Evaluation and Scoring

All teams will be evaluated based on five main dimensions of their responses: *understanding of cyber policy; identification of key issues; policy response option - analysis and selected option; structure and communication; and originality and creativity*. These dimensions will be scored based on a common grading scorecard and instructions shared by all the judges. The resulting numerical scores will be used to determine the winners of each round.

At the conclusion of each round, teams will be provided specific, detailed feedback on strengths and areas of improvement for their policy and presentation skills.

Rule 14. Elimination

In the event a team is eliminated, all teams are welcome and encouraged to take part in the networking functions, speeches, and other events accompanying the challenge across the two dates. Please note that eliminated teams are still eligible for some of the prizes and awards to be offered (see Rule 15).

Rule 15. Prizes and Awards

In addition to the main prize of the competition, the Cyber 9/12 Strategy Challenge will, at its discretion, award additional prizes for outstanding achievement during the course of the competition. The categories of prizes to be offered will be announced before the date of the competition. Teams will also be eligible for awards based on their final standing in the competition.

Rule 16. Notification of Rule Changes

The above rules are provided for planning purposes only. The Cyber 9/12 Strategy Challenge reserves the right to alter the rules based on logistical and technical considerations. In the event of changes to the competition rules, a new version of this document will be posted and distributed to teams before the start of the competition. All participants must be familiar with the rules before participating in the competition. As teams will be evaluated based on a combination of written and oral tasks, a thorough understanding of the rules is important to success.