Cyber 9/12 Strategy Challenge

Description and Rules

Updated 6 January 2019

Contents

Competition Mission

The Cyber 9/12 Strategy Challenge is designed to offer students from across a wide range of academic disciplines, a better understanding of the strategy and policy challenges associated with cyber conflict and incident. Part interactive learning experience and part competitive scenario exercise, the Cyber 9/12 Strategy Challenge gives students interested in cyber conflict, strategy 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-incident and analyse the risks it poses to national, 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 skills to a panel of judges. Ultimately this is an opportunity to develop research, analysis and communication skills that will be applicable well beyond the scope of this event. Feedback from those expert judges will also ensure that all participants have an opportunity to improve and develop their skills, as well as to take advantage of networking opportunities during the competition.

Importance of the Rules

All participants must be familiar with the rules before participating in the event. A thorough understanding of the rules and requirements is important to success.

Competition Contact

For any questions about the competition, please contact the Cyber 9/12 team through the Competition Director, Pete Cooper (pcooper@atlanticcouncil.org) or Safa Shahwan (SShahwan@Atlanticcouncil.org)

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 strategy priorities and recommendations as part of successive oral presentations.

Qualifying Round — REPORT

Before the formal stage of the competition, teams will be provided with a package of scenario materials that describe the background to a potential evolving cyber incident. Teams will then be expected to analyse the material and undertake any necessary supporting research in order to prepare a written brief no longer than 500 words exploring and analysing the key issues and implications. Further detailed instructions on the audience and content of the brief can be at Rule 8 ‘Outputs’, which also details the date prior to the event for submission of this brief.

The qualifying round, held on day one, consists of oral presentations of no longer than 10 minutes outlining the findings included in the written brief. This will be followed by 10 minutes of questions to the team from a panel of judges. You will wish to consider in advance how as a team you manage those questions. You will also be required to deliver a decision document that outlines three potential policy options including a recommendation for one of those along with a summary of the rationale behind that recommendation. At the conclusion 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 and on the basis of those scores, teams will advance into the next 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 new intelligence material that develops the information on the original cyber incident. This material will be provided to advancing teams at the conclusion of day one to allow for consideration overnight. The semi-final round consists of one 10 minute oral presentation updating the analysis of the situation and recommended policy responses accompanied by a written decision document, followed by 10 minutes to answer questions from the panel of judges. Teams which will advance to the final will be decided based on the judges' score on the oral presentation and the response to questions.

Final Round — REACT

The final round, held in the afternoon on day two, will involve a spontaneous reaction to intelligence material that further develops the scenario. Teams will have to respond to questions from the panel of judges with only little preparation, testing their ability to analyse information as a team and synthesise a response on the spot. Organisation will be key. Judges will deliver a final evaluation, and winners will be selected based on the final round scores.

A summary of the required outputs is at Rule 8.

Rule 2. Registration

To be considered for the competition, interested teams must submit all registration materials, including 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

For the UK competition, all students currently enrolled full time at a UK University who have not yet entered full-time employment by the date of the registration deadline are eligible to compete. There is no explicit major, coursework, or prior experience in cyber strategy necessary to compete, but successful applicants will have a strong link between cyber strategy / policy and their current academic interest. The Cyber 9/12 Strategy Challenge cannot support team travel or accommodation expenses. Applicants are encouraged to inquire about funding from their home institutions.

Rule 4. Team Composition

Each team can include a maximum of four students. Teams that register less than four competitors may be considered at the discretion of the Competition Director. There are no requirements for team composition based on the academic discipline or education level of team members. Each team must also recruit a faculty member to act as their team coach and mentor. While coaches are not required to take part in the competition event, their participation is necessary to ensure that all teams have access to assistance in developing

their responses. If teams are struggling to find a coach, in extremis, it may be possible for one to be found for them and they should contact the competition Director.

Rule 5. 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 scenario exercise, teams will prepare both written and oral policy briefs based on a response to the initial scenario intelligence material. The written policy brief will be due prior to the competition event. 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. Teams are also required to find a faculty member to serve as coach who can help review and develop student policy briefs.

Rule 6. 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.

Rule 7. The Scenario Exercise

The competition will focus on an evolving cyber incident scenario described through various packs each of which contains a number of inserts. The exercise encompasses tasks, both written and oral, that challenge students to respond to the political, economic, and security problems created by the evolving 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. Outputs

The following outputs will be expected from teams during the competition.

Qualifying Round

Teams will be provided with a detailed scenario pack ('Pack 1') that sets the scene for the evolving cyber incident. From this, teams will have three tasks to prepare before the competition event.

Written Cyber Policy Brief

Teams will write a 500-word brief exploring and analysing the key issues and implications related to the cyber incident described in the scenario materials. This written policy brief discusses the key elements and national security concerns and shows your ability to summarize the scenario. Importantly it gives space to explain the reasons and confidence levels behind your analysis of the key issues and implications of the ongoing cyber incident. When thinking about this task, imagine that a senior within Govt. / Industry had spoken to your team asking; "What's going on and what should I be concerned about?". This written brief is to be no more than 500 words across 2 pages of A4, the use of graphics or diagrams is down to team choice. This will need to be submitted to SShawan@atlanticcouncil.org and JWatson@atlanticcouncil.org **by 2359 on Monday 28th Jan.**

Oral Cyber Policy Brief

Teams will be given 10 minutes to present their analysis of the situation and three potential strategy / policy options, one of which must be put forwards as the favoured option along with rationale. After this presentation, there will be 10

minutes for judges to ask questions to the teams about their analysis and selected option.

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” a maximum of two single-sided pages (one double-sided page) in length, outlining the team’s three policy response alternatives, decision process, and recommendation.

Semi-Final Round

After the advancing teams are announced at the end of Day 1, participants will receive further intelligence material. This material will describe some change in the original scenario and entail new problems for the actors involved. Advancing teams will be required to prepare the following.

Oral Cyber Policy Brief

Teams will be given 10 minutes to present their analysis of the situation and three potential strategy / policy options, one of which must be put forwards as the favoured option along with rationale. After this presentation, there will be 10 minutes for judges to ask questions to the teams about their analysis and selected option.

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 two single-sided pages (one double-sided page) in length, outlining the team’s decision process and recommendations.

Final Round

After the advancing teams are announced, participants will receive the final intelligence material updating 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

Each team will present to a senior panel of judges and deliver a 10-minute presentation of their reaction regarding further changes to the scenario and their strategy recommendations. This will be followed by 10 minutes to answer direct questions from the panel of judges. Due to the compressed timescale, note that a decision document is not required and that generation of 3 distinct strategy / policy options is not expected.

Rule 9. Permissible Assistance and Cheating

Before the competition, teams are encouraged to seek assistance 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.

During competition events, when teams are presenting or answering judge questions, no outside assistance is allowed. However, teams may confer with their coaches during the breaks between rounds and stages.

No presentation aids of any kind (e.g., PowerPoint, props, and posters) are permitted during the oral briefing.

Teams will not be allowed to use electronic devices such as mobile phones and computers during the competition events, when teams are presenting or answering judge questions.

However, teams may use electronic devices such as mobile phones and computers during the breaks between rounds.

Cheating during the competition will not be tolerated and will result in the immediate disqualification of a team. All teams are expected to comply with 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.

Rule 10. Judges

Each round of the competition will be judged by a panel of cyber strategy and policy experts. To standardise 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

A limited number of observers may be present at the event. Every effort will be taken to ensure that they do not disturb or assist any of the participating teams in the competition. The Cyber 9/12 Strategy Challenge reserves the right to use photos and video from the event to support and promote competition aims. Any participant who wishes not to be photographed is to bring this to the attention of the competition Director who will take appropriate measures. In addition, members of the press may be present to cover the event in person. All participants in the event and observers in the event are expected to conduct themselves in a responsible and professional manner.

Rule 12. Timekeeping

Competition staff will manage a tight schedule 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 at which point all presenting must finish. A penalty will be considered for teams exceeding / ignoring the time limit.

Rule 13. Team Evaluation and Scoring

All teams will be evaluated based on three main dimensions of their responses: evaluation of the scenario problem; analysis of strategy and policy response options presented; and quality of writing or oral presentation. 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. Grading scorecards and guidelines will be distributed to all teams in advance of the competition.

Rule 14. Elimination

In the event a team is eliminated, they are invited to participate in the rest of the competition as observers. Eliminated or not, all teams are welcome and encouraged to take part in the networking events, listen to keynotes and participate in other events accompanying the competition which will be announced on arrival. Specifically, for those teams not making it through to the Semi-Final, there will be a bespoke coaching session during the morning of day 2 at the top of BT Tower given by respected industry seniors. Please also note that eliminated teams are still eligible for some of the prizes and awards to be offered.

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 at the start of the competition. Teams will also be eligible for awards based on their final standing in the competition and all teams will receive certificates in commemoration of their participation.

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.