The Cyber 9/12 Strategy Challenge
South Africa Regional Competition
Description and Rules

Updated September 2, 2021

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 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 feedback from expert panels of judges will ensure that all participants have an 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. Because teams will be evaluated based on a combination of written and oral tasks, a thorough understanding of the rules is important to success.

Competition Contact

For any questions about the competition, please contact the staff at the Atlantic Council's Cyber Statecraft Initiative or at the Cybersecurity Capacity Centre for Southern Africa (C3SA).

Ms. Safa Shahwan Edwards, Deputy Director, Cyber Statecraft Initiative,
SShahwan@AtlanticCouncil.org

Ms. Nthabiseng Pule, Project Coordinator and Outreach Manager, C3SA,
nthabiseng.pule@uct.ac.za

Competition Rules

Rule 1. Format

The Cyber 9/12 Strategy Challenge consists of a cyber-attack 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. Further detailed instructions, including page length and word count limits, can be found in the document "Written Brief Instructions," which will accompany Intelligence Report I. Intelligence Report I will be provided to teams approximately three weeks before the competition.

Semi-Final Round — RESPOND
The semi-final 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 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 (see Rule 7 below).

Final Round — REACT
The final round, held on day two, will give 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 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 less than 24 hours to prepare and modify their policy priorities and recommendations following day one. Further detailed instructions can be found in the document "Written Brief Instructions," which will accompany Intelligence Report II.

Final Round judges will deliver a final evaluation, and winners will be selected based on their cumulative scores, i.e. teams will be scores holistically and based on the results achieved from the written brief, and presentations

Rule 2. Registration

To be considered for the competition, interested teams must submit all registration materials 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 cybersecurity necessary to compete, but successful applicants will have a strong link between cyber conflict policy and their current academic interest.

Students with an interest in cyber conflict and policy from across South Africa are invited to apply to compete. The 2021 South Africa Cyber 9/12 competition will be held 100% virtually.

Rule 4. Team Composition

Each team must be composed of three or four students. 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. 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 crafting their responses.

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 and Semi-final Rounds of the scenario exercise (see Rule 7), teams will prepare both written and oral policy briefs based on a response to the initial scenario intelligence report. The written policy brief will be due approximately one week prior to the competition. The oral policy brief will be presented at the competition as part of the Semi-final 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 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. Teams selected to participate will complete a supplementary information packet in advance of the competition.

Rule 7. The Scenario Exercise

The competition will focus on a single cyber-attack scenario described through various intelligence reports. The exercise encompasses tasks, both written and oral, that challenge students to respond to the political, economic, and security challenges created by the evolving cyberattack 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

The competition will focus on a single cyber-attack scenario described through various intelligence reports. The exercise encompasses tasks, both written and oral, that challenge students to respond to the political, economic, and security problems. Further detailed instructions can be found in the document "Written Brief Instructions," which will accompany each intelligence report.

Qualifying Round

Prior to the competition, competitors will receive Intelligence Report I and will have approximately two weeks to complete and submit a written cyber policy brief.

- *Written Cyber Policy Brief*

- Teams will write a policy brief exploring the challenges faced by state, military, and industry actors related to the cyber incident described in the scenario materials. The brief must also recommend appropriate actions and policy responses for the actors involved. The page length and word count limits of the brief can be found in the "Written Brief Instructions" accompanying Intelligence Report I.

Semi-Final Round

On day one of the competition, will deliver an oral cyber policy brief and decision document in response to Intelligence Report I.

- *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 prepared form, a maximum of one single-sided page in length, outlining the team's decision process and recommendations.

Final Round
At the end of day one, teams will receive the final intelligence report detailing further changes to the scenario and will work overnight to use the new information to revise their policy responses.

- *Oral Cyber Policy Brief*
  - The teams will present a 10-minute presentation of their reaction regarding further changes to the scenario and their policy recommendations, followed by to 10 minutes of questions from the 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 prepared form, a maximum of one single-sided page in length, outlining the team's decision process and recommendations.

Rule 9. Permissible Assistance and Cheating

Before day one of the competition, teams are encouraged to seek outside help to develop their policy briefs. Teams are also encouraged to refer to playbooks and scenarios from past Cyber 9/12 competitions. Playbooks include the competition materials and recommendations of award-winning teams. Find past scenarios and playbooks here: https://www.atlanticcouncil.org/technology-innovation/cybersecurity/2020-cyber-9-12-strategy-challenge-playbooks/

Teams are expected to rely on their coaches in particular to help develop and revise their policy ideas for the competition. Commencing on day one of the competition, no outside assistance is allowed for teams. Teams may confer with their coach during the breaks between rounds.

During the competition rounds, teams are not allowed to use electronic devices, apart from the device they are using for video teleconferencing. 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.

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 three 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

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.

Teams may not observe rounds that they themselves are not competing in.

The Cyber 9/12 Strategy Challenge reserves the right to partner with the media to provide coverage of the event. 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 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 winner of the competition.

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

functions, speeches, and other events accompanying the event. 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.