Atlantic Council CYBER 9/12 STRATEGY CHALLENGE / GCSP Geneva Centre for Security Policy

25-26 April 2019
Geneva,
Switzerland

A major cyber attack has occurred. How should Europe respond?

We frequently hear the terms 'Cyber 9/11' and 'Digital Pearl Harbor,' but what might policymakers do the day after a crisis? The Cyber 9/12 Strategy Challenge is an annual cyber policy competition for students across the globe to compete in developing national security policy recommendations tackling a fictional cyber incident. In 2019, the 5th European Cyber 9/12 Strategic Challenge will take place in Geneva, Switzerland from 25-26 April 2019.

Winners of the 2018 European Challenge: Team Black Knights from the US Military Academy at West Point in the United States receives the 2018 award from Ambassador Christian Dussey, GCSP Executive Director (far left) and Ms Chelsey Slack, NATO Deputy Head of Cyber Defence (far right).

What is the challenge all about?

The Cyber 9/12 Strategy Challenge is a unique competition designed to provide students from a range of academic disciplines with a deeper understanding of the policy challenges associated with cyber crisis and conflict. Part interactive learning experience and part competitive scenario exercise, it challenges teams to respond to a realistic, evolving cyberattack and analyse the threat it poses to national, international, and private sector interests.

Students and professionals have a unique opportunity to interact with expert mentors and high-level cyber professionals while developing valuable skills in policy analysis and presentation. To date, the competition has engaged over one thousand students from several European countries, the United States and beyond.

Facing the Global Strategic Challenge

In the European competition, hosted by the Geneva Centre for Security Policy (GCSP) in partnership with the Atlantic Council, students respond to a major cyberattack on European critical infrastructure and services. Competitors provide recommendations balancing individual national approaches and a collective crisis management response, considering capabilities, policies, and governance structures of NATO, the EU, and individual nations. The competition fosters a culture of cooperation and a better understanding of these organisations and their member states in responding to cyberattacks.

How to participate

...in the Student Track:

Graduate and undergraduate students from any university, including defence colleges and military academies, are invited to apply to compete in teams of four. There are no requirements for team composition based on academic majors, education levels, or nationalities of team members.

...as a competitor in the Professional Track:

Graduate and undergraduate students from any university, including defense colleges and military academies, are invited to apply to compete in teams of four. There are no requirements for team composition based on academic majors, education levels, or nationalities of team members. Competitors in this category will have substantial relevant professional experience related to cybersecurity, policy and strategy.

...as a coach:

Each team must recruit a coach to assist in preparing for the competition. One coach can serve for several teams. Teams are expected to consult with their coaches to help develop and revise their policy ideas for the competition and confer with them during breaks between competition rounds.

...as a judge:

Experts with significant policy and cybersecurity experience are invited to serve as judges. Judges evaluate the student teams' oral presentations based on the quality of their policy responses, their decision-making processes, and their presentation skills. Previous judges include practitioners from various sectors, such as government, international organisations, information and communications technology, finance, and the press.

...as an observer:

All competition events are open to the public, and we welcome anyone interested in cybersecurity policy to join us as an observer.

...as a sponsor:

The competition is a unique opportunity for companies to support next-generation cybersecurity education on both sides of the Atlantic and position themselves as innovative thought leaders in the field. Depending on the level of sponsorship, our partners receive great benefits including the potential to recruit top tech and policy talent; advertisement in print and online; promotional side events; and keynote and judging opportunities.

Timeline:

One Month before the competition:

Teams receive Intelligence Report I. The stage is set for the simulated cyberattack and the teams start preparing written policy briefs.

Two Weeks before the competition:

Teams submit the written policy briefs.

Competition Day 1 – Qualifying:

Teams give a ten minute presentation to a panel of judges, followed by ten minutes of judges' questions and final feedback. Advancing teams receive Intelligence Report II.

Competition Day 2 – Semi-final and Final:

Semi-final teams present modified policy recommendations based on the evolving scenario. Teams in the final round are given Intelligence Report III and limited time to adjust their recommendations. Finalists present on stage to a panel of distinguished judges, who award the winners in a closing reception.

Past supporters

Deloitte.

NATO OTAN

Microsoft

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA

PERMANENT MISSION OF FINLAND GENEVA

Permanent Representation of Estonia to the UN and other International Organisations in Geneva

COUP4

KUDELSKI SECURITY

CLANED GROUP

nixu cybersecurity.

To register or for more information, please contact: Ms Radostina Raykova of the Geneva Centre for Security Policy at r.raykova@gcsp.ch **www.gcsp.ch/events/cyber-9-12-student-challenge-2019**