Atlantic Council

Cyber 9/12 STUDENT CHALLENGE

A MAJOR CYBERATTACK HAS OCCURRED. HOW SHOULD YOUR NATION 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 Student Challenge is an annual cyber policy competition for students across the globe to compete in developing national security policy recommendations tackling a fictional cyber catastrophe. In **2016**, the Student Challenge will take place in **Washington, DC** on **March 11-12** and in **Geneva, Switzerland,** on **April 7-8**.

Winners of the 2015 Euro-Atlantic Challenge, Team Switzerland, with NATO Assistant Secretary General for Emerging Defense Challenges Ambassador Sorin Ducaru and GCSP Director Ambassador Christian Dussey.

THE STUDENT CHALLENGE

In **Washington, DC**, student teams confront a serious cybersecurity breach of national and international importance. Teams will compose policy recommendations and justify their decision-making process, considering the role and implications for relevant civilian, military, law enforcement, and private sector entities and updating the recommendations as the scenario evolves.

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

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

WHAT IS THE CHALLENGE ALL ABOUT?

Now entering its fourth year, the Cyber 9/12 Student Challenge is a one-of-a-kind competition designed to provide students across 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 analyze the threat it poses to national, international, and private sector interests.

Students have a unique opportunity to interact with expert mentors and high-level cyber professionals while developing valuable skills in policy analysis and presentation. The competition has already engaged over four hundred students from universities in the United States, United Kingdom, France, Poland, Switzerland, Hungary, Finland, and Estonia.

Gen. Michael Hayden (Ret.), former NSA and CIA Director, addresses students at the 2015 Challenge in Washington, DC.

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 – Semifinal and Final
Semifinalist teams present modified policy recommendations based on the evolving scenario. Teams advancing to the final round are given Intelligence Report III and very limited time to adjust their recommendations. Finalists present on stage to a panel of celebrity judges, who award the winning team in a closing reception.

Student team presenting policy recommendations to a panel of judges in Geneva, 2015.

Heli Tiirmaa-Klaar, Head of Cyber Policy Coordination at the European External Action Service, in a conversation with students in Geneva in 2015.

HOW TO PARTICIPATE

. . .as a competitor:
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.

. . .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 organizations, 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 recruitment of top tech and policy talent; advertisement in print and online; promotional side events; and keynote and judging opportunities.

. . .as a host:
We offer opportunities to host one- or two-day qualifying and affiliated events. These events are run by students, faculty, or university staff with support from the Atlantic Council.

To register or for more information, please contact:

Anni Piiparinen
Program Assistant
Cyber Statecraft Initiative - Atlantic Council
Email: APiiparinen@AtlanticCouncil.org
Phone: +1-202-292-5164

PAST SUPPORTERS

Symantec. F-Secure. codenomicon

THE WILLIAM AND FLORA HEWLETT FOUNDATION

NATO OTAN

This event was supported by NATO's Public Diplomacy Division

COLUMBIA | SIPA School of International and Public Affairs

leidos SAIC.