
*We frequently hear the terms "Cyber 9/11" and "Digital Pearl Harbor," but we rarely discuss what they actually mean or what policymakers might do after such an event. The Cyber 9/12 Project explores how the international community should respond the day after a major cyber catastrophe.*


Entering its third year of competition, the Cyber 9/12 Student Challenge remains the only student competition devoted to national security policy recommendations for day-after responses to a major cyber incident. The competition is designed to offer students, across a wide range of academic disciplines, a better understanding of the policy challenges associated with cyber conflict. In 2015 the competition will include two events, one at American University in Washington, DC on March 13-14 and one in Geneva, Switzerland on April 22-23.

Part interactive learning experience and part competitive scenario exercise, the Cyber 9/12 Student Challenge gives students interested in cyber conflict policy an opportunity to interact with expert mentors, judges, and cyber professionals while developing valuable skills in policy analysis and presentation. Throughout the competition, students will respond to a serious cybersecurity event by composing their ideal policy recommendations and justifying the decision-making process used to rank priorities. Student teams will be challenged to react to an evolving scenario involving a major cyberattack and analyze the threat it poses to public 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.

**Learn more about how to become a competitor, judge, or sponsor at:**
**http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12**

## EURO-ATLANTIC STUDENT CHALLENGE

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

The European competition, hosted in partnership with the Geneva Centre for Security Policy and scheduled to take place in Geneva in April 2015, will focus on cooperative security in the Euro-Atlantic space. The evolving scenario will build around a major cyberattack on European networks. Competitors will be asked to give recommendations on the appropriate balance of individual national responses and a collective response in the management of a crisis, including capabilities, policies, and the governance structures of NATO, the EU, and individual nations. Beyond being a prime educational experience, the competition will foster a culture of cooperation and better understanding of NATO, EU, and national policies, capabilities, and structures in responding to and mitigating the effects of cyberattacks.

## ABOUT THE COMPETITION

The Cyber 9/12 Student Challenge consists of a single fictional simulated cyberattack scenario described through various intelligence reports that evolve over three elimination rounds of competition. The exercise encompasses tasks, both written and oral, that challenge students to respond to political, economic, and security issues, requiring advancing teams to modify their policy recommendations.

In the qualifying round, teams are judged based on a written policy brief submitted in advance of the competition and an oral presentation delivered to a three judge panel of experts on day one. Scores from the brief and presentation are combined to narrow the field of teams that advance to deliver presentations to a separate panel of judges during the semifinal round at the beginning of day two. Testing their ability to analyze information and synthesize a response with limited advance preparation, semifinal teams will be given an intelligence report that alters the original scenario at the qualifying awards ceremony reception at the end of day one. Semifinal scores are tallied and teams advancing to the final round are held in isolation as each team is brought on stage to make a presentation to a panel of celebrity judges. Finalist teams will react to an intelligence report that further alters the scenario with very limited time to adjust their recommendations.

## COMPETITION ROUNDS

Teams will write a policy brief, limited to five single-sided pages in length, recommending appropriate actions and policy responses for the actors involved. During each presentation, teams will be given ten minutes to present their policy recommendations, followed by ten minutes to answer direct questions from a panel of judges. Answering the scenario, teams must produce four policy response alternatives that respond, counteract, mitigate, and/or disrupt the damage and continued threat of the current cyberattack. For the brief and presentations, teams consider a variety of offensive and defensive response alternatives that take into account the roles of state, private sector, and international actors. In particular, teams consider the role of cooperation between different actors necessary to achieve desired policy outcomes.

## FOR COMPETITORS

Graduate and undergraduate students from US and international universities, including defense colleges and military academies, who are interested in the disciplines of cybersecurity policy, international relations, computer science, law, and other related fields are invited to apply to compete in teams of four individuals. Teams that register 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.


*Suzanne E. Spaulding, Under Secretary for the National Protection and Programs Directorate, Department of Homeland Security*

*General Michael Hayden (Ret.), Principal, Chertoff Group, Former Director, NSA and Former Director, CIA*

## FOR JUDGES

We are seeking experts with previous policy and cyber experience to serve as judges. Each round of the competition will be judged by a panel of cyber policy experts. Experts representing various sectors including government, finance, telecom, and the press engage small groups of students to promote awareness of cybersecurity policy issues and provide students feedback on new ideas on the future of cybersecurity policy.

## FOR COACHES

Each team must recruit a coach to assist in preparing for the competition. Teams are expected to rely on their coaches in particular to help develop and revise their policy ideas for the competition and confer with them during the breaks between rounds and stages.


*Deborah Lee James, Twenty-third Secretary of the Air Force*

## FOR OBSERVERS AND VOLUNTEERS

The success of the competition relies on dedicated and engaged volunteers. All competition events are open to the public.

**To register or for more information and sponsorship opportunities please visit**
**http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12**
**or contact Cyber912@AtlanticCouncil.org**

## FOR SPONSORS

The Cyber 9/12 Student Challenge is a unique opportunity for companies to recruit top talent from both technical and policy fields and a prime branding opportunity. Hosting competitions both in the US and Europe lets our partners reach markets on both sides of the Atlantic.

### Global Partnership Sponsors - $50,000

- "Platinum Sponsor" level sponsorship recognition at both Cyber 9/12 competitions in the US and Europe
- Membership on the Cyber 9/12 Steering Committee
- Benefits of the President's Circle corporate membership

*Plus all benefits of lower levels*

### Platinum Sponsors - $35,000

- Additional page for advertisement in program
- Provide a banner and other signage for display in the judge and competitor lounges
- Provide company representative for keynote introduction and final round panel of judges
- Additional piece of company literature in competition bag

*Plus all benefits of lower levels*

### Gold Sponsors - $20,000

- One-page advertisement in program
- Provide brief video content that may be added to our video loop played during the competition
- Competition bag insert—one piece of company literature in the competition bag distributed at registration to all competitors, judges, coaches, and other special guests

*Plus all benefits of lower levels*

### Silver Sponsors - $10,000

- Half page advertisement in program
- Your company logo on a slide at the keynote presentation and judge and competitor lounges

## ABOUT THE ATLANTIC COUNCIL

The Atlantic Council promotes constructive leadership and engagement in international affairs based on the Atlantic Community's central role in meeting global challenges. The Council provides an essential forum for navigating the dramatic economic and political changes defining the twenty-first century by informing and galvanizing its uniquely influential network of global leaders. Through the papers we write, the ideas we generate, and the communities we build, the Council shapes policy choices and strategies to create a more secure and prosperous world. For more information, please visit www.AtlanticCouncil.org.

## ABOUT THE CYBER STATECRAFT INITIATIVE

The focus of the Cyber Statecraft Initiative is to examine the overlap of national security, international relations, and economic security issues to provide practical and relevant solutions to challenges in cyberspace.
The Cyber Statecraft Initiative has made its mission "Saving Cyberspace," to help create a more sustainable Internet, one that will be as open, free and awesome for future generations as it was for its pioneers.

The Initiative works with Fortune 500 companies, governments, and other stakeholders to position themselves as thought leaders in cyber statecraft—the key tool to generate innovative solutions for a better Internet.

## ABOUT THE GENEVA CENTER FOR SECURITY POLICY

The Geneva Centre for Security Policy (GCSP) is an international foundation with over 40 member states from across the globe. It provides forward-thinking and innovative solutions for leaders and policymakers. Committed to the highest professional standards, the GCSP trains government officials, diplomats, military officers, international civil servants and NGO staff in pertinent fields of international peace and security. GCSP activities are organised across three separate programmes. Its Emerging Security Challenges Programme deals with, among others, cyber security issues. In this context the programme has engaged in various research activities, training modules and dialogue events. For further information, please visit www.gcsp.ch.