Atlantic Council

CYBER 9/12 STRATEGY CHALLENGE

A MAJOR CYBERATTACK HAS OCCURRED. HOW SHOULD YOUR NATION RESPOND?

We frequently hear the terms "Cyber 9/11" and "Digital Pearl Harbor" to describe a crippling cyberattack; but what might policymakers and operators do the day after a crisis? The Cyber 9/12 Strategy Challenge is an annual cyber policy and strategy competition for students across the globe to compete in developing national security policy recommendations tackling a fictional cyber crisis.

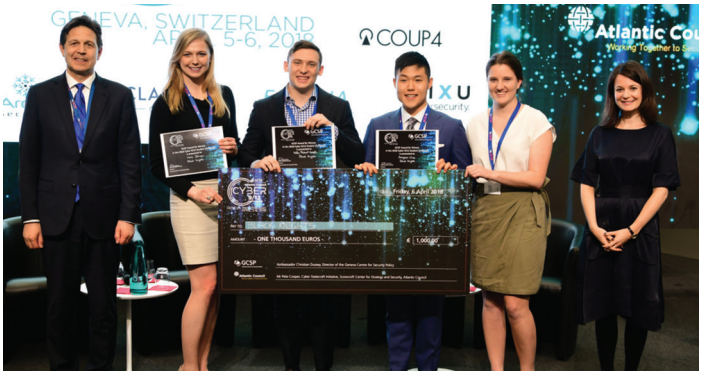
In 2019, the Strategy Challenge will take place in **Austin, Texas** and **Lille, France** in January; **London, United Kingdom** in February, **Washington, DC** in March, **Geneva, Switzerland** in April and **Sydney, Australia** in October.

WHAT IS THE CHALLENGE ALL ABOUT?

Now entering its seventh year, the Cyber 9/12 Strategy 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**. 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. The competition has already engaged **over one thousand students** from universities in the United States, Europe, Indo-Pacific, and the Middle East. Students have a unique opportunity to interact with and receive feedback from expert mentors and high-level cyber professionals while developing valuable skills in policy analysis and presentation.

OUTCOMES OF THE CYBER 912 STRATEGY CHALLENGE

1. Build a diverse community of cyber professionals who will remain in contact through the duration of their careers;
2. Foster trust and understanding through building bridges between the tech and policy communities and giving cyber military personnel a chance to work alongside their civilian colleagues;
3. Inculcate forward-looking and strategic thinking about the management of trade-offs while developing actionable policy solutions;
4. Connect next-generation cyber professionals with leading and emerging experts in major international policy hubs;
5. Cultivate multidisciplinary thinking in the next generation of cybersecurity professionals and policymakers, encouraging innovative solutions to one of the most challenging threats we face;
6. Immerse future leaders in challenging scenarios that simulate real-life cyber crises, while providing them with feedback and insights from judges who have had first-hand experience in responding to those crises.



Winners of the 2018 Cyber 9/12 Geneva competition with Ambassador Chritian Dussey, Director of the Geneva Centre for Security Policy and Chelsey Slack, Deputy Head of NATO's Cyber Defence Section.

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


Competitors at the Cyber 9/12 Washington, DC competition with Rob Joyce, Former Special Assistant to the President and White House Cybersecurity Coordinator and Klara Jordan, Director of the Atlantic Council's Cyber Statecraft Initiative.

Student team presents in the final round of the 2017 Student Challenge in Washington, DC.

A NEW NAME AND STRUCTURE FOR A GLOBAL CYBER CHALLENGE

In 2019, we aim to make adaptations to the Cyber Statecraft Initiative's flagship program in the United States—both in the name of the competition, as well as its structure and the professional development opportunities we will offer competitors. First, to better adapt to this growth the Cyber Statecraft Initiative has proceeded to alter the name of competition from the Cyber 9/12 Student Challenge to the **Cyber 9/12 Strategy Challenge** to better reflect that this is a **strategy and policy competition and not a technical capture the flag competition** with **global appeal.**

Second, to adapt to the diversity of teams in terms of both professional backgrounds and experience the competition is now structured to account for the experience and skill sets of teams. The competition will be comprised of two separate tracks—**Professional** and **Student**. The Professional Track will be comprised of teams whose members have substantial relevant professional experience and the Student Track will be comprised of teams whose members are undergraduate students and have less professional experience.

Third, we will offer more professional development opportunities for competitors. These development opportunities will include coaching on policy presentations, mentorship sessions with cyber professionals, alternate cyber crisis exercises for teams that do not advance to the semi-final round, access to cybersecurity-related events and organizations for competitors and the launch of a Cyber 9/12 Alumni Network to better connect past coaches, competitors and judges.

David Edelman of the MIT, Bobbie Stempfley of US CERT, Jen Weedon of Facebook, BG Jennifer Buckner of the US Cyber Command, Dmitri Alperovitch of Crowdstrike, and Kate Charlet of US Department of Defense.

HOW TO PARTICIPATE

. . .as a competitor in the Student 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 little or no relevant professional experience related to cybersecurity, policy and strategy.

. . .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 may 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 provides a unique opportunity for companies to support next-generation cybersecurity education and position themselves as innovative thought leaders in the field. Depending on the sponsorship level 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.

To register or for more information, please contact:

Safa Shahwan
Assistant Director
Cyber Statecraft Initiative - Atlantic Council
Email: SShahwan@AtlanticCouncil.org
Phone: +1 202 864 2861