Modeling, Simulation, Wargaming and Analysis for Cybersecurity

The United States is facing complex cybersecurity challenges, including public and private sector networks and information that are being exploited at an unprecedented scale. The United States must take action to protect the critical components upon which our economy, government, and national security are based from exploitation, disruption, or destruction. Organizations need a structured means to understand this threat.

Booz Allen can help you be ready for what’s next

To help prepare organizations for what’s next, Booz Allen Hamilton, a leading strategy and technology consulting firm, has been at the forefront of creating innovative wargaming experiments and exercises to test and validate concepts and strategies that examine current and future cyber security challenges.

Our clients benefit from the power of our functional and wargaming expertise. We have decades of experience in planning and executing scenario-based wargames and experiments for the US government. Our experts have supplied premier wargaming capabilities to clients with results that have fundamentally changed our clients’ operational approaches.

Booz Allen’s wargaming services and approach

Booz Allen handles all of the details of a wargaming event, freeing the client to concentrate on the big picture. We help our clients create the analytic framework for the event, build realistic and challenging scenarios, incorporate new simulations that stress the human dimension of cyber security operations, provide cyber security experts for analysis, and write concise after-action reports that outline observations and results from the event. We offer stakeholders and subject matter experts from our vast network spanning the federal government, academia, think tanks, and the private sector to assist with the wargame.

To meet the objectives of the wargame and address the client’s challenges, Booz Allen prepares the right game design, scenario, and simulation and conducts a thorough analysis.

- **Design.** The Booz Allen construct involves exploring identified issues with key stakeholders involved in cyber security activities, as well as interagency partners.

- **Scenario Development.** Booz Allen develops scenarios to help clients identify and explore trends, drivers, uncertainties, and wildcards shaping the future security environment. We develop a range of conceivable alternative scenarios, determine the implications, and help clients formulate hedging strategies to manage risk and position themselves for potential future opportunities.

- **Simulation.** Our simulations bring together outside experts to play side by side with officials to address a potential crisis or other policy challenge. By adopting the objectives of another actor, participants gain greater insight into actors’ underlying motivations and can fully explore the range of potential US actions or responses and their ramifications.
• **Analysis.** Booz Allen’s combination of process and subject matter expertise ensures the wargame analytical products go far beyond mere narratives. Our game reports consist of not only insights from game discussions and moves but also a quantitative and qualitative analysis generated by our suite of modeling and analytic tools.

**Booz Allen experience and expertise**

Booz Allen conceived and conducted a series of collaborative problem-solving exercises in the 1980s, internally referred to as “wargames.” Originally developed by Senior Vice President Mark Herman and game designers for the US Department of Defense (DoD), these simulations helped military leaders establish procedures for procurement, equipment maintenance, transportation, and other logistical details. In addition to DoD and federal government wargames, Booz Allen has facilitated hundreds of simulations and wargames for corporations, local governments, and nonprofit organizations since the 1980s.

Recently, Booz Allen has partnered with many clients to help them explore the complex nature of the cyber threat and understand how it affects their mission and organization. The following are examples of our recent cyber work:

• **Cyber Storm I and II.** Booz Allen has supported Department of Homeland Security (DHS) Cyber Exercise programs in regional and federal exercises, including the National Cyber Exercise—Cyber Storm I (February 2006). In March 2008 Cyber Storm II superseded Cyber Storm I and became the largest cyber exercise conducted to date by the US government. Cyber Storm II was designed as a full-scale simulation of a well-planned and coordinated cyber attack on critical cyber and physical infrastructures, exercising the readiness of public and private sectors to conduct a coordinated and well-informed response. The exercise’s objectives focused on the ability to evaluate policy and procedures in response to various cyber attacks and identified where further planning and process improvement may be needed.

  Cyber Storm II provided an opportunity to exercise communication and coordination among federal, state, international, and private sector entities. It also served as an opportunity to educate the public on the need for, and the importance of, cyber security. Cyber Storm II provided a venue to further preparedness, policy, and relationships in the greater cyber community.

• **Cyber Strategic Inquiry 2008 (CSI’08).** To further the public’s understanding of the cyber security vulnerabilities facing our nation, Business Executives for National Security (BENS), a non-partisan organization, teamed with Booz Allen to develop the CSI’08 in December 2008. CSI’08 brought together more than 180 senior leaders from government, industry, and civil society over a 2-day period to step through the challenges of cyber security and, from this, to realize potential processes, skills, and collaboration needed to address it.

  The inquiry was designed to represent a variety of functional and stakeholder interests and to highlight interconnectedness in a challenging scenario. The stakeholder teams included government teams representing defense, civil agencies/law enforcement, intelligence, and homeland security/law enforcement; industry teams representing financial services, telecommunications and information technology, energy, and transport; and a civil society team.

Whether you’re managing today’s issues or looking beyond the horizon, count on us to help you be ready for what’s next.