



Cyber Training

Developing the Next Generation of Cyber Analysts

Ready for what's next.

Booz | Allen | Hamilton



Table of Contents

The Crisis Moment	1
The Cyber Skills Gap	1
Developing a World-Class Cyber Workforce	2
Emulating the Medical Model.....	2
Aligning Training with Mission Goals.....	2
Keeping Pace in the Tech Race	5
Connecting the Dots in Cyber Space.....	6
Conclusion	8
About Booz Allen	9
Principal Offices	Back Cover

Cyber Training: Developing the Next Generation of Cyber Analysts

The Crisis Moment

You're a government technology leader responsible for protecting the systems that power critical infrastructure across your entire jurisdiction—but you've never seen anything like this.

A piece of malware has infected a power plant that delivers electricity to millions of citizens, and it's not interested in stealing information or spying—it's built to inflict physical damage. This super worm has taken control of the plant's automated factory control system and is now calling the shots. Service interruptions have already begun, but you're more worried about the safety of your citizens. If it's capable of crossing the digital divide and manipulating actual plant processes, what else is it capable of?

The malware has infected the plant's IT infrastructure without any action by internal personnel—nobody downloaded a rogue link. You've got your best cybersecurity experts conducting analysis, but time is running short. Do they possess the necessary cyber skills required for an effective response?

The Cyber Skills Gap

It would be comforting if the example above was hypothetical, but the description mirrors the Stuxnet computer super worm that was discovered in 2010. Stuxnet marks a transformative leap in cyber warfare, as a weapon capable of destroying physical assets. It is known to have infected tens of thousands of computers across the globe, seeking out targeted industrial systems. In November of that same year, Iran's president confirmed that the worm halted activities critical to the country's uranium enrichment program.¹

More sophisticated, complex, and powerful than any piece of malware to date, Stuxnet is essentially a “cyber missile” and a chilling reminder of the digital threats that nations face in the information age. Our enemies are less hindered by borders, cost, and availability of weapons than at any point in our history. Previous methods of attack—like bombs or missiles—could only be executed by a select few. By contrast, cyber attacks only require a certain amount of expertise and access to a computer, and the anonymity of the cyber environment lowers the risk of retaliation. Our national security experts used to worry about rogue individual hackers, but now they are facing threats from malware developers who are supported by governments and other political organizations capable of devoting significant resources to the creation of more intricate cyber weaponry.

The bad news is that as the threat evolves, the stakes get higher. The world's citizens are increasingly reliant on IT systems to deliver essential services like energy, communications, and healthcare. Critical infrastructure networks are more connected than ever before, and we share vast amounts of information online. As our society becomes more dependent on information technology, cybersecurity becomes absolutely essential, and the United States needs more cybersecurity professionals with the skills required to defend our citizens against these emerging threats.

Part of the solution involves identifying and recruiting top thinkers into the field of cybersecurity, but the more immediate challenge is ensuring that cyber professionals have access to the training and information they need to keep their cyber intelligence analysis skills relevant and effective. Due to the rapidly evolving nature of the threat, education and training must be continuous, and this document focuses on

¹ Ashford, Warwick, “Iran confirms Stuxnet hit uranium enrichment centrifuges.” *ComputerWeekly.com*, November 30, 2010, www.computerweekly.com/Articles/2010/11/30/244264/Iran-confirms-Stuxnet-hit-uranium-enrichment-centrifuges.htm (accessed 11 Feb. 2011)

strategies and best practices for developing a cyber force that maintains America's position as a global leader in the information age.

Developing a World-Class Cyber Workforce

The United States must begin developing a different kind of cyber analyst. Current cyber training is typically focused on the technical skills required to identify and respond to cyber threats. While those skills are essential, they are only effective when implemented within the broader context of intelligence analysis. It's not enough to know how to take down a network, or prevent an intrusion. Today's cyber analyst must be able to "connect the dots"—anticipating where threats could potentially originate from and understanding the broader, strategic implications of a cyber response. While necessary, technical skills alone are insufficient without the analytical skills required to develop a holistic threat picture and a proactive cyber strategy.

It really comes down to understanding what our enemies want, and how they think. The United States needs cyber professionals capable of anticipating attacks based on the attacker's motivation and culture. So what do our enemies want? Ideas are a highly sought after commodity in the digital age. Some attackers are attempting to steal trade secrets for economic gain. Others want to gain access to national security information. Still others are looking to bring down networks and halt critical infrastructure processes as a show of intimidation or terrorism. Defending our country's most critical assets requires a force of all-source intelligence analysts that also possess the skills and competencies to operate within modern cyber warfare. We need professionals who can recognize why an agency, network, or data set would be a target to an

enemy, and understand the cyber tactics that an enemy may employ to achieve its ends.

Emulating the Medical Model

The medical profession can serve as a helpful guide in building a comprehensive, well-rounded cyber force. Medicine, like cybersecurity, is a rapidly changing, complex field. Every day, new viruses are discovered, new treatments are developed, and practitioners must consistently incorporate the latest thinking into patient care. The medical profession also strives to be proactive rather than reactive, focusing research on prevention as well as prescription.

The world of cyber is very similar, as analysts are constantly challenged by new technology, (e.g., worms), new vulnerabilities, and emerging enemies. It's unreasonable to expect a single cyber analyst to be trained to respond to the incredible variety of threats that exist, but at the same time, there are some foundational skills that all cyber pros should possess. The goal is a cyber force comprised of general practitioners, specialists, and emergency responders.

The medical model shows that creating an effective force in a constantly evolving field requires continuous training. Doctors, surgeons, and nurses are required to stay up to date on current treatment methods, and much of this is done through rigorous qualifications, accreditations, and certifications that have been established within the profession. The cyber community can achieve the same results using a similar model, but the challenge lies in identifying the skills analysts must possess to ensure training initiatives align with current mission goals.

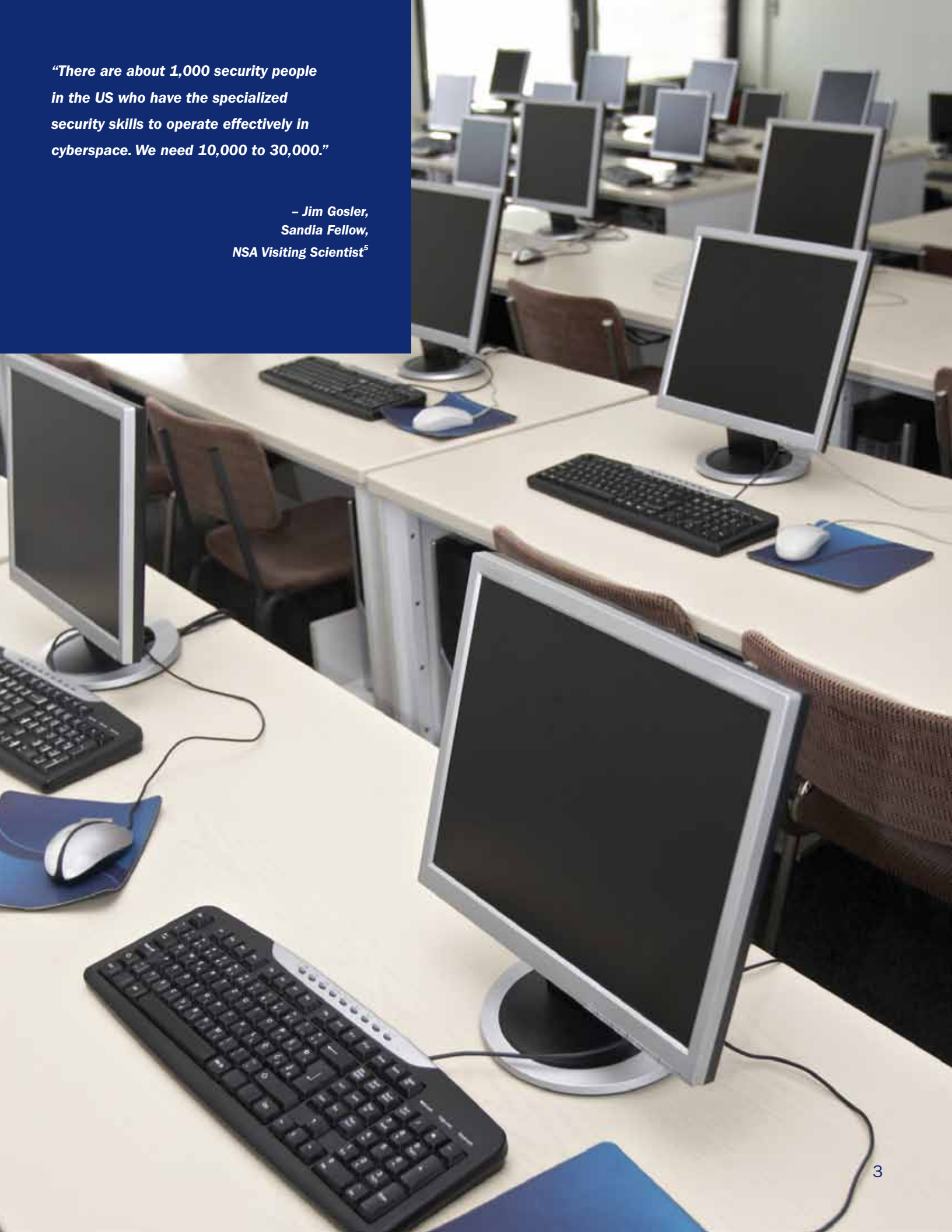
Aligning Training with Mission Goals

Too often, our top cyber certifications focus solely on technical competencies, and don't incorporate the

² Center for Strategic and International Studies, CSIS Commission on Cybersecurity for the 44th Presidency, *A Human Capital Crisis in Cybersecurity*, November 2010, http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf

“There are about 1,000 security people in the US who have the specialized security skills to operate effectively in cyberspace. We need 10,000 to 30,000.”

*– Jim Gosler,
Sandia Fellow,
NSA Visiting Scientist⁵*





structured analytical training techniques that produce cyber analysts capable of “big picture” thinking. We need to reexamine the processes we use to teach our cyber professionals how to think.

There have been many independent attempts by well-meaning organizations within the government to establish training standards, position descriptions, and certifications around cyber, but these disparate attempts lack uniformity and have led to confusion. In fact, the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency found that not only is the current system inadequate, it's also dangerous.³ Organizations are spending resources on training initiatives that aren't improving analysts' abilities to address threats, and these credentials are creating a false sense of security within the industry.

These are extremely distressing findings for the cyber community and a clear indication that analysts need access to more effective training methods that leverage best practices based on current industry research.

That's where Booz Allen Hamilton comes in.

For decades, Booz Allen has engaged in defining cyber roles and competencies with government agencies like the Office of Personnel Management (OPM), Office of the Director of National Intelligence (ODNI), and Department of Homeland Security (DHS). We know the challenges that our cyber clients are facing, we know the competency gaps, and we know how to conduct cyber training that gets results.

To guide organizations through the process of becoming “cyber ready” we've developed the Cyber People Readiness Suite, which is a modular approach for building a next-generation cyber workforce. Our methodology combines the latest technical training with

structured analytical techniques designed to develop necessary critical thinking skills. We understand that government needs a new type of cyber analyst—one capable of taking technical intelligence and merging it with traditional intelligence to produce a holistic threat picture. Booz Allen is currently guiding several federal agencies through this process—building critical thinking skills through 23 distinct analytical techniques that incorporate immersive, active learning exercises. During the process of building both technical and analytical general practitioner skills, we also offer specialist courses focused on developing regional expertise. Analysts use these courses to develop an understanding of the historical, cultural, and religious influences that impact the way our enemies think, what they value, and how they might engage in cyber warfare.

In support of these efforts, Booz Allen is using its Cyber University to increase the cyber talent pool for government agencies. The Cyber University has evolved into boot camps, advanced training and mentoring programs, and technical certifications where cyber professionals can acquire new competencies. Booz Allen's own consultants have the opportunity to learn about new tools and strategies, allowing them to stay ahead of emerging cyber trends, threats, and innovations and to better serve clients. Our training, education and performance support (TEPS) community of practice includes over 1,400 learning professionals, providing learning and education support services worldwide. We leverage their knowledge of the latest tools, technologies, and skills to meet current and future government mission requirements.

Keeping Pace in the Tech Race

The cybersecurity landscape has changed rapidly over the past decade, and the obsolescence curve is

³ Center for Strategic and International Studies, CSIS Commission on Cybersecurity for the 44th Presidency, *A Human Capital Crisis in Cybersecurity*, November 2010, http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf

unrelenting. Threats have evolved through technology innovation, and cyber professionals are being challenged to keep pace. Security experts used to worry about viruses taking down systems or monitoring networks to obtain valuable information. Now cyber analysts must prepare for the next generation of super worms like Stuxnet, capable of controlling and manipulating physical technology processes.

When new threats like Stuxnet emerge, the cyber community will be forced to act quickly. “Just-in-time” training will be replaced by “just-invented” training created in response to a specific emerging threat. To go back to our medical analogy, teams of emergency responders will need to be created to quickly understand these increasingly complex attacks. But, there are still general practitioner technical skills and previously identified threat detection techniques in which all analysts will need to be proficient in. Regardless of functional area, mission or title, competencies in network architecture, network security, information assurance, and Web technology will serve as foundational knowledge across cyber roles. Specialists in digital forensics, cloud computing, hacking methodology, and secure coding will also continue to be in high demand. For updating, refreshing, and building these technical security skills, existing commercial-off-the-shelf (COTS) training offerings can be extremely effective.

The SysAdmin, Audit, Network, Security (SANS) Institute, a leading provider of information security training, certification, and research provides high quality, off-the-shelf technical certification solutions that have proven successful in the past. And for technical training, why reinvent the wheel? Some of these courses are currently being used to satisfy requirements within DoD Directive 8570, which identifies key training for information

assurance roles within the defense industry. Today's COTS solutions are scalable, customizable, focused on cutting-edge cyber topics, and offer great value when training large teams. They are particularly effective for developing those foundational, general practitioner technical skills that all analysts need to have. COTS solutions work on the technical front because technical skills are more cut and dry, and easier to test. The real challenge lies in developing highly-complex problem solving abilities and threat detection techniques, because the United States needs cyber analysts, not just technical security experts.

Connecting the Dots in Cyber Space

Our clients are finding that their analysts need a richer skill set. They need professionals with advanced networking skills who can also conduct an all-source intelligence analysis. They need people capable of building contextual connections within highly complex information environments and making timely, informed decisions based on that data. They need analysts with critical thinking skills who understand the way our enemies are attacking systems and possess the ability to write credible reports based on those findings. They need people capable of leading interagency collaboration efforts and facilitating information sharing best practices. We've reached a tipping point within the cyber community—we need a different kind of analyst.

So how do we create the twenty-first century cyber pro? It all starts with learning how to think, and establishing a culture that values analytical reasoning and the ability to see things from alternative perspectives.

It sounds so fundamental, but thinking analytically is a skill that can be taught, learned, and improved with practice.⁴ In the world of intelligence, the key to success is processing information as accurately as

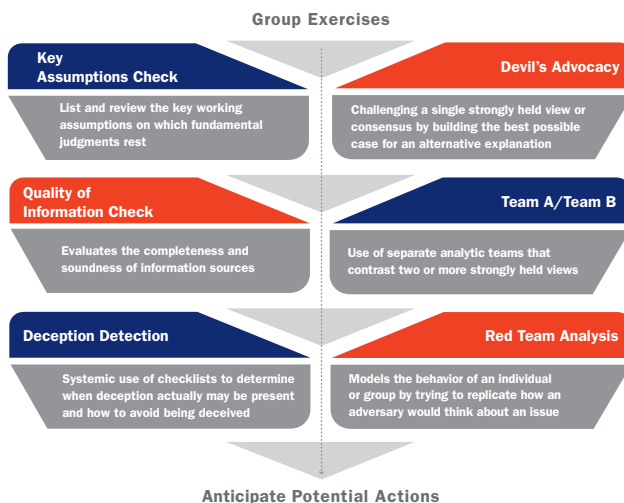
⁴ Heuer Jr., Richards, J., *The Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Pherson Associates, 1999.

possible in order to make informed strategic decisions. To do this, cyber analysts must understand the science of analysis, while recognizing the limitations of the human mind.⁵ Between past experiences, education, and cultural values, we all bring certain biases and mental constructs to the process of evaluating complex problems. This becomes a challenge for intelligence analysts when these existing biases lead to premature or incorrect assumptions. We tend to perceive what we expect to perceive, which can hinder our ability to get at the truth. For analysts, this process is made even more complicated by the fact that there is often organizational pressure to be “consistent” with interpretations. So analysts are encouraged, both internally and externally, to maintain original analyses, even in the face of new evidence. We know these things about the way the human mind works, and it’s important to teach analytical techniques that counterbalance these inherent weaknesses.⁶

Unfortunately, this is where COTS offerings fall short. Analytical skills are best developed through interactive, immersive training experiences. In other words, you can’t learn this stuff from a book. At Booz Allen, we’ve found success in a number of group exercises and “war games” that force analysts to question the fundamental basis of their interpretations. Some examples are listed in Exhibit 1.

The Red Team Analysis and Deception Detection exercises bring up another key challenge that cyber analysts face—understanding the motivations of our enemies. It’s common for all people to project their own cultural values onto other societies in order to make sense of them. Unfortunately, in the intelligence gathering world, this can result in misperceptions and misunderstandings. Foreign behaviors can often appear irrational through an American lens, and in order to

Exhibit 1 | Analytical Techniques for Improved Decision-Making



Source: Booz Allen Hamilton

truly understand motivation, analysts must thoroughly understand the cultures that shape enemy thinking.

To help build regional cyber specialists, Booz Allen has created customized training courses that examine the history, government, education, geography, religion, and existing military theories that shape thinking in strategic regions across the globe. To understand Pakistan, analysts need more than information on Pakistan, they need to understand the mental models, mind-sets, biases, and analytical assumptions that Pakistani citizens bring to complex global issues. An analyst can only anticipate potential actions when he or she is able to view the world as a potential enemy does.

These complex analytical skills can’t be measured through a multiple choice test. Critical thinking is enhanced by placing analysts in real-world scenarios involving rapidly changing threat data that demands a

^{5,6} Heuer Jr., Richards, J., *The Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Pherson Associates, 1999.

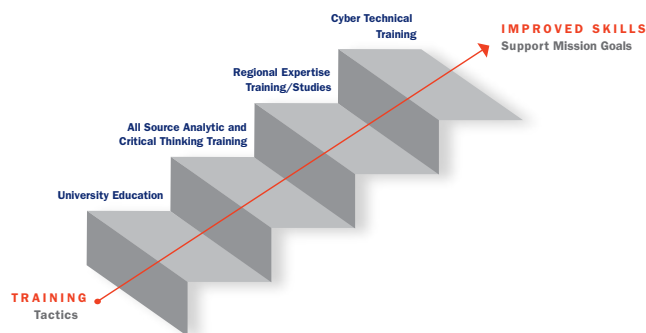
nanced response. There are many emerging tactics that have been proven to achieve significant results, including simulations, war games, social media tools, collaboration, case study reenactments, and board games. But, threat analysis is only one part of the process. These exercises must also simulate the management and strategic implementation of communications strategies between relevant stakeholders. Today's cyber leaders not only have to be capable of identifying threats, but also leading and orchestrating coordinated responses to cyber events.

Our clients are looking for customized analytical training exercises that prepare cyber personnel to deal with practical, current, real-world situations. Booz Allen works closely with agency training departments to create exercises that prepare analysts for today's security threats, but academia plays a strong role here, as well. One example comes from the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS). NPS has developed "CyberCIEGE,"⁷ a cutting-edge 3D video game in which players construct a networked computing system and defend it against a variety of attacks.

Simulations like CyberCIEGE are part of the next wave of learning solutions in the cyber community, and the emergence of social media has a role to play, as well. Analysts need to communicate with other analysts that have experienced complex cyber threat situations and exchange valuable intelligence on best practices. Chat rooms, forums, and Wikis are all tools that can rapidly expand the collective knowledge base of the entire cyber community. There is no replacement for experience, which is why Booz Allen training consultants base exercises on real-world events and map decisions to actual consequences.

All training tactics must be constantly evaluated for effectiveness and their ability to demonstrably improve skills that support mission goals, but it's clear that the cyber community must place more emphasis on analytical skills such as critical thinking, problem solving, stakeholder management, and communications. As analytical training evolves and matures, meaningful certifications and more relevant university degree programs must be developed to reinforce best practices.

Exhibit 2 | Developing a Next Generation Cyber Analyst



Source: Booz Allen Hamilton

Conclusion

The information age has redefined the way we think about warfare. In this new cyber environment, the United States requires leaders that possess both the analytical skills of a traditional intelligence analyst, and the technical skills of a cybersecurity expert. Building a cyber force with this unique skill set will require an evolution in training methodology, and the creation of a culture that values critical thinking. The challenge is great and the stakes have never been higher, so let us work with you to build your team of next-generation cyber analysts.

About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, the firm is a major provider of professional services primarily to US government agencies in the defense, intelligence, and civil sectors, as well as to corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning strategy and organization, technology, engineering and operations, and analytics—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant’s problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm’s many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and has annual revenues of over \$5 billion. *Fortune* has named Booz Allen one of its “100 Best Companies to Work For” for six consecutive years. *Working Mother* has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999. More information is available at www.boozallen.com.

To see how Booz Allen can help your cybersecurity workforce effort, please contact one of our consultants:

Michael Parmentier

Principal
parmentier_michael@bah.com
703/984-0081

Lee Ann Timreck

Principal
timreck_lee_ann@bah.com
703/984-0096

Grey Burkhart

Senior Associate
burkhart_grey@bah.com
703/377-6822



Principal Offices

ALABAMA

Huntsville
256/922-2760

CALIFORNIA

Los Angeles
310/297-2100

San Diego
619/725-6500

San Francisco
415/391-1900

COLORADO

Colorado Springs
719/387-2000

Denver
303/694-4159

FLORIDA

Pensacola
850/469-8898

Sarasota
941/309-5390

Tampa
813/281-4900

GEORGIA

Atlanta
404/659-3600

HAWAII

Honolulu
808/545-6800

ILLINOIS

O'Fallon
618/622-2330

KANSAS

Leavenworth
913/682-5300

MARYLAND

Aberdeen
410/297-2500

Annapolis Junction
301/543-4400

Lexington Park
301/862-3110

Linthicum
410/684-6500

Rockville
301/838-3600

MICHIGAN

Troy
248/680-3500

NEBRASKA

Omaha
402/522-2800

NEW JERSEY

Eatontown
732/935-5100

NEW YORK

Rome
315/338-7750

OHIO

Dayton
937/781-2800

OKLAHOMA

Oklahoma City
405/610-6523

PENNSYLVANIA

Philadelphia
267/330-7900

SOUTH CAROLINA

Charleston
843/529-4800

TEXAS

Houston
713/650-4100

San Antonio
210/244-4200

VIRGINIA

Alexandria
703/822-8920

Arlington
703/526-2400

Chantilly
703/633-3100

Charlottesville
434/973-2722

Falls Church
703/845-3900

Herndon
703/984-1000

McLean
703/902-5000

Norfolk
757/893-6100

Stafford
540/288-5000

WASHINGTON, DC

202/548-3061

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com.

Booz | Allen | Hamilton

delivering results that endure