

# Cyber Warfare Training Program

*The weaponry and strategies of digital conflict*



November 2009

## Syllabus

1. Introduction and Overview
2. Setting the Cyber Security Stage  
- *Vulnerability Analysis Model*
3. Cyber Hactivism  
- *Social Media Case Study*
4. Cyber Espionage  
- *Navy Case Study*
5. Cyber Terrorism  
- *al-Qaeda's Case Study*
6. Cyber Intelligence  
- *Counter Cyber Intelligence Case Study*
7. Cyber Weapons  
- *Cyber Weapons Classification Study*
8. eBombs, TEDs and Pulse Devices
9. Cyber Attack Process  
- *July 4<sup>th</sup> Attack Case Study*
10. Cyber Warfare Doctrine & Strategy  
- *Hypothetical Attack Design & Analysis*
11. International Issues (Investigations)  
- *Attribution Case Study*
12. GhostNet  
- *Case Study and Analysis*
13. The Problems of the Near Future  
- *Technology Scan Analysis*
14. Group Assignment Presentations
15. Summary & Review
16. Examination

This program is specifically designed to introduce participants to the fundamental components that comprise the cyber threat environment and their relationship to the principles of cyber warfare. This program is heavily weighted with current real-world cyber events and threat analysis.

Through programs like this, Technolytics delivers a comprehensive global cyber security and cyber intelligence review, encompassing risks and threats to your organization's reputations and information assets. Our formats range from 1.5 hour briefings to a 2 day-long formal training course as well as our 16 week academic program.

Modern societies around the world, as well as the militaries that defend them, are heavily reliant on computers and information technology and that reliance is expected to grow for the foreseeable future. The use of cyber weapons and attacks as an instrument of power projection and influence is becoming increasingly more challenging. The science of modern warfare has entered the information age. The rapid advancement of cyber attacks and the emergence of cyber warfare have caught government and military leaders around the world off guard. Cyber warfare issues are of a growing national interest and concern. Cyber capabilities are a critical aspect of modern day warfare and as such must be integrated into military doctrine. A number of nations are incorporating cyber warfare as a new part of their military doctrine. The development, acquisition and use of cyber attack capabilities demand governments, militaries and the technology sector take decisive actions to mitigate our risks.

As nations around the world continue their efforts to pull together all the components of a cyber security program, the greatest challenges to success may be enacting a multi-nation approach and enticing governments and the high tech industry to work together to address this growing threat. When you consider the foreign relations issues, the intricacies of international law and the blur of attribution, as well as the political issues that surround cyber conflict, the complexity of the cyber threat environment becomes clear and deeply concerning. As this complexity continues to increase, decision makers in the upper echelons of the national and international security community require a solid understanding of cyber security, cyber terrorism and cyber warfare in order to effectively interact with military officers, senior civilians, political appointees, Congress, the media, leaders of industry, and international organizations.

Cyber warfare is now viewed as a component of a comprehensive national security strategy rather than a stand-alone option. It is paramount that the military, intelligence agencies, government leaders, and the homeland security community develop an appropriate doctrine to systematically and appropriately counter the threat of cyber terrorism and cyber warfare. The program outlined below examines the current international and domestic issues as they might apply to acts of cyber aggression, and uses case study summaries of actual events in an effort to develop real-world insights. Of special interest to the military, intelligence, government leaders and homeland security communities, this program provides a common context for discussion, coordination and decision making. *Note: A classified version of this program is available.*

technolytics

The

# Technolytics Institute



November 2009

## Cyber Security

National and international cyber security has become a strategic imperative. The executive branch of government is gravely concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. Unlike many consulting companies, this is not a new issue for Technolytics. Given the Netscape background of many of our consultants, we can provide unique and valuable insights into the challenges of national and international cyber security.

Next year the information security market is expected to climb to nearly \$80 billion. That does not include the significant spending that will be needed to defend the critical infrastructure from cyber attacks. Technolytics has briefed dozens of Wall Street analysts on the exploding cyber defense market. We work with organizations and security product vendors and help them capitalize on the rapidly evolving security marketplace.

Technolytics provides a variety of service capabilities for our defense and intelligence customers including cyber defense analysis, cyber warfare strategies and analysis, homeland cyber security and national cyber security strategy. In addition, we provide briefing and educational programs including our new program — The Weaponry and Strategies of Digital Conflict based on our Cyber Commander's Handbook that will be released in the first quarter of 2010.

### The Technolytics Institute

4017 Washington Road  
Mail Stop 348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193  
I [www.technolytics.com](http://www.technolytics.com)

### Personal Contact

KGColeman@technolytics.com  
P 412-818-7656

Founded in 2000, the Technolytics Institute is an executive think-tank that focuses on the needs of management in business, government and industry. The Institute operates three centers of excellence: Business and Commerce, Security and Intelligence, and the Center for Science and Technology. Our cutting-edge research coupled with our thought leadership combine to create strategic value for our clients. We focus on initiatives that combine strategies, processes and the latest technologies. Our business is about understanding and identifying business dynamics, and developing break-through strategies and solutions that increase an organization's critical measures of success. In many cases our consultants become thought partners and strategic advisors to many of our clients. Working closely with members of our clients' executive management team, we provide an unbiased opinion and a fresh insight into the strategic problems encountered by organizations in business, government and industry.



The Technolytics Institute's Strategic Thought Leadership Program was founded on the belief that executives in business, government and industry demand a higher level of independent and objective insight regarding strategic issues in security. Our program provides these executives the opportunity to directly leverage strategic analysis, insight and guidance that applies specifically to their security interests, needs and issues. Our research and training programs are tailored to build strategic leadership capacities and skills through the development of state-of-the-art curriculum and activities in cooperation with national and international partners. In addition, our work influences government policy makers, security industry direction, corporate executives' knowledge and more.

Technolytics is not your typical think-tank or consulting company. We are not just involved in the conception of a strategy. We follow through and monitor and measure the progress being made toward the desired security posture. We work with security product and services providers and help them modify their thinking and adapt to the new management realities to make sure the defined solution works. Our Institute's dedicated staff, associates and advisors are the thought partners that help our clients address the strategic issues they face today.

technolytics

# Professional Biography of Kevin G. Coleman



November 2009

## Current Focus

Most recently Kevin has turned his attention on the international policy issues that surround acts of cyber aggression. This includes addressing the use of cyber attacks as an instrument of foreign policy and cyber activism / hacktivism as a means of political expression. In addition, he has investigated and reported on technology regulation, international cyber law and ethics regarding the acquisition and use of cyber weapons. He explores important characteristics of cyber warfare doctrine and investigates the current international and domestic military structures as they may apply to acts of cyber aggression and leverages analogies to traditional domains of conflict to develop relevant insights and forecasts for the evolution of cyber warfare. His insights and reports provide essential points of departure from traditional governmental research.

### Published Cyber Warfare Works

- Cyber Commander's Handbook
- Cyber Security Foreign Policy Issues
- Cyber Defense - Critical Infrastructure Protection
- Cyber Warfare - Private Sector Implications
- President Elects Obama's Cyber Policy Review
- Is the U.S. Prepared for a Cyber War?
- Cyber Command & Infrastructure
- Cyber Warfare
- Cyber Warfare 2.0
- Cyber Threat Analysis
- Cyber Soldiers of Fortune
- Cyber Warfare Doctrine
- Cyber Terrorism
- The Cyber Arms Race
- Advanced Cyber Weapons

### QUOTE

"What an eye opening briefing you provided during the Intelligence Summit. Particularly interesting was your perspective on cyber warfare. Your thoughts and observations were spot on and your insights into the future of unrestricted warfare has changed my thinking about our offensive and defensive capabilities."

*Conference Attendee*

Kevin G. Coleman is a seasoned technology executive with a comprehensive background in cyber security. Having eighteen years of success in the development and implementation of cutting-edge technology strategies, he continues to work with innovative leaders in business, government and industry on strategic issues of critical importance. He served for six years on the S&T Advisory Panel of the Johns Hopkins University Applied Physics Lab, an institutional thought-leader that conducts nearly \$1 billion in advanced research on topics including Asymmetric Warfare, Cyber Warfare and Unrestricted Warfare. With strong expertise in security assessments, analysis, design, development and implementation, he has built a reputation for solving strategic client's issues in the area of enterprise security and risk management. Currently, he advises clients with combined revenues nearing \$100 billion and a number of government agencies. He has personally briefed over 30 boards of directors and spoke at numerous corporate events on enterprise risk and security. In addition, he has twice brief U.S. StratCom and participated in multiple studies with them as well as working on recommendations to address the cyber breach that struck the Pentagon in November of 2008. He has testified twice before Congressional Commissions, briefed over fifty members from the U.S. Intelligence Community, presented on cyber terrorism at the United Nations, as well as briefing dozens of Wall Street analysts on the impact of cyber warfare on the defense industry. Finally, he lectured at the Harvard Kennedy School of Government, Senior Executive Program on National and International Security specifically addressing Cyber Security with attendees from twenty countries.



A Kellogg School of Management Executive Scholar, Coleman has authored dozens of articles addressing strategic security issues. Currently, he is a Senior Fellow with the Technolytics Institute and the Cyber Security Strategist and Adviser. Prior to Technolytics, Coleman served as the Chief Strategist at Netscape, a true American technology start-up success story. Before joining Netscape he was Vice President and Chief Strategist of Claremont Technology Group, which was Business Week's 44th fastest growing company. He joined Claremont from industry giant Computer Sciences Corporation where he was a Director in the National Consulting Practice and he began his career at the prestigious management consulting firm of Deloitte & Touche.

technolytics