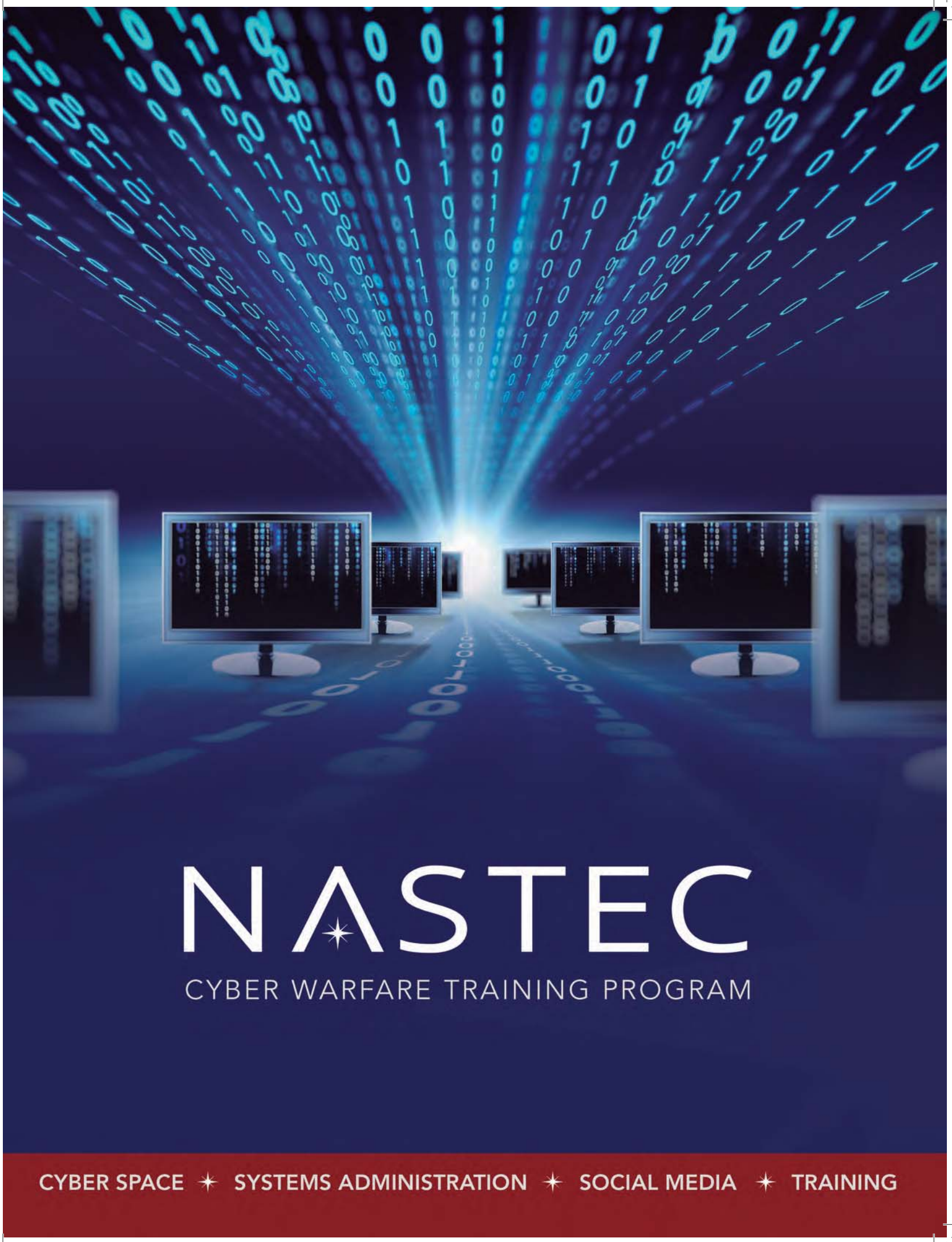

NASTEC
CYBER WARFARE TRAINING PROGRAM
CYBER SPACE ✦ SYSTEMS ADMINISTRATION ✦ SOCIAL MEDIA ✦ TRAINING

MILITARY LEADERSHIP CHALLENGES FOR THE 21ST CENTURY...

For the Qatar Ministry of Defense, the future operating environment will be less predictable, and diversity will increase both within and outside the military. Flexible and versatile leaders will need to deal with this increased uncertainty and diversity.

In the future, military leaders will be characterized by higher political/public visibility from media presence and speed of communications, and from other unofficial information which flows out of the area of operations. There is likely to be increased visibility, which may result in a higher potential for immediate interference and critical scrutiny of leader decisions and actions.

It will become more difficult to distinguish friend from enemy; military from civilian. Threats may be more confined or more urban, rendering some equipment and weapons ineffective. Additional challenges will be marked by more complex chains of command involving multiple connections (e.g., joint missions across all Qatari services; Qatari Military working with military forces from various countries and cultures; Qatari Military working with civilian agencies; Qatari troops under commanders from other services, other countries, and other civilian agencies).

Information overload resulting from the complex chains of authority and from the communications technology will require leaders at all levels to make decisions based on a greater awareness of the big picture. Information flow and volume are increasing at an exponential rate; leaders will have to filter critical information from high volumes of words and data.

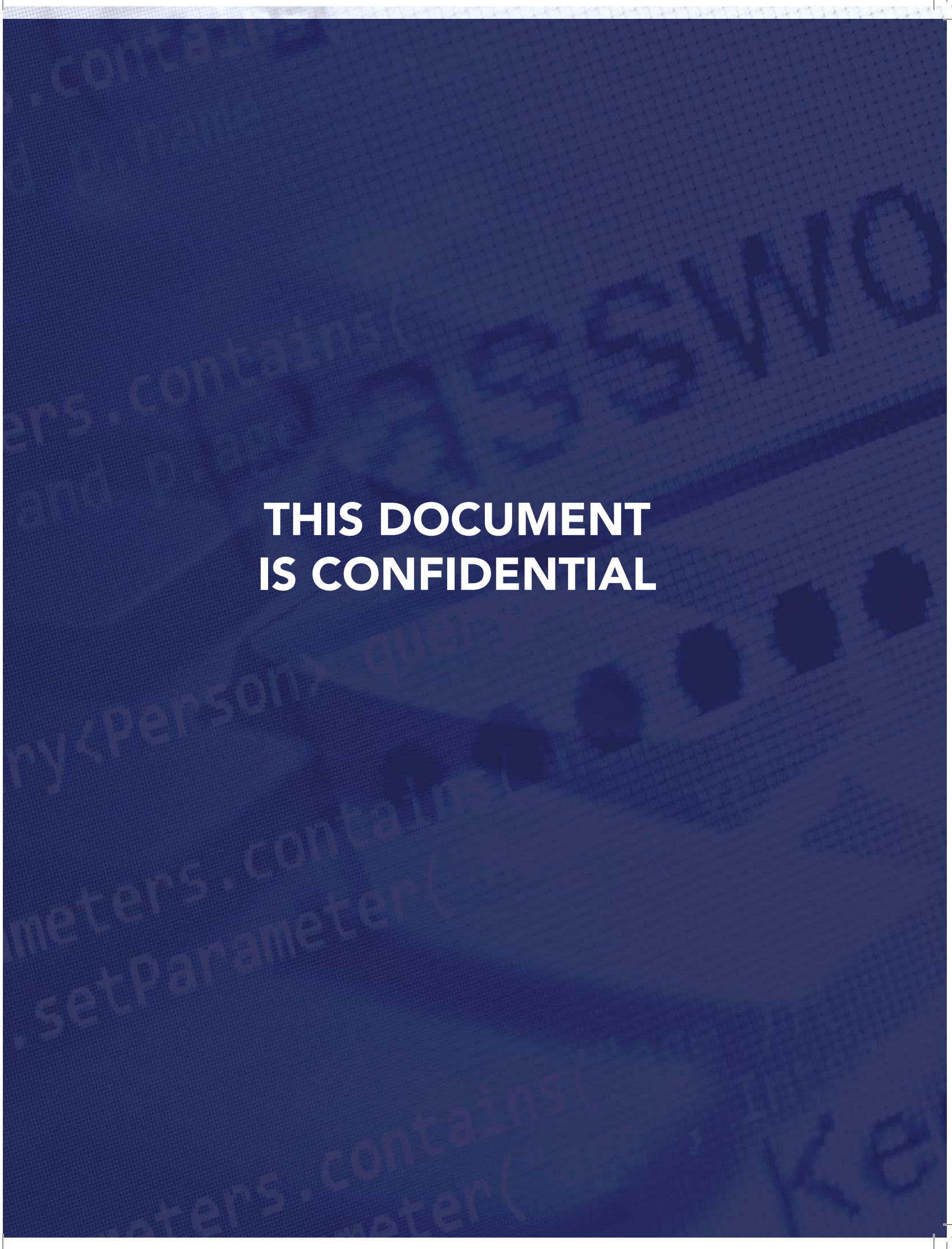
Investing resources to increase leaders' cognitive capacity and intuition will yield greater long-term returns than investments in information technology alone—the human brain processes information in orders of magnitude more efficiently than computers do today.

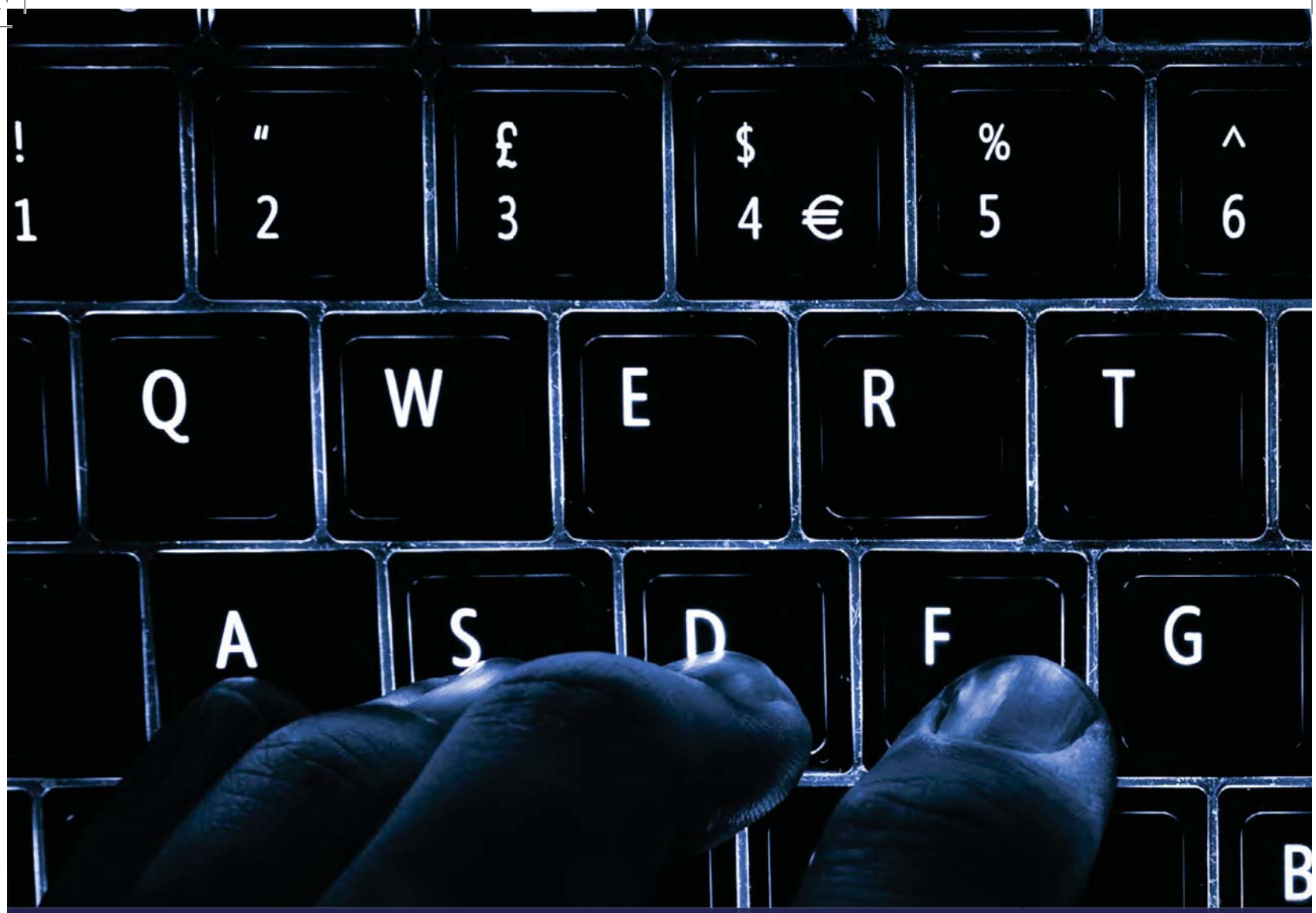
Leaders make decisions; computers do the information processing and analysis—the interaction between the leader and the supporting system is what is important.

Military leaders must understand the threats that exist in the ever-changing world environments, and manage the strategies that will defend and protect Qatar. Specifically, troop utilization must be balanced with effective training and resources that maximize the benefit of their experiences and technical expertise.

"Prior Planning Prevents Poor Performance"

Robert C. Ferguson
Nastec International, Inc.

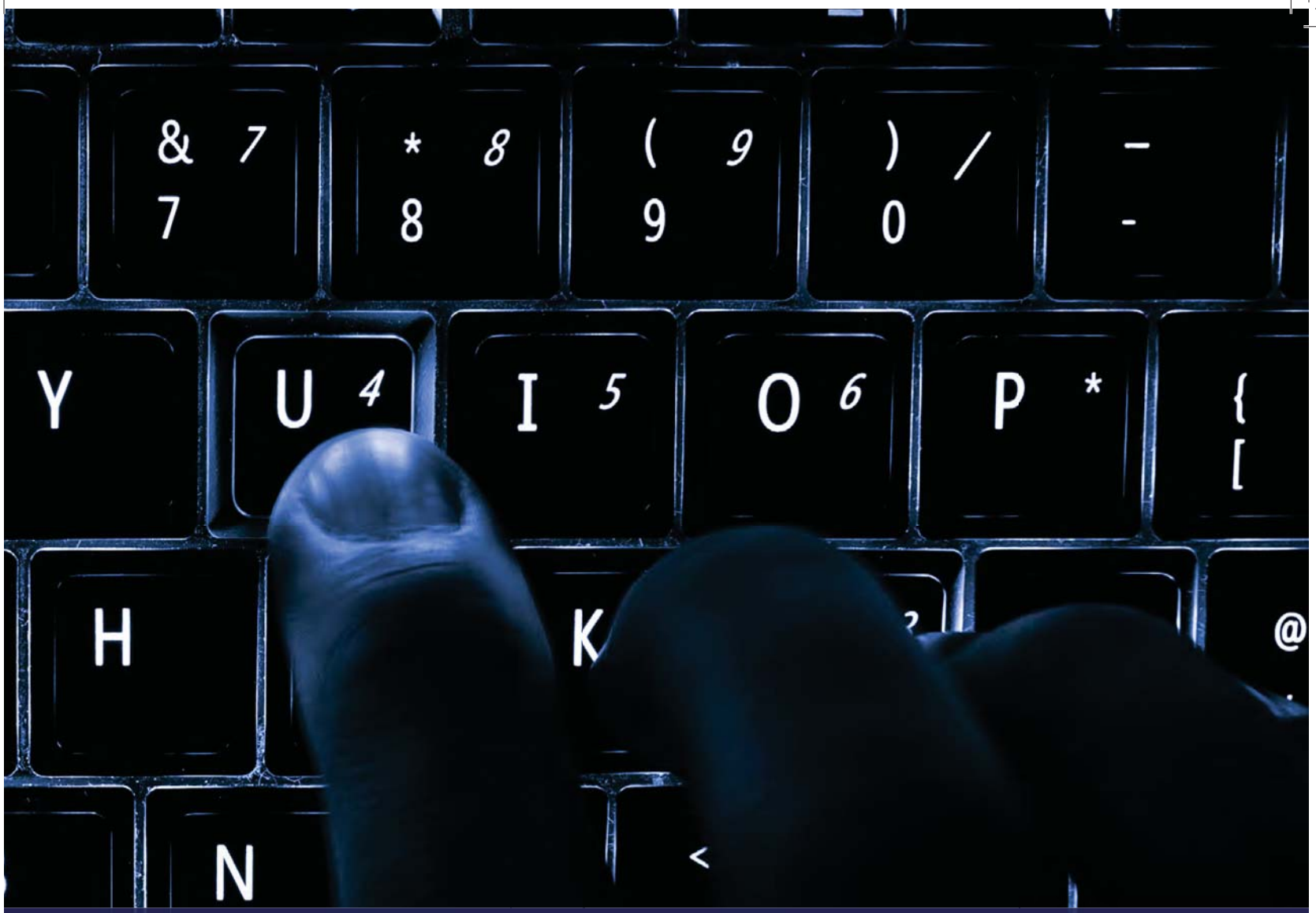

THIS DOCUMENT
IS CONFIDENTIAL



PREFACE

As Qatar enters the twenty-first century, the biggest threat to its national security is terrorist organizations. These ideological combatants use “CYBER WARFARE” as an alternative to conventional weapons. An attacker with great technical capabilities can create disruption by using a single computer wherever he or she is located. While the use of conventional weapons requires expensive manufacturing and physical travel to target locations, cyber-attacks can be conducted from anywhere. Traditional weapons have a cost that might be prohibitive for many and are hard to transport (or deliver) in secrecy. In other cases, attacks might require the sacrifice of the offenders. Cyber-attacks are quick, can be equally destructive and can definitely be inexpensive to execute.

Adding to this growing national security concern is the exploitation of social media as a terrorist’s preferred tool. In recent years, terrorist organizations have attempted to control their image, attract new recruits, and inspire “lone wolf” attacks through the use of social media, including disseminating images of graphic violence. Terrorist use of social media is resonating with vulnerable populations. Media platforms like Twitter are used to spread their message and enable supporters to find one another. These social media outlets are purportedly contributing inadvertently to the radicalization of the vulnerable and disenfranchised population in support of the terrorist’s sinister objectives.
It is vital that Military and Government Leaders develop an in-depth understanding of these new threats to the safety and security of the country and region, so that defensive strategies can be developed to identify, defend against, and mitigate the attackers of our liberty and way of life.



NASTEC International, Inc. has created a Cyber Warfare Training Program for Senior Military and Government Leaders, taught in the USA, which provides a firm foundation and understanding of Cyber Warfare and mitigation strategies. NASTEC fuses commercial technological opportunities—with the advanced military institutions available to us—with the ultimate goal of providing a comprehensive program that melds an in-depth Cyber Warfare capabilities and understanding with a social media component that identifies areas of concern and mitigation strategies, so that Leaders are better equipped to lead their various departments in this ever-increasing battle to defend cyber-attacks.

In the following pages you will find our Cyber Warfare Training Program. It is laid out by month, consolidating the various topics and disciplines in an efficient and easy to understand format.

Our instructors are at the top of their professions, and the various in-depth briefings held at locations, facilities and military installations will give the participant a first-hand view of how theory, practice and execution of the Cyber Warfare defenses becomes an integral part of national defense.

Welcome aboard...

“THE PROGRAM” ....

The NASTEC “Cyber Warfare Training Program” offers senior government and military leaders the unique opportunity to receive training (first-hand) instruction, and opportunities to interact in-person with Cyber Warfare units and commands situated in various locations across the USA.

You will learn from the “best” talent in the sector and learn the skills to stay on top of the ever-changing world of Cyber Security/Warfare. All of our classes are taught using the latest technology and we focus on providing the student with an awesome interactive experience.

Learn the Offensive Mission

Cyber Security is a rapidly evolving and growing field. It is a 24/7 monster that never sleeps. We strongly believe that the only way of having a solid defense is to understand aggressive practical offense. As you will see in our program catalog, we currently provide instructions in all areas of Cyber Security/Warfare.

Social Media Understanding and Terrorist Mitigation

Social Media represents the single fastest source of recruiting and radicalization of people today. Preventing “Terrorists” from exploiting the internet and Social Media to Recruit Terrorists and Incite Terrorist Acts is a block of specific instruction in “The Program”.
In the Social Media block of instruction you will discuss current threats posed by the use of the Internet and social media for terrorist purposes. Topics to be covered: Current threats and challenges posed by terrorist use of the Internet and social media for radicalization to terrorism, incitement to terrorism, training to conduct terrorist attacks; recruitment and travel assistance to foreign terrorist fighters; and coordinating, planning and financing of terrorist activities.

On-site Visits

The participants will travel to many of the important locations across the USA, such as major military installations, who have mission objectives concerning Cyber Warfare. You will meet with the Cyber Warfare Command Leaders where you will have the opportunity to discuss Cyber Warfare strategy and mission.
You will also visit Google, Facebook, Twitter, Microsoft and others, to experience the culture and inter-workings of the largest social media facilities in the world, and hold in-depth symposiums, classes and one-on-one discussions with the leaders in Social Media today.

Logistics

Upon Program Approval, Nastec will arrange all support (VIP level) regarding participant travel, transportation, accommodations, security and medical contingency. All courses, lectures, seminars and site visits are pre-approved and arranged so that the participant will gain maximum exposure to the Cyber Warfare communities and take advantage of the numerous planned site visits.

“Cyber Warfare Training Program”: Duration: 6 months. Tentative dates: December 2016 - June 2017

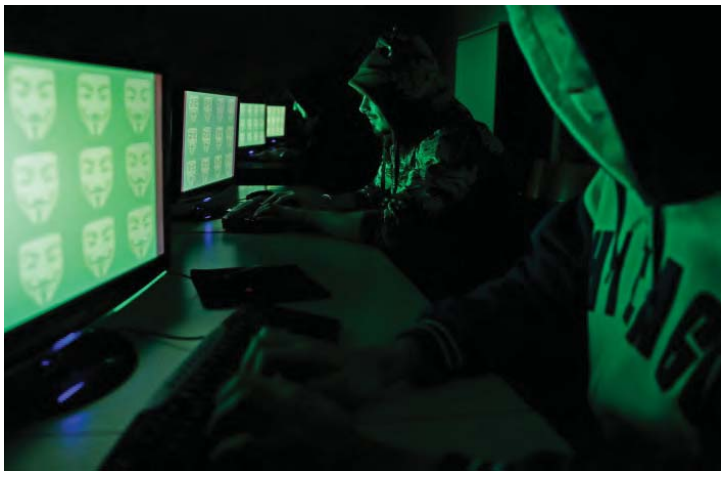
TABLE OF CONTENTS

INTRODUCTION TO CYBER WARFARE

The participant will gain an understanding of Computer Network Attack (CNA) and Computer Network Exploitation (CNE), which are derived from several public unclassified DoD documents, manuals, and directives. You will examine parallels between the cyber and kinetic counterparts and learn strategic uses, including when to deploy CNA and CNE operations. You will discover the limitations and legal considerations of CNA and CNE operations, and you'll walk through various attack scenarios to determine your proper course of action

CYBER WARFARE FOR PRACTITIONERS

This course explores the battlefields, participants and tools and techniques used during today's digital conflicts. The concepts discussed in this course will give information security professionals at all levels a better idea of how cyber conflicts are carried out now, how they will change in the future and how to detect and defend against espionage, hacktivism, insider threats and non-state actors like organized criminals and terrorists.



CYBER WARFARE MANAGEMENT

This course combines the views of both military and commercial analysts to provide participants with a well-rounded understanding of the conflicts within a cyber-war and how to best overcome them. Participants will understand the strategic, operational and tactical aspects of these conflicts and then use this knowledge to assist in developing more efficient procedures and technical defenses.

GLOBAL CYBERSECURITY

An in-depth study of cybersecurity from a global perspective. Topics include cyberterrorism, cybercrime, and cyberwarfare; the international legal environment; nation- and region-specific norms regarding privacy and intellectual property; international standard setting; effects on trade (including offshore outsourcing); and opportunities for international cooperation.

RISKS IN CYBER CRIME, CYBER TERRORISM AND WARFARE, CYBER THREATS...WHAT YOU NEED TO KNOW

The objective of this seminar is to provide practical and immediately usable information to professionals on how to protect both data and infrastructure from the ravages of electronic terrorism and associated cyber-crimes. Once only a topic for made-for-television thrillers, cyber terrorism has captured global front page headlines and reported top news stories from every facet of commerce. Individuals engaged in international, industrial espionage, organized crime, competitive intelligence gathering, political warfare, and destruction of critical infrastructure pose a threat to governments, organizations and citizens alike. This seminar is designed to provide the attendee with a fresh examination of the inherent risks associated with individuals or groups, who use cyberspace to threaten international governments, interfere with domestic operations, terrorize the citizens of a country, and attempt to disrupt corporate operations and how to minimize exposure to these risks.

PREVENTION AND PROTECTION STRATEGIES IN CYBERSECURITY

An in-depth study of the theories and practices for prevention of cyber-attacks. Countermeasures discussed include training, encryption, virtual private networks, policies, practices, access controls, secure systems development, software assurance arguments, verification and validation; firewall architectures, anti-virus, patching practices, personnel security practices, and physical security practices. Business continuity plans and disaster recovery plans (BCP, DRP) are also discussed. Strategies for large-scale prevention are also discussed, such as critical infrastructure protection, international collaboration and law enforcement.

LEARNING OBJECTIVES

- Analyze the strengths and weaknesses of firewall technologies and methodologies in protecting enterprise networks.
- Analyze the advantages and disadvantages of the different access control models, policies, and mechanisms used in large-scale networks.
- Use data protection techniques such as encryption and decryption to ensure confidentiality of sensitive data.
- Review and analyze current data breach methodologies and protection strategies for data leak protection.
- Assess the primary threats to software programs, services, and applications, and the advantages and disadvantages of measures used to protect them.
- Assess the threats posed by malicious software (malware) and the advantages and disadvantages of the anti-virus and anti-malware measures used to protect against them.
- Analyze the advantages and disadvantages of the main measures and techniques used to secure operating systems and to protect database and storage systems.
- Assess virtualization strategies and apply the principles and procedures used in configuring and deploying virtual networks.
- Analyze the requirements for effective digital and physical security management for organizations and individuals.
- Assess enterprise and national security incident handling tactics and techniques to minimize consequences of cyber-attack.

THE LAW, REGULATION AND ETHICS OF INFORMATION ASSURANCE

An overview of the legal, regulatory, and ethical issues related to cyberspace. Emphasis is on developing skills in spotting ethical and legal issues and navigating through the complex and changing legal and regulatory environment as it applies to behavior in cyberspace. Various resources and materials about the ethical and legal operation of modern computer systems, applications, and networks are presented.

LEARNING OBJECTIVES

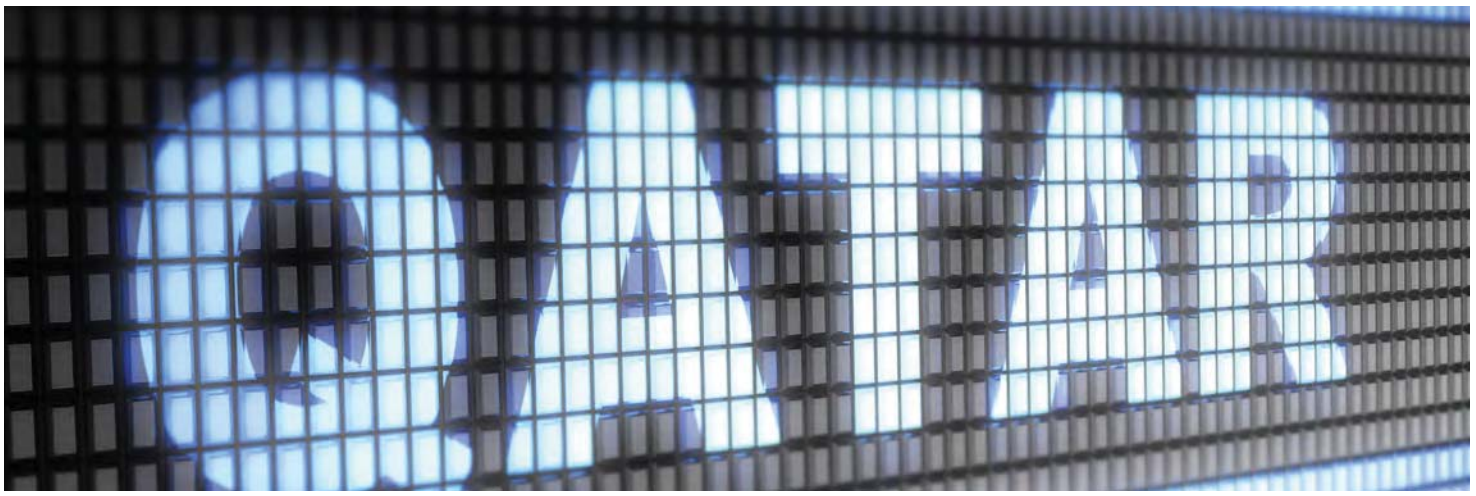
- Evaluate existing processes intended to ensure organizational compliance with regulatory legislation pertaining to information assurance, such as HIPAA and Sarbanes-Oxley, and recommend best practices to further strengthen oversight.
- Analyze and evaluate proposed or extant information security policies, practices and procedures in order to assess, in concert with their organization's legal representatives and advisors, potential ethical and legal liabilities that might flow from implementing them.
- Develop legally sound information handling requirements for cyber-attack incident response processes and procedures.
- Assess legal and regulatory compliance requirements pertaining to electronic commerce and draft use policies for an online enterprise.
- Demonstrate comprehension of the consequences of information privacy law violations for a business environment, and, in light of these concerns, apply entity- and industry sector-specific privacy laws and regulations to the management of information systems in that setting.
- Examine the legal and regulatory compliance requirements pertaining to the acquisition, use and licensing of intellectual property and digital rights, and develop policies to manage and enforce these rights in a specific environment.

ADVANCED SECURITY ESSENTIALS - ENTERPRISE DEFENDER

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC 501: Advanced Security Essentials Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

LEARNING OBJECTIVES

- How to build a comprehensive security program focused on preventing, detecting, and responding to attacks
- Core components of building a defensible network infrastructure and how to properly secure routers, switches, and network infrastructure
- Methods to detect advanced attacks of systems that are currently compromised
- Formal methods for performing a penetration test to find weaknesses in an organizations security apparatus
- Ways to respond to an incident and how to execute the six-step process of incident response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
- Approaches to remediating malware and how to clean up a compromised system



APPLIED CYBERSECURITY

Fundamentals of computer security technology, including cryptography, authentication, digital signatures, firewalls, intrusion detection, and network security tools and applications. Linux is used heavily throughout the course as it is a very commonly deployed operating system for servers.

LEARNING OBJECTIVES

- Design, deploy, and customize a firewall based on security policies
- Design, deploy, and customize intrusion detection system based on security policies
- Demonstrate an understanding of computer authentication, as well as how to audit passwords
- Demonstrate an understanding of cryptography, as well as how to deploy public/private key cryptography
- Demonstrate how to cope with ethical issues regarding security in organizations

CCFP - CERTIFIED CYBER FORENSICS PROFESSIONAL

In this course, you will learn the latest tools and techniques in a live, hands-on laboratory environment to conduct a simulated cyber investigation. The lab exercises include computer forensics using commercial tools, network forensics and Internet forensics. Such areas as email, applications, forensic timelines, social media and mobile devices will be addressed in addition to the traditional computer forensics examinations.

CCFP demonstrates your ability to gather, analyze, and deliver digital evidence that is accurate, complete, and reliable. The certification covers a range of skills necessary to support these environments from intrusion analysis to incident response, and newer challenges, such as mobile forensics and cloud forensics.

Outside of the laboratory exercises, you will address legal and ethical considerations, the foundations of digital forensic science within the context of the forensic sciences, and emerging and hybrid technologies as they impact the digital forensic investigator. The course is a combination of instructor lecture, hands-on lab exercises, instructor demonstrations and practicum exam with after-exam review.

LEARNING OBJECTIVES

1. Legal and Ethical Principles
- Nature and Characteristics of Evidence
- Chain of Custody
- Rules of Procedure
- Code of Ethics

2. Investigations
- Investigative Process
- Evidence Management
- Crime Scene Investigation Protocol
- Hybrid Crime Investigation
- Criminal Investigations
- Civil Investigations
- Administrative Investigations
- Forensics Responsibility to Security Incidents
- Electronic Discovery
- Intellectual Property (IP) Investigation

3. Forensic Science
- Introduction to the Scientific Method
- Fundamental Principles
- Forensic Analysis and Examination Planning
- Report Writing and Presentation
- Quality Assurance, Control, Management and Accreditation Procedures

4. Digital Forensics
- Digital Forensics Tools
- Media and File System Forensics
- Demonstration: Introduction to FTK
- Anti-Forensic Tools and Techniques
- Demonstration: Exploring the Evidence
- Lab – The Evidence: Basher's Second Computer
- Virtual System Forensics
- Embedded Device Forensics
- Mobile Device Forensics
- Demonstration/Discussion: Cellebrite
- A Few Forensic Tools and Techniques
- Demonstration – Network Forensics

5. Application Forensics
- Software Forensics
- Web, Email, and Messaging Forensics
- Demonstration – Web Forensics
- Demonstration – Email Forensics
- Database Forensics
- Demonstration – Database Forensics
- Lab – Creating and FTK Report
- Malware Forensics
- Demonstration – Malware Forensics

6. Hybrid and Emerging Technologies
- Cloud Forensics
- Social Networks
- The Big Data Paradigm
- Control Systems
- Critical Infrastructure
- Online Gaming and Virtual/Augmented Reality
- Labs

CERTIFIED CYBER FORENSICS PROFESSIONAL (CCFP)

The course is comprised of a total of the six CCFP domains based on the Common Body of Knowledge (CBK). The modular format is designed to organize and chunk information in order to assist with learning retention as participants are guided through the CCFP course materials. Each module/domain includes one or more of the following design approaches to ensure learning reviews and activities to support knowledge retention and transfer: Presentation, Short Lecture/Discussion, Group Activity, and Individual Activity. The lab exercises will include computer forensics using commercial tools, network forensics, and internet forensics. Such areas as email, applications, forensic timelines, social media, and mobile devices will be addressed in addition to the traditional computer forensics examinations.

LEARNING OBJECTIVES

- Further develop the skills and knowledge needed, as an experienced practitioner
- Address each element of the CCFP CBK (Common Body of Knowledge) through various learning techniques and lab exercises
- Use the latest tools and techniques in a live, hands-on laboratory environment to conduct a simulated cyber investigation

CERTIFIED ETHICAL HACKER

The Certified Ethical Hacker(CEH) training course enables participants to identify, counter and defend hackers from penetrating networks and gaining access to vital information. This will allow participants to deploy proactive countermeasures and in turn, stay ahead of information security developments.

COMPLIANCE CHECKLISTS (NIST FRAMEWORK)

This course prepares attendees to gauge their organization's cyber security posture and assess their readiness to implement a formal risk assessment and management process. In this course, attendees practice applying one widely implemented risk management framework.

COMPUTER AND SECURITY FUNDAMENTALS

A comprehensive overview of network security concepts that include: remote access, e-mail, the Web, directory and file transfer, wireless data, common network attacks, cryptography, operational/organizational security, disaster recovery, business continuity, and Cyber Ethics.

COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)

Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud. The CHFI course will provide participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law. It is no longer a matter of will your organization be comprised (hacked)? but, rather, when? Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber—criminal, then this is the course for you. Many of today's top tools of the forensic trade will be taught during this course, including software, hardware and specialized techniques.

LEARNING OBJECTIVES

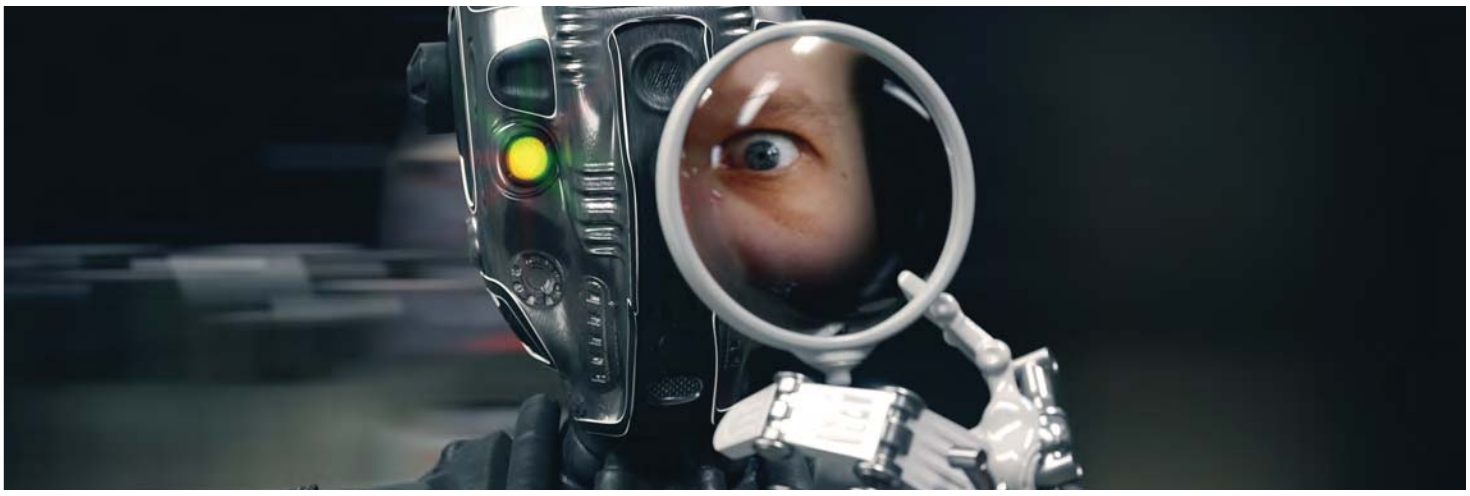
- Computer Forensics in Today's World
- Law and Computer Forensics
- Computer Investigation Process
- First Responder Procedure
- Understanding File Systems and Hard Disks
- Understanding Digital Media Devices
- Windows, Linux and Macintosh Boot Processes
- Linux Forensics
- Data Acquisition and Duplication
- Computer Forensic Tools
- Forensics Investigations Using Encase
- Recovering Deleted Files and Deleted partitions
- Image Files Forensics
- Steganography
- Application Password Crackers
- Network Forensics and Investigating Logs
- Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Router Forensics
- Investigating DoS Attacks
- Investigating Internet Crimes
- Tracking E-mails and Investigating E-mail Crimes
- Investigating Corporate Espionage
- Investigating Trademark and Copyright Infringement
- Investigating sexually harassment incidents
- Investigating Child Pornography
- PDA Forensics
- iPod Forensics
- Blackberry Forensics
- Investigative Reports

COUNTERINTELLIGENCE IN CYBER SPACE

The CICS course consists of lecture and practical exercises designed to teach basic information gathering techniques for online environments, personal electronic devices, and other emerging technologies.

COVERT ELECTRONIC SURVEILLANCE PROGRAM

Provide Law Enforcement personnel with tools for investigating cyber-crime related activities.



CRITICAL INFRASTRUCTURE PROTECTION

This course begins by examining in depth the events of the past 20 years, including the lessons learned about the interdependencies of the critical infrastructures following the Oklahoma City bombing and the terrorist attacks against the World Trade Center and what we learned in the aftermath of hurricanes Katrina and Rita in the summer of 2005. While there are many cross-sector interdependencies to consider, we will focus on the dependence of the various infrastructure sectors on the Internet and the impact of highly complex computer controlled systems. We will also discuss the creation of the US Department of Homeland Security and its role in protecting the nation's critical infrastructures from cyber intrusions.

LEARNING OBJECTIVES

- Receive detailed explanations of specific pervasive Internet technical problems and conduct in-depth examinations of the types of attacks that might do the most harm to your organization and your infrastructure sector.
- Learn how to develop business continuity and disaster recovery plans to counter current cyber threats and threat actors that take advantage of this model.
- Gain knowledge about the new directions being taken by criminals, terrorists, spies, and nation states and what our nation is planning to do for the defense of our critical infrastructure against these new threats.
- Learn how to protect your networks from the dangers lurking in cyberspace while developing a full understanding of emerging techniques used to detect and contain outbreaks of malicious activity on the Internet.

CRITICAL SECURITY CONTROLS: PLANNING, IMPLEMENTING AND AUDITING

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Council on Cyber Security. These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block the known attacks and the best way to help find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network though effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented.

Learning Objectives

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

CSFI: DEFENSIVE CYBER OPERATIONS ENGINEER (DCOE)

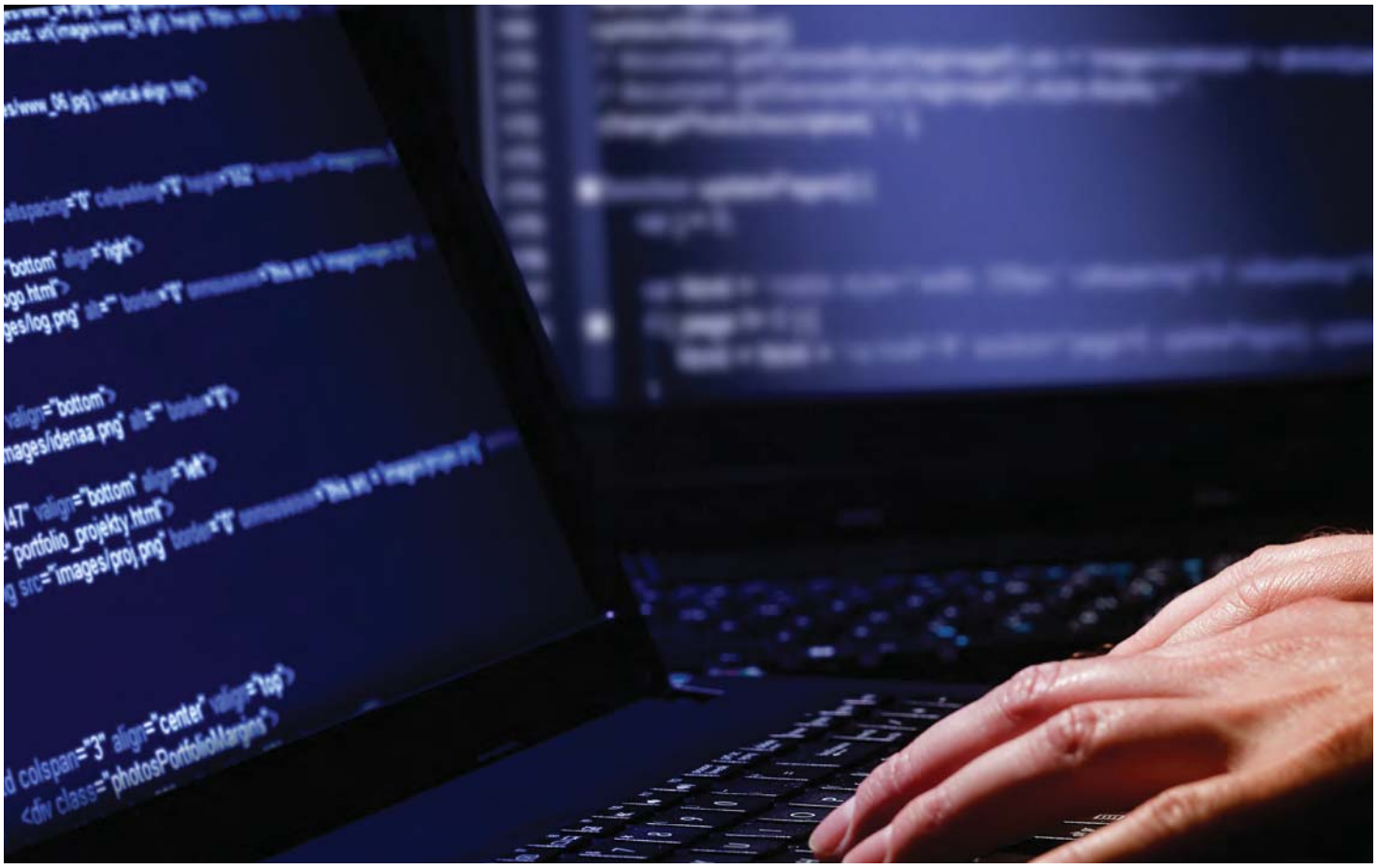
This course, founded on concept operations and real cyber capabilities, provides you with the understanding, tools, and processes needed to conduct malware analysis with real-world malicious code samples to dissect. You will prepare and plan an effective offensive and defensive strategy, as well as evaluate covert protocols. Analysis of system specific, non-descript tools will be introduced to aid in attack and defense.

CYBER ANALYST COURSE

This course presents analytical methodologies and information sources applicable to a cyber environment. Topics include interpreting analysis and forensic reports, Internet research, computer system and network analysis, log analysis, data-hiding techniques and intrusion identification. Provided with incident and technical reports, log files and access to online repositories, students conduct analysis and create analytical products, including a written report and a link analysis chart

Learning Objectives

- Review multiple reports containing relevant artifacts using basic cyber analysis techniques
- Analyze electronic artifacts in existing forensic and information reports
- Analyze basic data contained in text-based and binary logs
- Develop charts to visualize relevant data
- Develop information from Internet-based resources while maintaining anonymity
- Classify network intrusions and malicious code types
- Investigate network traffic and explain network monitoring concepts



CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS

An in-depth study of the theory and practice of digital forensics. Topics include computer forensics, network forensics, cell phone forensics, and other types of digital forensics. Discussion also covers identification, collection, acquisition, authentication, preservation, examination, analysis, and presentation of evidence for prosecution purposes.

Learning Objectives

At the end of this course, students should be able to:

- Identify the basic principles and tools used in computer forensics.
- Understand the main techniques used in data acquisition and analysis and in recovering image files.
- Critically evaluate the procedures in processing crime and incident scenes, especially on digital evidence controls, and in presenting digital evidence in court.
- Analyze the specific forensic techniques for Windows, Mac, Unix, and cell phone operating systems.
- Discuss the main issues and techniques associated with network forensics and malware investigation.
- Explain the issues, procedures and techniques used in contingency planning, cyber-attack recovery, and business continuity planning and execution.

CYBER ETHICS

Cyber Ethics is designed to teach students the proper techniques with which to approach the difficult ethical dilemmas that arise from using the modern Internet. In addition to providing students with the skills to assess future ethical dilemmas for themselves, Cyber Ethics also looks at some of the more pressing concerns related to Internet usage today.

Learning Objectives

The student will demonstrate an understanding of:

- The fundamental concepts, terms, and ideas required for an informed discussion on ethical topics
- A brief introduction to several commonly seen and referenced philosophies regarding ethics in general
- An overview of ethical business practices
- An intellectual object
- A review of current U.S. copyright law, how copyrights are obtained, other intellectual property issues; what an intellectual object is, how intellectual objects differ from traditional (physical) objects, and how those objects may be owned
- Explain the differences between those protections and copyrights
- Why professional codes of conduct are important for cybersecurity professionals
- Commonly used and invoked professional codes; employer/employee relationships and the impact those relationships have on the practice of 'whistle-blowing'; responsibility, accountability, and liability as they relate to professional codes of conduct
- Freedom of Speech on the Internet; issues surrounding speech on the Internet and the associated legal concerns; cyber-squatting, spam, and censorship; forms of speech that some argue are protected including pornography and hate speech; defamation on the Internet;
- Hacking, describing the two main categories of hackers, black hat hackers, their motivations, and their characteristics, 'white hat' hackers and key differences between white hat and black hat hackers; hacktivism, cybercrime, and cyberterrorism, and how those acts are similar and dissimilar.

CYBER FORENSICS: IDENTIFICATION, ACQUISITION, PROCESSING AND ANALYSIS OF DIGITAL EVIDENCE

The role and responsibility of a cyber-forensic investigator is to accurately report upon actions taken to expertly identify, extract, and analyze those data that will ultimately represent evidential matter as part of an investigation of an individual who is suspected of engaging in unauthorized activities. This hands-on workshop is designed specifically to provide the opportunity for participants to link theory and practice, resulting in a more comprehensive understanding of the science of cyber forensics, and how data become evidence.

Learning Objectives

- Understand the basics of a cyber-forensic investigation.
- Identify the various tools necessary for and use in a cyber-forensic investigation.
- Explain the process by which an image of the acquired data is obtained.
- Perform hands-on exercises in the imaging of potential evidential data.
- Discuss the processes involved in performing basic forensic analysis.
- Participate in a hands-on, basic forensic analysis lab exercise.
- Understand Windows XP Recycle Bin Basics.
- Explain RAM Slack and File Slack.
- Recognize GREP expressions and where to find data.
- Explain Registry Forensics.
- Determine the elements of a typical forensic report.
- Discuss the requirements of being an expert witness and court testimony.
- Perform hands-on exercises in Windows Recycle Bin and Registries.

CYBER INCIDENT ANALYSIS & RESPONSE

This course covers various incident analysis tools and techniques that support dynamic vulnerability analysis and elimination, intrusion detection, attack protection and network/resources repair. The student will be presented with real-world examples and scenarios to help provide knowledge, understanding, and capacity for effective cyber incident analysis and response.

Learning Objectives

- Students will demonstrate an understanding of background and concepts for cyber incident management, as well as an overview of the cyber incident management process.
- Topics include the types of cyber incidents, common forms of malware and attacks, an outline of the cyber incident management process, and common standards for cyber incident management.
- Students will demonstrate an understanding of the preparation phase of cyber security incident management.
- Topics include cyber incident management policies; services and procedures; the organizational structure, roles, and personnel; and cyber incident management training and awareness programs.
- Students will demonstrate an understanding of reactive cyber incident management activities. Some of these activities include monitoring, log management, detection, cyber incident triage, event scope and characteristics, incident investigation, impact and escalation, and cyber incident management software and services.
- Students will demonstrate an understanding of protecting and restoring systems that have been compromised by cyber security incidents including incident containment, identification, eradication, and recovery. The mitigation of specific common types of cyber incidents is also covered.
- Students will demonstrate an understanding of cyber incident proactive and post services, legal issues, and human resource issues.
- Some topics include attack categories, outcome discussions, vulnerability analysis, evidence and digital forensics, chain of custody, as well as training and skills for Computer Security Incident Response Team members.

CYBER INSIDER THREATS ANALYSIS

This course defines insider threat, examines relevant laws and regulations, and explores motivations and indicators of insider threat agents. The course looks at information sources that support investigations, such as system and network logs, detection tools, public records, and agency checks, and also covers tools used to analyze and evaluate information. Acquiring competency in the analytical process enables practitioners to identify probable cyber insider threat actors and develop strategies to mitigate or exploit the threat activity.

Learning Objectives

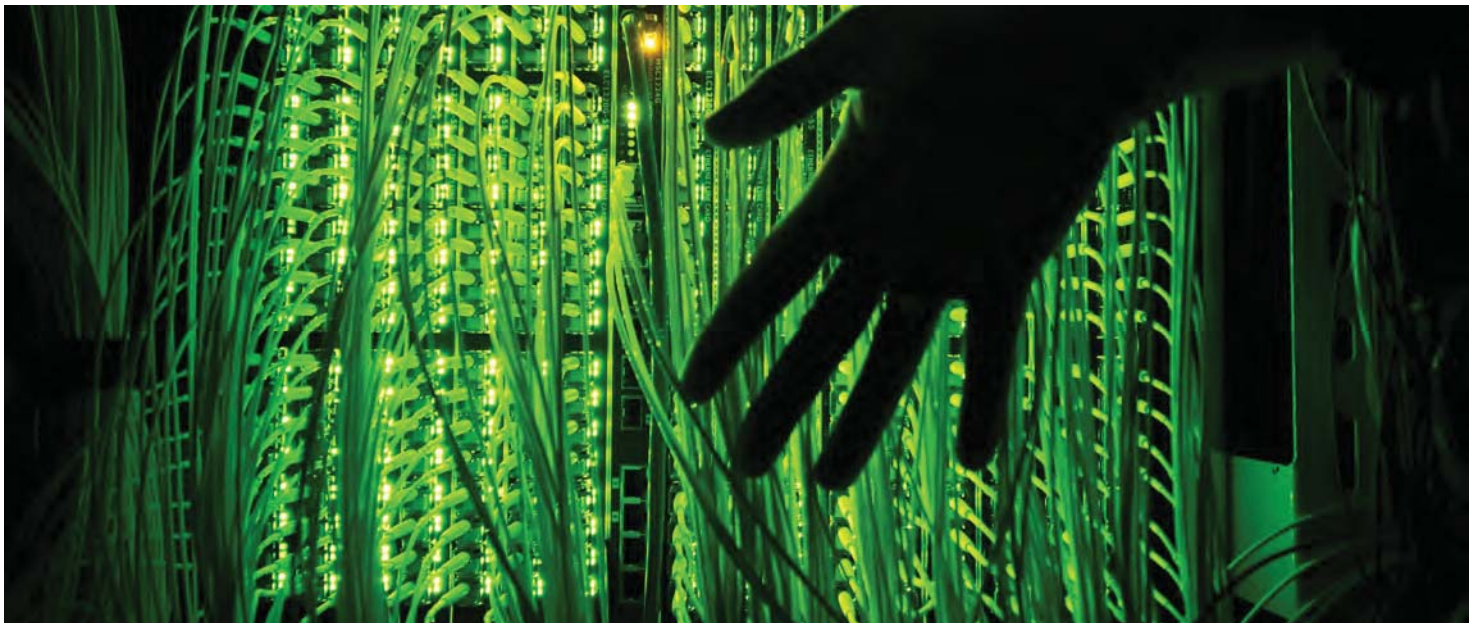
- Assess potential cyber insider threat activity
- Appraise collected data to differentiate relevant information from false positives
- Assess data to identify cyber insider threat activity

CYBER INTELLIGENCE (CYI)

This course examines the Cyber Leader's role in Cyber Intelligence from two perspectives: first, as an enabler of Cyber Intelligence through the acquisition and delivery of Strategic Information Technology (Strategic IT) systems supporting intelligence missions, processes, and functions across the Intelligence Community (IC); and, second, as a consumer of Cyber Intelligence products and services as part of planning and executing cyberspace-dependent operations.

Learning Objectives

- The course presents an overview of the IC's general roles and responsibilities, including the intelligence cycle in support of national security decision making, before analyzing Cyber Intelligence operational requirements, production, and services.
- Concludes with how to develop and implement appropriate Cyber Intelligence IT strategies and operational plans.



CYBER LAW & WHITE COLLAR CRIME

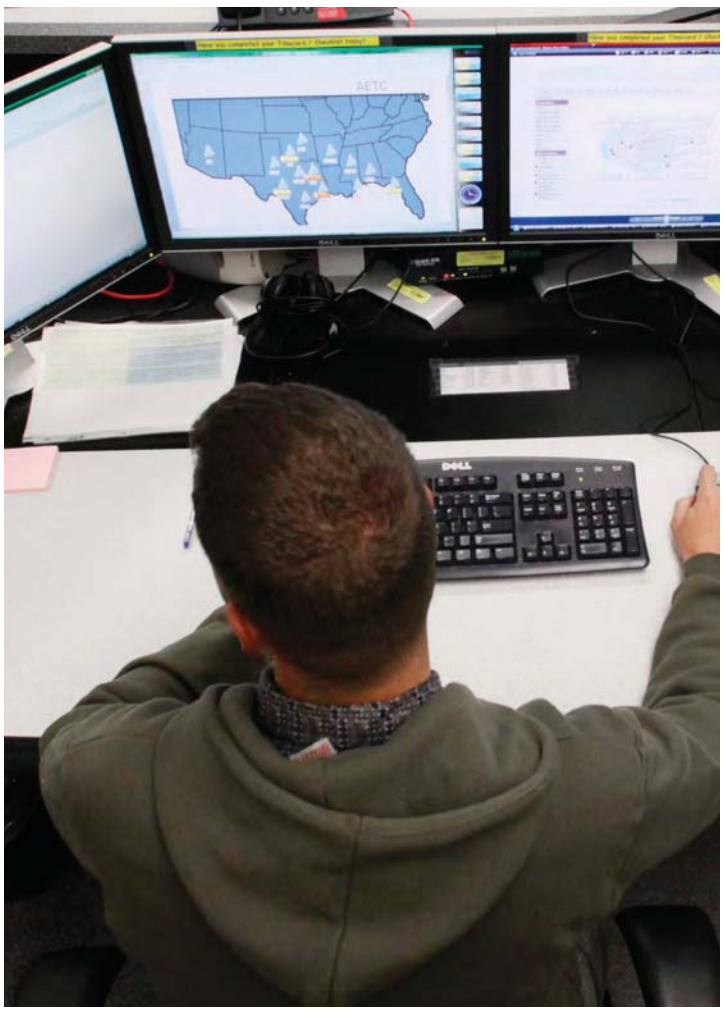
Cyber Law and White Collar Crime highlights the various computer crimes and appropriate response by first defenders and others that may encounter these types of issues. Participants learn legislations and organizational efforts to control or prevent such crimes. This course covers intellectual property law (copyright, trade secrets, unfair competition, and unfair business practices), personal jurisdiction, electronic commerce and software contracts, telecommunications, antitrust, privacy, the right to accuracy of information, the right to access to information.

CYBER LAW, REGULATIONS & ETHICS

Provides an overview of the ethical challenges faced by individuals and organizations in the information age and introduces the complex and dynamic state of the law as it applies to behavior in cyberspace. Topics include the legal pitfalls of doing business in an interconnected world and an introduction to the various organizations and materials that can be turned to for assistance in understanding how to ethically and legally provide services and operate modern computer-based systems and networks.

Learning Objectives

- Identify and apply the governance processes required of the statutes and regulations pertaining to information assurance.
- Analyze and evaluate proposed or extant information security policies, practices and procedures in order to assess, in concert with their organization's legal representatives and advisors, potential legal liabilities that might flow from implementing them.
- Use basic ethical theories to evaluate the fairness of a proposed or extant collection of policies, laws, regulations, guidelines and practices designed to mitigate the liability risks and punish the misuse of on-line systems.
- Identify the public policy issues and user expectations regarding privacy and apply privacy rules to management and operation of information infrastructures.
- Identify and apply the legal and regulatory compliance requirements pertaining to the acquisition, use and licensing of intellectual property. This includes the federal laws governing copyrights, patents and trade secrets, and both federal and state laws governing trade and service marks.
- Identify and apply the legal and regulatory compliance requirements pertaining to electronic commerce.
- Be able to explain the role of scientists and engineering expert witnesses in litigation.
- Develop legally sound information handling requirements for responding to subpoenas, discovery demands, and cyber-attack incident response processes and procedures.



CYBER OPERATIONS AND PLANNING

This course concentrates on providing cyber security specialists from various disciplines a baseline understanding across the major areas of cyber operations (network operations, defense, exploitation and attack) and planning. It will cover unclassified capabilities and techniques, tactics and procedures for effectively planning and operating in each of these areas. This course will also familiarize students with pertinent cyber laws and policies governing Private, MoD and Federal Agencies. This course will conclude with a cyber exercise in a virtual environment in which students will employ offensive and defensive cyberspace capabilities.

FOUNDATIONS OF INFORMATION SECURITY AND ASSURANCE

An overview of techniques for ensuring and managing information security. Topics include administrative and technical security controls to prevent, detect, respond to, and recover from cyber-attacks; risk and vulnerability analysis to select security controls; security planning; security architecture; security evaluation and assessment; and legal, ethical, and privacy aspects of information assurance. Discussion also covers information security fundamentals, such as cryptography, authentication, and access control techniques, and their use in network, operating system, database, and application layers. Security issues of current importance are stressed.

FOUNDATIONS OF INFORMATION SYSTEM SECURITY

A survey of various means of establishing and maintaining a practical cyber and information security program to protect key organizational assets. The aim is to develop an information security program that is aligned with organizational strategy and to evaluate and recommend information and security technologies to support the information security program. Discussion covers the integration of confidentiality, integrity, and availability into an organization's security program through the use of physical and logical security controls. Topics include data protection, telecommunications systems, applications, and emerging technologies. Threats and vulnerabilities are assessed to determine the level of risk.

FUNDAMENTAL FORENSICS FOR AUDITORS AND INFO SECURITY PROFESSIONALS

Traditional forensics professionals use fingerprints, DNA typing, and ballistics analysis to make their case. Infosec professionals have to develop new tools for collecting, examining and evaluating data in an effort to establish intent, culpability, motive, means, methods and loss resulting from e-crimes. This overview seminar will introduce the attendee to the broad field of cyber forensics and present the various tools and techniques designed to maintain control over organizational assets, digital or otherwise. This seminar covers computer forensics theory and methodology. It is not limited to the use of a specific software tool.

GLOBAL CYBERSECURITY

An in-depth study of cybersecurity from a global perspective. Topics include cyberterrorism, cybercrime, and cyberwarfare; the international legal environment; nation-and region-specific norms regarding privacy and intellectual property; international standard setting; effects on trade (including offshore outsourcing); and opportunities for international cooperation.

GOVERNANCE, RISK & COMPLIANCE IN CYBERSECURITY

Investigating external and internal threats that compromise data and digitized intellectual property. Implementing effective policies for mitigating risks and security and remediation measures in organizations.

HUMAN ASPECTS IN CYBERSECURITY: ETHICS, LEGAL ISSUES AND PSYCHOLOGY

An examination of the human aspects in cybersecurity. Topics include ethics, relevant laws, regulations, policies, standards, psychology, and hacker culture. Emphasis is on the human element and the motivations for cyber-crimes. Analysis covers techniques to prevent intrusions and attacks that threaten organizational data.

HOW TO THINK LIKE A CYBER ANALYST

This course will be a series of lectures covering specific skill sets an analyst must possess to be a successful analyst. Students will learn how their role as an analyst fits into the overall defensive strategy. They will learn how to react to incidents, how to report on incidents, who to inform of an attack or an impending attack and how to interact with law enforcement.

ICS/SCADA SECURITY ESSENTIALS

ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

IDENTITY MANAGEMENT TRAINING

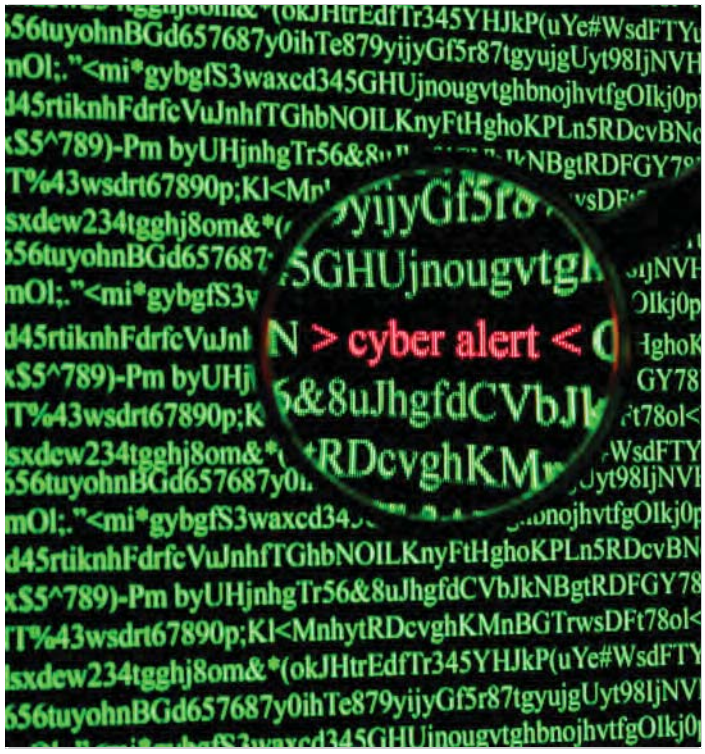
This course provides a comprehensive introduction to IM (and IAM) solutions that are increasingly being used to solve identity management security problems in authentication systems. Organizations today increasingly rely on services provided by the Internet and networked systems to conduct business, and for security are forced to authenticate multiple times to multiple authentication systems. At the same time, cyber-crime and security violations pose an ever-growing threat to business-critical functions and data. Single Sign-On (SSO), Public Key Infrastructure (PKI) and Federations, provide the overall security framework and tools for IM, enabling organizations to reduce security threats, safeguard sensitive data and maintain business continuity. Once implemented, IM can lower overall security costs and increase interoperability within and between various enterprise systems. This course presents the best and the most practical solutions and skills for creating your own IM strategy. By implementing the latest Microsoft PKI and Federation solutions, managers and administrators are able to select appropriate IM strategies for their organization, as well as provide SSO best practices for enterprise, BYOD mobile devices, and Azure and Amazon cloud applications. After participating in this course, attendees will be able to implement IM solutions in the specific context of their organization.

IMPLEMENTING NIST CYBERSECURITY FRAMEWORK USING COBIT 5

This course is focused on the NIST Cybersecurity Framework (CSF), its goals, the implementation steps and the ability to apply this information. The course and related exam are for individuals who have a basic understanding of both COBIT 5 and security concepts, and who are involved in improving the cybersecurity program for their enterprises.

Learning Objectives

- Apply the goals of the Cybersecurity Framework (CSF)
- Align to the content of the CSF
- Conduct the seven CSF implementation steps
- Apply and evaluate the implementation steps using COBIT5



INFORMATION SECURITY BASICS

Information Security Basics is designed to teach entry and mid-level IT staff the technological fundamentals of information security. The goal of this course is to provide students some preliminary knowledge of computer security to help in identifying and stopping various cyber threats. In addition to providing an introduction to information assurance, students will also learn general concepts (terminologies), an overview of TCP/IP, introductory network security, introductory operating system security, and basic cryptography.

INFORMATION SECURITY MANAGEMENT DOMAIN EXPERTISE: CYBER FORENSICS

Traditional forensics professionals use fingerprints, DNA typing, and ballistics analysis to make their case. Infosec professionals have to develop new tools for collecting, examining and evaluating data in an effort to establish intent, culpability, motive, means, methods and loss resulting from e-crimes. This overview seminar will introduce the attendee to the broad field of cyber forensics and present the various tools and techniques designed to maintain control over organizational assets, digital or otherwise. This seminar covers computer forensics theory and methodology. It is not limited to the use of a specific software tool.

INFOTECH COMPUTER FORENSICS AND ELECTRONICS DISCOVERY EL

The Computer Forensic and Electronic Discovery course is designed to train cybercrime investigators to furnish irrefutable burden of proof from a digital artifact. In taking this course you will learn electronic discovery, advanced investigation techniques, seizure concepts, forensic examination and much more.

INFOTECH COMPUTER HACKING FORENSICS INVESTIGATOR CLASS (EC COUNCIL)

The CHFI course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be taught during this course, including software, hardware and specialized techniques. The need for businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the "cyber-criminal." It is no longer a matter of "will your organization be comprised (hacked)?" but, rather, "when?" Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

INFOTECH SECURING CISCO NETWORKS WITH THREAT DETECTION & ANALYSIS

The Securing Cisco Networks with Threat Detection Analysis (SCYBER) course, version 1.0 is an instructor-led course offered by Learning Services High-Touch Delivery. The course combines lecture materials and hands-on labs throughout to make sure that you are able to successfully understand cyber security concepts and to recognize specific threats and attacks on your network. This course is designed to teach you how a network security operations center (SOC) works and how to begin to monitor, analyze, and respond to security threats within the network. The job role for a security analyst will vary from industry to industry and differ in the private sector versus the public sector.

INTERNATIONAL PERSPECTIVE ON CYBERSPACE (IPC)

This course provides an overview of the issues surrounding transnational cyberspace policies, international investment strategies, and implementation of information and communication technologies (ICT) that affect the global economy and transforms the flow of information across cultural and geographic boundaries.

INTRODUCTION TO CYBER INVESTIGATIONS

This online course prepares students to perform or support the role of case agent for basic cyber investigations. Students learn basic technical concepts and the legal framework that guides the conduct of cyber investigations. Major topics include an overview of cyber investigations, technical and legal fundamentals, special aspects of cyber case management (including online evidence collection) and subjects of cyber investigations.

INTRODUCTION TO CYBER NETWORK OPERATIONS

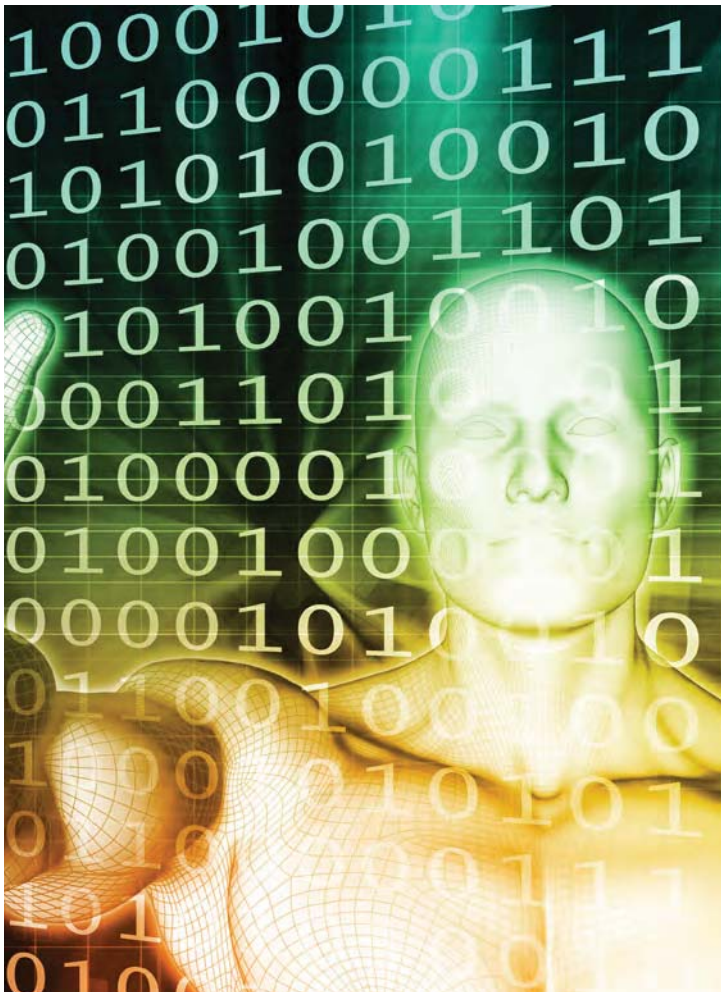
Full spectrum information superiority and dominance is key to influencing operations associated with war or Military Operations Other Than War (MOOTW). This survey of Computer Network Operations (CNO) introduces the concept of how Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE) are leveraged to collect information, disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks that host them. Strategic and operational considerations will be considered to affect an adversary's decision cycles with information superiority.

INTRODUCTION TO CYBER SECURITY FOR PRACTITIONERS

This course is an introduction to networking basics, cybercrime and security concepts. This instructor-led experience presents basic security procedures and challenges that arise in the workplace, and includes discussions of the various security threats and attacks to which today's computer users are vulnerable. The student learns how to address incident response and restrict site access, identify secure websites and establish security for a wireless network access point. Internet safety is a focus of the delivery, including topics such as, transacting business, communicating via instant messaging and using portable, wireless devices.

Learning Objectives

- Recognize and understand essential cyber security terms and concepts
- Identify and define risks, threats, and vulnerabilities
- Define cyber security implications for business, government and individuals



INTRODUCTION TO LEGAL AND ETHICAL ASPECTS OF CYBER SECURITY

Students will be introduced to the different aspects of how legal issues fall into their day to day roles. Students will identify what they can and can't do as it relates to tracking an attacker. Students will also distinguish how the nature of NSM has a fine line in the debate of individual privacy.

LAW OF DATA SECURITY AND INVESTIGATIONS

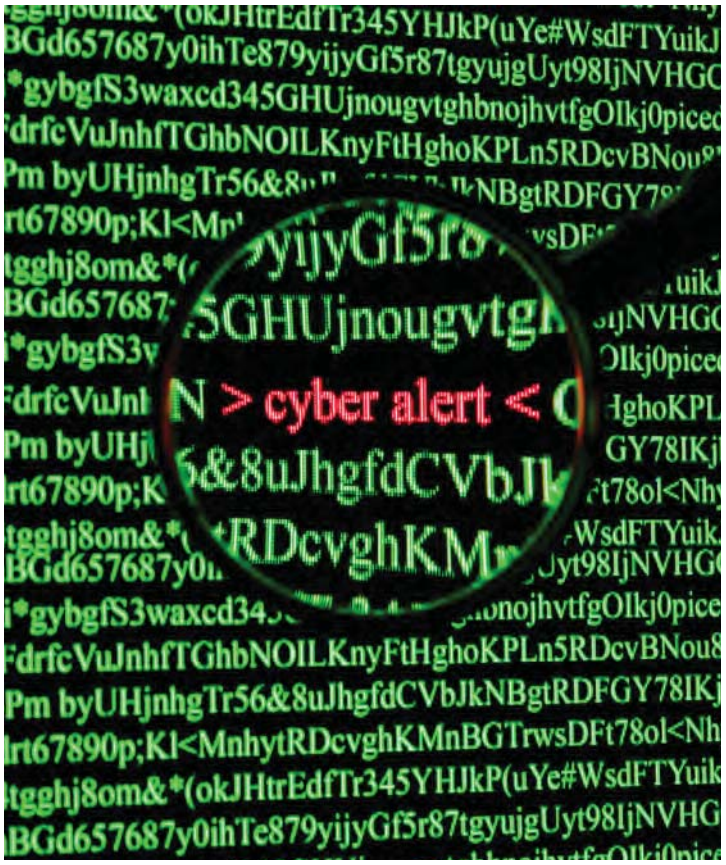
This course covers the law of business, contracts, fraud, crime, IT security, IT liability and IT policy, all with a focus on electronically stored and transmitted records. The course also teaches investigators how to prepare credible, defensible reports, whether for cyber, forensics, incident response, human resources or other investigations.

LINUX INTERMEDIATE FUNDAMENTALS (LIF)

This course teaches the core techniques, concepts and fundamentals of Linux system operation. Students acquire intermediate Linux command-line skills used in cyber investigation studies and real-world investigation and security. Students gain competency in functions relevant to standard Linux environments, including user and permission configuration and partition and file system manipulation.

Learning Objectives

- Describe the features of Linux that differentiate it from Microsoft Windows-based operating systems
- Manipulate Linux files and directories using common Linux commands
- Manipulate user and group accounts using common Linux commands
- Change Linux file system permissions using common Linux commands
- Create multiple file systems using common Linux commands
- Demonstrate how to mount file systems using common Linux commands
- Describe the characteristics of common Linux file systems



MANAGING CYBER INVESTIGATION UNITS

This online course prepares students to take on or support the role of manager of a cyber investigation unit (CIU). Major topics include establishing a cyber investigation unit, budgeting and procurement, personnel selection and managing investigations. Students learn how to establish a CIU on an organizational level and direct operational policies. The course explores requirements for personnel and facilities, and the importance of training to maintain consistent lab quality.

Learning Objectives

- Explain organizational needs specific to establishing a CIU
- Give examples of budgetary expenditures and concerns specific to cyber investigations
- Explain personality traits and skill sets to be considered for the recruitment and retention of CIU personnel
- Summarize how to manage a cyber investigation

CERTIFIED DIGITAL FORENSICS EXAMINER (CDFE)

The Certified Digital Forensics Examiner program is designed to train Cyber Crime and Fraud Investigators whereby participants are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation.

CERTIFIED PENETRATION TESTING CONSULTANT (CPTC)

The Certified Penetration Testing Consultant course is designed for cybersecurity Professionals and IT Network Administrators who are interested in conducting Penetration tests against large network infrastructures similar to large corporate networks, Services Providers and Telecommunication Companies. Instead of focusing on Operating System level penetration testing, this course covers techniques on how to attack and prevent underlying network infrastructure and protocols.

CERTIFIED SECURITY SENTINEL (CSS)

The Certified Security Sentinel training is intended for anyone that uses a computer on the internet. Attendees will fully understand the security threats that attack daily and they will also understand the countermeasures associated with these attacks. Students will learn that the weakest link in any security program is a poorly trained employee. Once a student understands what can happen, they will know what to look for and with these common sense tactics and be able to keep their computer as safe as possible.

The Social Engineering portion of the class is not specifically targeted to IT or security personnel alone but rather is designed to teach the participants the skills used by Social Engineers to facilitate the extraction of information from an organization using technical and non-technical methods.

INFORMATION SYSTEMS 20 CONTROLS (IS20)

IS 20 Controls course covers proven controls and methodologies that are used to execute and analyze the Top Twenty Most Critical Security Controls. This course allows the security professional to see how to implement controls in their existing network(s) though highly effective and economical automation. For management, this training is the best way to distinguish how you will assess whether these security controls are effectively being administered.

MOBILE DEVICE FORENSICS

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The scope of devices can include mobile phones and any digital device that has both internal memory and communication ability such including PDA and GPS devices and tablet computers. This course focuses on the forensic study of mobile devices due to the rapid proliferation of smartphones and applications such as contacts, photos, calendars and notes, SMS and MMS messages, video, email, web browsing information, location information, and social networking. This increased usage has also seen a marked increase in cybercrime involving smartphones. Students will learn how to perform the forensic examination of mobile devices using the most advanced tools available.

MOBILE DEVICE INVESTIGATIONS PROGRAM

Provide Law Enforcement personnel with tools for investigating cyber-crime related activities.

MONITORING, AUDITING, INTRUSION DETECTION, INTRUSION PREVENTION, AND PENETRATION TESTING

An in-depth study of the theory and practice of intrusion detection and prevention in cyberspace. Topics include network security, monitoring, auditing, intrusion detection, intrusion prevention, and ethical penetration testing. Emphasis is on methods to identify system vulnerabilities and threats and prevent attacks.

NETWORK AND PACKET ANALYSIS

This course provides the student the concepts, methodologies, and hands-on tools to analyze network traffic for the purposes of focused operations, cyber operations, pen testing, intrusion detection, and incident response. Each student will be provided an overview on how packet analysis applies to their cyber security position. This course will provide an overview of the TCP/IP Stack to include UDP as it relates to architecture but also includes how packet analysis can identify and create network based attacks. Students will learn how to use TCP Dump, T-Shark, and will be given an overview of commercial tools to conduct analysis.

NETWORK SECURITY ESSENTIALS

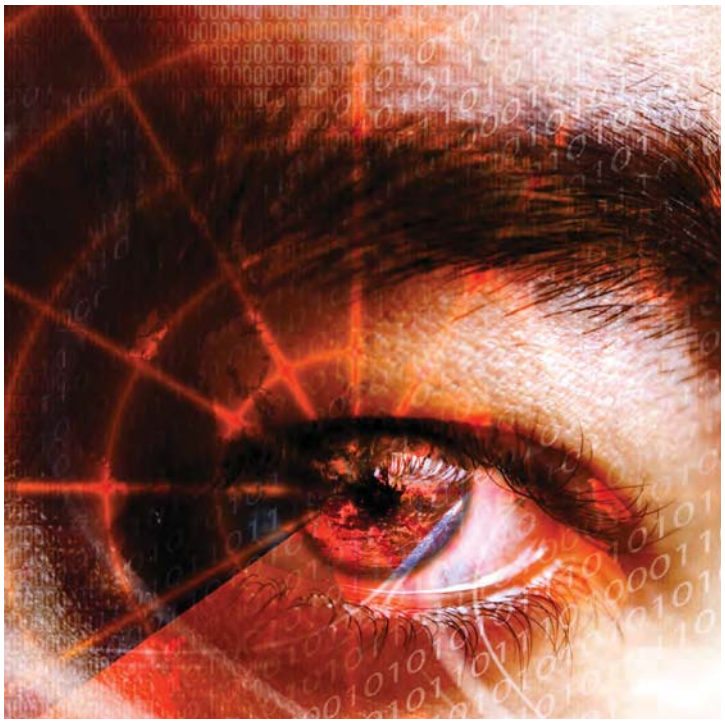
Learn the basics of network security, such as TCP/IP protocols and applications, network threats, vulnerable points of access, and network security management concepts and techniques.

ON-LINE UNDERCOVER TECHNIQUES

This course provides investigators with the foundational knowledge and skills needed to successfully operate in cyberspace while maintaining the integrity of their investigations and operations. Students learn how to construct an online undercover persona, operate a persona, and investigate a persona. This course is designed for those involved in counterintelligence or criminal investigations.

Learning Objectives

- Construct an online undercover persona
- Optimize and operate an undercover persona in cyberspace
- Investigate a cyber persona



OPEN SOURCE INFORMATION COLLECTION AND ANALYSIS FOR CYBER DEFENSE AND OFFENSE

This course introduces students to collection and analysis of open source and publicly available information, white hacking techniques for stealth collection, methodology for evaluation and validation of sources of open and publicly available information, and OSINT best practices. The course also addresses the ethical and legal aspects associated with activities conducted in the cyberspace domain.

OVERSIGHT OF INFORMATION SYSTEM SECURITY AND CYBERSECURITY

This course will explore the role of the non-technical DoD security specialist related to information systems security, information assurance and cybersecurity. Emphasis will be placed on developing effective relationships between the many organizational players who have a role in information systems security, information assurance and cybersecurity and how these relationships serve to increase operational effectiveness and security of the organization.

The course will include the following topics:

- Links between Information Systems Security, Information Assurance, Cybersecurity and other security disciplines.
- Three Elements of Information Systems Security (CIA)

  1. Confidentiality
  2. Integrity
  3. Availability

- Six elements of an Information System:

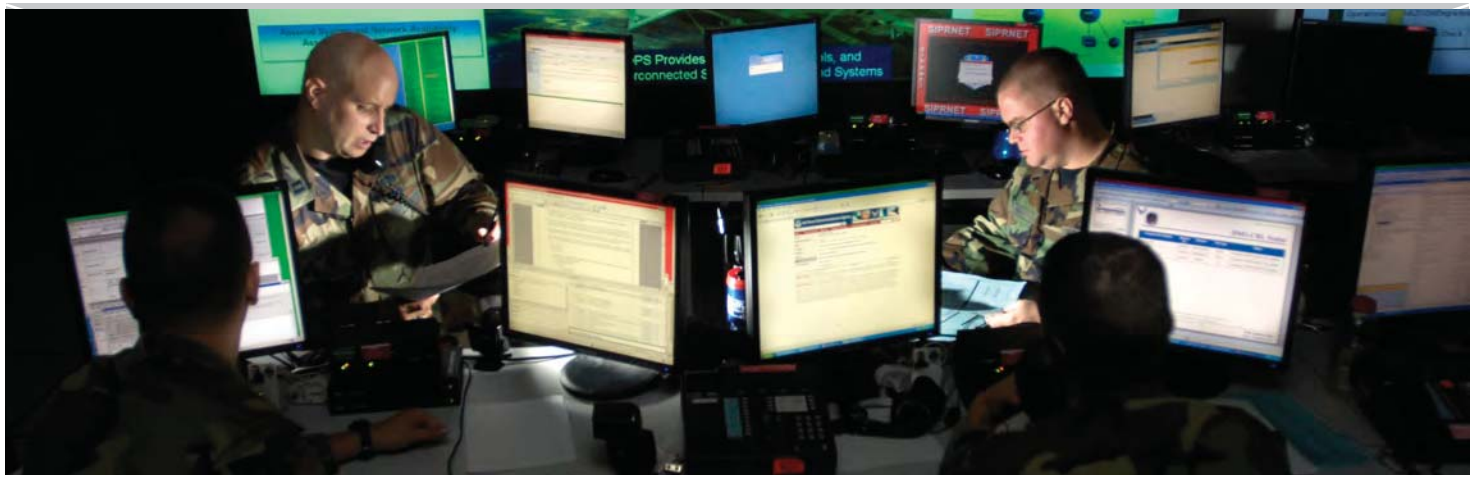
  1. Hardware
  2. Software
  3. Data
  4. Procedures
  5. People
  6. Communication

PRACTICAL APPLICATIONS IN CYBERSECURITY MANAGEMENT

A study of cybersecurity that integrates knowledge gained through previous coursework and experience and builds on that conceptual foundation through integrative analysis, practical application, and critical thinking. The goal is to protect an organization's critical information and assets by ethically integrating cybersecurity best practices and risk management throughout an enterprise. Emerging issues in cybersecurity are considered.

PRINCIPLES OF CYBER SECURITY

This class explores the overarching security architectures and vectors of information assurance from a management perspective to allow the learner to formulate the basis for sound business decisions. Students gain an appreciation for systems, networks, processes, methodologies, documentation requirements, recovery processes, certification and accreditation processes as well as “best practice” implementation, training and continuous improvement. Discussions in this course give the correct acumen of personnel security, physical security, and technical operational security as these principles relate and interface with information security principles. Defense-in-depth principles also are covered for designing proper physical security programs. At the completion of the course students should be able to manage an IA function and evaluate an organization’s Contingency Planning process for adequacy.



PYTHON FOR CYBER SECURITY PROFESSIONALS

This hands-on course will provide students demos and lessons on Python basics and walk through labs portraying the usefulness Python has in a variety of information security areas. Students will have guided instruction and walk through programming in Python. Each lab builds upon the next allowing for guided instruction.

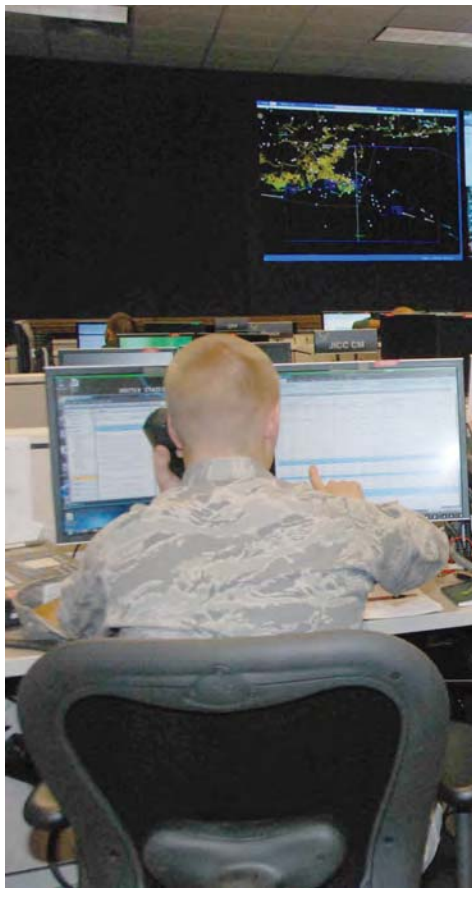
Learning Objectives

- Introduction to Python Concepts
- Advance Further into Python
- Web Recon
- Port Scanning
- Packet Sniffing
- TCP Packet Injection
- Perform forensic analysis
- Perform malware analysis

RISK MANAGEMENT WHEN ONLINE

This course introduces students to operational security practices in the cyberspace domain; securing cyber technology such as iPads, smartphones, laptops, and desktops to keep these devices from broadcasting the user's activities and patterns of interaction in the cyberspace domain; understanding social engineering methods and awareness on how to prevent becoming the victim of a phishing and/or social engineering attempt; best practices for interacting with social media platforms; and best practices to surf the World Wide Web without leaving footprints that can be used to compromise your private life and your enterprise. The course also addresses the ethical and legal aspects associated with activities conducted in the cyberspace domain.

RMF FOR DOD IT INTENSITY



This course provides a practical overview of the transition to the RMF for DOD IT process for system authorization. Although primarily oriented toward the DoD audience, the strategies, methodologies, and technical security countermeasures presented in this course are equally applicable to any commercial organization endeavoring to enhance their overall cybersecurity posture through effective validation testing of security countermeasures.

Learning Objectives

- Describe the goals of the transformation process
- Recognize how the process will align with NIST and the Federal government
- Identify key Federal laws, NIST publications and DOD Policies
- Recall key terminology and definitions
- Understand the key concepts of the RMF
- Discuss the six steps of the RMF
- Apply of the RMF to DOD information systems
- Identify the purpose and uses of the Knowledge Service
- Use eMASS for system registration and authorization
- Understand the situation and applicability to external parties
- Know the protection requirements for unclassified and classified information
- Demonstrate basic operations of various tools used for certification testing

SECURING SMARTPHONES WITH MOBILE APPS

This course provides an introduction to essential techniques to protect mobile devices from attack via application weaknesses. Attendees examine real cyber-attacks and application-level countermeasures against them.

SECURING WEB APPLICATIONS

This course explores risk management in Web applications, identifying and classifying weaknesses, and strategies for developing secure Web applications. The Internet is an integral part of most organizations today, but this widely used public network is also the source of data theft, cyberstalking, and many other threats. Organizations with a significant Web presence, such as e-commerce sites, must ensure their Web applications are as secure as possible. This Web-based course is designed for IT professionals who manage Web servers or are involved with application development projects.

SECURING WEB APPLICATIONS, SERVICES, AND SERVERS

Organizations today increasingly rely on the Internet and networked systems to conduct business. At the same time, cyber-crime and security violations pose an ever-growing threat to business-critical functions and data. If Web applications are not enabled with the appropriate security countermeasures, third parties are able to eavesdrop and compromise the integrity of information passed to and from your Web applications. For organizations that share proprietary data across the Internet, intranets or other public networks, this is of particular concern. This course systematically exposes potential security threats, provides proven solutions and shows you the steps you can take today to help ensure the integrity and privacy of your Web applications. Special attention is paid to the Open Web Application Security Project (OWASP) Top Ten security issues.

Learning Objectives

- Implement and test secure web applications in your organization
- Identify, diagnose and remediate the OWASP top ten web application security risks
- Configure a web server to encrypt web traffic with HTTPS
- Protect Ajax–powered applications and prevent JSON data theft
- Secure XML web services with WS–Security

SECURITY ESSENTIALS BOOTCAMP STYLE

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

SECURITY POLICY ANALYSIS

A study of various aspects of information assurance and cybersecurity policy planning in an organizational context. The aim is to examine key analysis procedures, such as security requirements analysis and risk assessments, to determine their roles in policy formation. Topics include the impact of current legislation, judicial decisions, and government regulations directing the focus of policy formulation. Projects include generating an information security profile for an organization.

SECURITY PROGRAM MANAGEMENT 101

This course teaches individuals the skills to oversee and manage information security program implementation within the organization or other area of responsibility. These responsibilities include: manage strategy, personnel, infrastructure, policy enforcement, emergency planning, security...

SECURITY RISK MANAGEMENT

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The scope of devices can include mobile phones and any digital device that has both internal memory and communication ability such including PDA and GPS devices and tablet computers. This course focuses on the forensic study of mobile devices due to the rapid proliferation of smartphones and applications such as contacts, photos, calendars and notes, SMS and MMS messages, video, email, web browsing information, location information, and social networking. This increased usage has also seen a marked increase in cybercrime involving smartphones. Students will learn how to perform the forensic examination of mobile devices using the most advanced tools available.

Learning Objectives

- Understand and be able to articulate the Risk Management process, including the need for identification of threats, vulnerabilities, and safeguards, and for testing the effectiveness of those safeguards.
- Understand the need for effective Information Technology Risk Management policy, standards, guidance, and procedures within organizations, today.
- Understand the need, uses, and content of a System Security Plan and Risk Assessment within the quantitative and qualitative analysis paradigms.
- Given an organizational scenario, be able to develop a detailed Risk Assessment.
- Given an organizational scenario, identify security policy and enforcement needs and be able to develop those needs into policy or procedures.
- Be able to create and execute effective questions and scenario processes for testing to determine the effectiveness of security controls related to the confidentiality, integrity, and availability of system/network assets in support of risk management.
- Given a series of identified network security safeguards, be able to devise effective and comprehensive Security Test and Evaluation tests.
- Given a series of network vulnerabilities, determine and justify application of cost-effective countermeasures.
- Given a network scenario be able to identify and argue the best long-term contingency planning solution.
- Given an organizational network scenario, be able to design an effective disaster recovery and testing process.

SIMPLIFYING SECURITY IN THE CYBER AGE

This continuing education course is designed for individuals pursuing professional development training in cybersecurity awareness. This course simplifies security in the cyber age for the everyday technology user by breaking the foundations of cybersecurity awareness down into easy to understand...

STARTER GUIDE TO CYBER SECURITY

This course is about establishing security in your environment. It is appropriate for managers in new positions, as well as those starting new groups and organizations. Security must begin somewhere, and the lessons of this course focus on assessing an environment, identifying needs and deficits...

STRATEGIES FOR ASSURING CYBER SUPPLY CHAIN SECURITY (SAC)

This course explores the strategies necessary to manage global supply chain risk within the Department of Defense and across the federal government.

SYSTEM AND NETWORK SECURITY INTRODUCTION

Organizations today increasingly rely on the Internet and networked systems to conduct business. At the same time, cyber-crime and security violations pose an ever-growing threat to business-critical functions and data. To mitigate security threats, safeguard sensitive data and maintain business continuity, it is essential that computers and networks be protected. In this course, you gain the knowledge and skills to effectively and accurately analyze the security risks to your computer and network systems. You also learn how to view security from the standpoint of the attacker, enabling a more successful implementation of Internet and system defenses. The issues of authentication, confidentiality, integrity, and availability form the core of the necessary analysis. Whatever your business environment, there are steps you can take today to help ensure the integrity and confidentiality of your data.

TERRORISM AND CRIME IN CYBERSPACE (TCC)

This course explores the nature of conflict in the cyber realm by focusing on two major Internet-based threats to U.S. national security: cyber terrorism and cyber crime.

UNDERSTANDING CYBERCRIME & IMPLEMENTING MITIGATING COUNTERMEASURES

Examines the ever changing, fast pace technology in relation to cybercrimes and cyber terrorism. Students will explore the threats of cybercrime, bullying, and terrorism and the mitigating countermeasures used against such threats. The course will also include the review and analysis of current cyber policy issues in both the public and private sectors.

Learning Objectives

- Understand cyber threat attack analysis, manage countermeasures, and mitigate risks of such threats and attacks.
- Understanding attacks on corporate and private industry IT enterprise and manipulation of their IT systems.
- Understanding the differences between criminal activity and cyber terrorism.
- Understanding and mitigating attacks on the US information infrastructure.
- Understanding and mitigating attacks on foreign country's national information networks.
- Creating Cyber Crime and Terrorism Threat and Risk Assessments and Mitigation Plans

CYBER WARFARE INSTRUCTORS