Carmel
Trainings & Deployments

CTR-902 Introduction to Cyber Warfare

About this course

This is a 40-hours course aimed at teaching students about cyber conflicts, which are global issues that, by definition, cut across national borders. Information security threats are widespread, persistent, and becoming more complex. By the end of the course, students will be able to apply what they've learned about cyberwarfare analysis and management. You'll have a firm grasp on cyberwarfare discussions, threats, motivations, and the significance of cyberspace peace. This course is intended to keep students up to date on current events while also encouraging meaningful dialogues among a variety of people. The practical repercussions of cyberwarfare and penalties will be highlighted in this course.

Audience profile

This course is for anybody interested in cyber security, such as cyber security professionals, system administrators, cyber security managers, cyber security auditors, and Chief Information Officers (CIOs).

At course completion

After completing this course, students will be able to:

- Debate the impact of combat in cyberspace after completing the course.
- Discuss both defensive and offensive aspects of network security, information assurance, intelligence, cryptology, and infrastructure protection.
- Identify and explain measures made to disrupt, deny, degrade, or destroy information in computers and computer networks using computer networks.
- Identify and describe the steps taken to safeguard information systems and computer networks by monitoring, analyzing, detecting, and responding to unauthorized behavior.
- Describe how to use computer networks to allow intelligence gathering capabilities from target or enemy automated information systems or networks.
- Examine cyber-related decisions from social, ethical, legal, and political perspectives as they relate to national and military strategy.
- Look into and assess national cyber-warfare actions.

Course details

Module 1: Introduction to Cyberwarfare

This module will teach you all you need to know about cyberwarfare. This programmer looks at cyber warfare from a variety of perspectives, including military, social, and scientific. You'll study how cyber-warfare has been utilized in the past, why various people rely on it, and how to defend against it.

Module 2: Controversy of Definition

This module is about the long-running public controversy or passionate discussion of opposing viewpoints and arguments surrounding the term "cyber warfare." This session delves into the debates around the idea of cyberwarfare. Digital attacks against an adversary state, which may disrupt actual warfare and vital computer systems, as well as actions by a nation-state or international organization attacking and attempting to damage another nation's computers or information networks, such as through computer viruses or denial-of-service attacks.

Module 3: Cyber Warfare and Cyber Sanctions

The goal of this course is to teach you about cyber warfare and cyber penalties. This module covers the employment of digital assaults, as defined by the cyberwarfare concept, as well as the retaliatory response to such attacks. As a result, you'll have a greater knowledge of how governments might utilize cyber sanctions as a response to being cyber-attack targets. It also examines how economic penalties, both unilateral and multilateral, can be utilized instead of cyberwarfare.

Module 4: Threats to the 4th Domain

This module focuses on computer systems, networks, and infrastructure targets. You'll learn about the ubiquitous use of information technology, the robustness and security of these systems, which are vital to a variety of infrastructure systems, as well as the resilience of industry, the military, society, and the community. You'll also learn how security changes, how attackers devise new ways to get into information technology systems, and how they gain access to sensitive data inside a domain.

Module 5: Types of Warfare

This module gives an overview of the many risks that a nation's cyberspace faces. At the most basic level, you'll learn how cyber-attacks may be utilized to help traditional combat. This module covers "hard" threats such as espionage and propaganda, as well as "soft" threats such as espionage.

Module 6: Motivation and Preparedness

This module educates students about the numerous risk-free possibilities for weakening offensive cyber operations while raising a nation's chances of surviving against cyber-attacks, as well as how to exercise and explore a variety of techniques in their cyber defense. This session covers a wide range of topics, including military, civil, hacktivism, income generating, private sector, and non-profit research.

Module 7: Nation-State Cyber Activities

This module will teach you how nation states use cyberspace to launch assaults to obtain strategic benefits for their nations, including how attacks may be carried out by interrupting target country activities, gathering cyber information, stealing secrets, or performing reconnaissance. You'll also learn about the various ways used by different countries to carry out cyber-attacks.

Module 8: Understanding Cyber Peace & Diplomacy

This module describes how to negotiate with state representatives to construct a global cyberspace order. In addition, this module provides an overview of many talks that have been made, as well as whether the concerned countries followed the rules and their present status of cyber warfare.

Module 9: Responsible behavior of cyberspace

This module will explore how security concepts should be applied to cyberspace, what constitutes the expected behavior of Nations in cyberspace, the role of private sector and civil society in fostering responsible behavior in cyberspace.

Module 10: Understanding Nations' Cyber Power and Capability

In this module, you will study about the effect and capabilities of important nations in cyberspace in this module. You'll learn about the personnel, technology, and organizational characteristics that combine to allow offensive cyber operations, as well as the rankings of various nations' cyber capabilities.

Prerequisites

- Level test - American test
- A basic understanding of using operating systems, networks, and the Internet. Be able to download and install software. A willingness to learn.
- Basic knowledge of Information Technology
- Strong analytical abilities and a strong eye for data patterns are required.
- Foundational knowledge about how to practice cybersecurity in the real world