## Purpose

This project provides you an opportunity to create a cyberwarfare defense plan that incorporates many of the concepts learned in this course.

## Required Source Information and Tools

**Web References:** Links to web references in this class related materials are subject to change. These links were last verified on August 19, 2022.

The following tools and resources will be needed to complete this project:

* A web browser and access to the Internet to perform research for the project
* Microsoft Word (or compatible) and Microsoft PowerPoint (or compatible)

(Optional) A tool for creating basic network diagrams, such as draw.io or Microsoft PowerPoint

## Learning Objectives and Outcomes

## At the end of this course you will be able to:

* Describe security issues within a supply chain.
* Identify the most likely cyber threat to a critical infrastructure and apply the Cyber Kill Chain.
* Apply the Adversary Model to a cyberattack group.
* Ensure defense in depth of a network and its underlying computers, devices, and data.
* Outline mission assurance processes for a critical infrastructure.

Identify relevant industrial control systems (ICSs), network defense technologies, and network operational procedures.

## Overall Project Scenario

## You are a security analyst that’s part of the security team at Red Cell 637 Defense, a U.S. Department of Defense (DoD) contractor specializing in cyber operations and defensive strategies.

## Your team has been informed by high-ranking officials that a foreign, government-based cyberattack group is suspected of hacking into computers that operate the U.S. Western Interconnection power grid to probe and map the network. Group members most likely originate from Russia, are well-funded and well-equipped, and are capable of a large-scale attack. The officials have intelligence that indicates the group may be planning to install malicious software within the grid’s computer network to, at some point, disrupt power to 11 states.

## To prepare for a possible attack on U.S. critical infrastructures, your team has been tasked with providing important parts of an overall cyberwarfare defense plan. Your company will work closely with the DoD and the North American Electric Reliability Corp to provide a plan that ensures the security and safety of the Western Interconnection power grid computer network.

## Deliverables

The project is divided into several parts. Details for each deliverable can be found in this document. Refer to the course Syllabus for submission dates.

* Project Part 1: Identifying Supply Chain Security Management Issues and Sources of Threat Information
* Project Part 2: Identifying Cyber Threats and Applying the Cyber Kill Chain
* Project Part 3: Ensuring Defense in Depth
* Project Part 4: Examining Mission Assurance and Operational Procedures

Project Part 5: Presentation to the DoD CIO

By the end of the course, you are expected to submit a presentation, such as a PowerPoint deck, to be presented to the DoD chief information officer (CIO) for this project and selected technology staff. The presentation will describe the overall scope of the project and address all major tasks in each part of the project.

## Project Part 1: Identifying Supply Chain Security Management Issues and Sources of Threat Information

#### Scenario

The Western Interconnection is a major power grid made up of electricity generators, or utilities, tied together to create the grid. The utilities can be thought of as the supply chain to the grid. Because the power grid is a critical infrastructure, it is imperative that the utilities are able to securely operate their technical infrastructures to avoid the collapse of the power grid.

#### Tasks

For this part of the project, perform the following tasks:

1. Perform research and write a report that:
2. Describes at three supply chain security management issues that could affect electricity generators and then the power grid overall
3. Includes a list of five information sources and their URLs (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, and so on) that would help grid operators maintain currency of computer network defense threat conditions and determine which security issues may have an impact on the power grid network
4. Cite sources, where appropriate.

#### Required Resources

* Internet access

Course textbook

#### Submission Requirements

* Format: Microsoft Word (or compatible)
* Font: Arial, 12-point, double-space
* Citation style: Your school’s preferred style guide

Length of report: 2–3 pages

#### Self-Assessment Checklist

* I performed research and write a report that:
  + Describes at three supply chain security management issues that could affect electricity generators and then the power grid overall, such as security problems that can arise
  + Includes a list of five information sources and their URLs that would help grid operators maintain currency of computer network defense threat conditions and determine which security issues may have an impact on the power grid network
* I created a professional, well-developed report with proper documentation, grammar, spelling, and punctuation.
* I followed the submission guidelines.

## Project Part 2: Identifying Cyber Threats and Applying the Cyber Kill Chain

#### Scenario

The DoD has requested a review of the vulnerabilities of the Western Interconnection power grid computer network, with strategies for reducing or eliminating the vulnerabilities. They also want a brief profile of the cyberattackers, using the Adversary Model as a foundation. You will need to research this model, which focuses on resources, capabilities, intent, motivation, risk aversion, and access.

#### Tasks

For this part of the project, perform the following tasks:

1. Perform research and write a report that:
2. Identifies and describes a specific type of malware that could affect the Western Interconnection power grid computer network. Explain how the malware could be installed in the network covertly, and the action the malware would take to disrupt the network.
3. Applies the Cyber Kill Chain to the identified malware, including a diagram that shows the steps to be taken to eradicate it
4. Applies the Adversary Model to the cyberattack group
5. Cite sources, where appropriate.

#### Required Resources

* Internet access

Course textbook

#### Suggested Resource(s) for the Adversary Model

https://www.networkworld.com/article/2227798/the-cold-war--then-and-now.html

#### Submission Requirements

* Format: Microsoft Word (or compatible)
* Font: Arial, 12-point, double-space
* Citation style: Your school’s preferred style guide

Length of report: 2–4 pages

#### Self-Assessment Checklist

* I conducted adequate independent research for this part of the project.
* I wrote a report that:
  + Identifies and describes a specific type of malware, explains how the malware could be installed in the power grid network covertly, and describes the action the malware would take to disrupt the network.
  + Applies the Cyber Kill Chain to the identified malware and includes a diagram that shows the steps to be taken to eradicate the malware
  + Applies the Adversary Model to the cyberattack group
* I created a professional, well-developed report with proper documentation, grammar, spelling, and punctuation.

I followed the submission guidelines.