Cyber warfare Defense Plan. Paper details Purpose This project provides you an opportunity to create a cyberwarfare defense plan that incorporates many of the concepts learned in this course. To complete the project, you will need a computer with: • Access to the Internet • Microsoft Word, Microsoft PowerPoint, and Microsoft Visio, or compatible editing, presentation, and drawing software Learning Objectives and Outcomes You will be able to: • Identify the most likely cyber threat to a critical infrastructure and apply the Cyber Kill Chain • 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 Deliverables The project is divided into three parts, as follows: • Project Part 1: Identifying Cyber Threats and Applying the Cyber Kill Chain • Project Part 2: Ensuring Defense in Depth • Project Part 3: Examining Mission Assurance and Operational Procedures By the end of the course, you are expected to submit a final project report and a project presentation. The electronic presentation, such as Microsoft PowerPoint, is to be presented to the Department of Defense (DoD) chief information officer (CIO) for this project and selected technology staff. The report and presentation will describe the overall scope of the project and address all major tasks as assigned in each part of the project. Final Project Report Submission Requirements • Format: Microsoft Word or compatible • Font: Arial, 12-point, double-space • Citation Style: Follow your school’s preferred style guide • Length: 8–10 pages, including an executive summary Project Presentation Submission Requirements • Format: Microsoft PowerPoint or compatible • Slide Titles: Arial font, 40-point • Slide Body Text: Arial font, 22- to 30-point bullet points; include SmartArt or similar illustrations on at least one-third of the content slides • Citation Style: Follow your school’s preferred style guide • Length: 12–15 slides, including a title slide and a summary slide Introduction You are a security analyst that’s part of the security team at Red Cell 637 Defense, a 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 three 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. Project Part 1: 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. Tasks Write a report that: • 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. • Applies the Cyber Kill Chain to the identified malware, including a diagram that shows the steps to be taken to eradicate it.