Lesson 5: Cyber Warfare

High School Cybersecurity Unit: CyberEthics, the Moral Quarrel

Lesson Overview	Career Highlight
In Lesson 1, we explored how communication and technologies advanced from physical hieroglyphics to electronic files and how more intensive codes and code breaking skills evolved to compete with opposing civilizations. Power struggles have always been tense between civilizations. Wars have erupted, disrupting lives, homes, economies, and changing history. For the most part, we can visualize war in the sense of tangible destructive forces; bombs, tanks, and explosions. But, what if a threat isn't tangible, but hidden in codes, networks, and wires? Imagine if entire cities lost power, bank accounts were frozen, and factories/airports/hospitals could be shut down all with the push of a button. This scenario is very possible and could be an attack from another country as a form of cyber war. The threat of hacking has gone beyond vandalism and criminal activities and become physical real-world disruptions that were once only possible by military attacks. Currently, cyber war attacks have caused over $10 billion in economic damage. In this lesson, students will explore examples of countries engaging in cyber warfare and engage in activities to understand the role the military plays in protecting the United States from cyberattacks.	Cybersecurity Specialist: Responsible for protecting networks against cyberattacks from enemy forces by monitoring, analyzing, detecting, and responding to unauthorized cyber activity.

STEM Course Connections	Timing
Computer Science Biology Chemistry Physics Earth Science Integrated Science Other: English, History, Sociology, Psychology, Anthropology	Four class sessions of 45 minutes each

Engineering Activity	
Science and Engineering Practice #	Obtaining, Evaluating, and Communicating Information

Essential Questions

- What is cyber warfare?
- How does the military help defend the United States in cyber warfare?

Lesson Objectives

Learning Goals:

- Students will analyze and categorize various examples of cyberattacks
- Students will design secure server environments that would best prevent cyberattacks
- Students will evaluate attempts to access a system to decide if the attempt is legitimate or a cyberattack

Materials

All materials in Student Handouts, unless otherwise noted.

- Estonia's Impact on Cyber War (answer key)
- Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations
- Cyber Challenge (answer key)
- Careers in Cybersecurity
- Cyber Warfare Case Studies
- Cybersecurity Wiki Outline

Teacher Note: The University of Texas at San Antonio's Center for Infrastructure Assurance and Security created the Cyber Threat Defender card game used in Day 4 of this lesson. Middle and high school teachers can request one complementary classroom set of cards through the UTSA Marketplace.

Lesson

Teacher Notes: If you wish to give students a more comprehensive understanding of the rules of armed warfare, show them What is Cyber Warfare? (YouTube, 2018). This may help students understand how these rules translate to cyber warfare. These rules of war stem from the Geneva Conventions. An extended background reading for the Geneva Conventions can be found at Geneva Convention (History.com, 2018).

Day One: Define Cyber War

- **Whole Group Hook: Have you been hacked? (Pwned) (10 minutes)**
  - Tell students that the word "pwned" originates in video game culture and is a code/derivation of the word "owned", due to the proximity of the "o" and "p" keys. It's typically used to imply that someone has been controlled or compromised. Have students check to see if their email (or parents/family/friends email) has been involved in a breach by going to Have I Been Pwned. If students find they have been pwned, have students change their email passwords. Discuss with students that even though they themselves did not do anything wrong, cyberattacks can still happen to companies/websites that have their information. Changing a password is an extra

deterrent from attack.

- Ask students what they think hackers are doing with information gathered from cyberattacks. Show them a picture of a house and ask them to identify why someone would break into a house. Students might volunteer answers like stealing expensive equipment or money. Tell them to imagine that the members of your family all live in several houses, but they keep the keys to those houses in a primary residence. If someone broke into that primary residence, they'd have the keys to all the other houses. The primary house is your email account. Access to it opens access to other accounts like banks, shopping, etc. It's always a good idea to change the locks (passwords) to the house once in a while. Ask students what homeowners can do to protect their homes from being broken into. They might suggest a security camera, extra locks, a guard dog, etc. As an analogy, you might tell students that their family wants to hide a cherished and expensive item inside the house, like crown jewels. You might put the jewels in a locked box, then inside a locked chest, which is inside a locked safe, inside a locked house, etc. The more security that is in place, the harder it is to get to the valuable item. In cybersecurity, the goal is to protect valuable data, detect when a cyberattack has occurred, and in the worst case scenario recover the valuable data that was stolen.

- **Whole Group: What is Cyber Warfare? (10 minutes)**
  - Ask students if they've ever been an observer on accounts like Reddit or Instagram - that is, looking at posts without commenting. Some may call this "lurking." Sometimes we do this to simply get ideas, understand concepts, or because we enjoy reading other's posts rather than contributing. Ask students what they think the main difference is between collecting information by browsing these accounts (for instance, learning a new way to make a meal) and spying. Students will most likely point to the intent of gathering the information. While students may say they are perusing these accounts for recreation, spies are gathering information for malicious intent.

  - Ask students where the line should be drawn in regards to gathering data. Is it always ok to do as long as no harm is intended? Students might say this is ok, like looking at Instagram, Reddit, or TikTok. Remind students that the information gathered from these platforms is posted publicly. Ask students how they would react if someone was reading their private messages to friends through text messages, but they didn't intend to do anything with the information. Is it still ok? Why or why not? Allow students to share their thoughts with their partner and call on a few students who would like to share what they discussed together. Most students would feel a violation of privacy has taken place in this scenario, even if the intruder didn't intend to use the information maliciously.

  - Tell students that the scenarios that were discussed relate in a bigger picture, globally, as countries gather information on each other, many times for malicious intent that may lead to what is called cyber warfare. Tell students that cyberattacks do not only come from hackers attacking companies or individuals, but can be seen as an act of war between countries to disable critical infrastructure. Ask students to talk to their partners about three of the questions posed below that seem most interesting to them. You may wish to display these on a projector:
    - "Why do countries engage in war?"
    - "Is the point of war to kill/terrorize people? Do people die anyway?"
    - "Is war necessary?"
    - "How could we accomplish the outcomes of war without loss of life? Is this better?"
    - "What are the rules of war? Does anything go? Why do we need rules in war?"
    - "What is cyber warfare? What qualifies as an act against sovereignty?"
    - "What are the rules of cyber war?"

- Focus students on the question: "Why do countries engage in war?" and refer back to Lesson 1: Cryptology, where civilizations protected themselves from invasion by creating barriers, coding their language, and going to war over resources. With technological advancements, countries are engaging in acts of war at the cyber level and they have devastating effects. On the other hand, cybersecurity and military experts defend and protect our country from these attacks.

- **Small Group: Origins of Cyber warfare (20 minutes)**
  - Show students the Cyber Warfare Attacks video to help lay a foundation for the following activity. Ask them to discuss one reason (there are many) as to why cybercriminals might be interested in infiltrating a country's networking system. What might the consequences be?

  - Tell students: "Cyber warfare wasn't always defined, but as new technologies arose and adverse uses increased, laws and regulations needed to be in place. One such historical example of this has to do with moving a statue. That's right, moving a statue led to a cyberattack. But this wasn't just any statue. At the end of World War II, a small country called Estonia declared independence from Russia. The Swedes had helped Estonia with their independence and helped wire the whole country (voting, paying for parking-everything was digital). This helped the country run efficiently, but it also left Estonia vulnerable to cyberattack. Today, we'll read *How a cyber attack transformed Estonia*. (McGuinness, 2017) and what came from this historical incident."

  - Tell students to individually read the article. As they read, they should answer the discussion questions in Part 1 of Estonia's Impact on Cyber War from the Student Handouts**.**

  - Tell students: "This attack changed history. Prior to this, there weren't any laws governing cyber warfare; what was considered an attack, who were attackers allowed to attack, and when or how countries were allowed to defend themselves. Essentially, what are the "rules of war" or humanitarian law when applied to the cyber world or cyber warfare? Just as the Geneva Conventions establish the "rules of war" or humanitarian laws regarding armed warfare to lessen the brutality of war and to protect those who are not fighting, we needed such laws for the cyber warfield. For instance, in armed warfare, civilians are never to be targets. Should this also be true in cyber warfare? The world needed something similar to the Geneva Conventions to help us navigate the world of cyber warfare. If the rules of war are broken, these are called war crimes. They are documented and investigated by States (countries) and international courts, and individuals can be prosecuted. NATO (The North Atlantic Treaty Organization) called in international experts, led by Law Professor Mike Schmitt of the Naval War College to create a policy around cyber warfare. As the attack on Estonia was centered in the town of Tallinn, this eventually became known as the Tallinn Manual and its focus is on cyber operations. It outlines how international law applies to cyber conflicts and cyber warfare."

  - Tell students they will now review the major issues covered by the manual by completing Part 2 of Estonia's Impact on Cyber War from the Student Handouts**.**

- **Whole Group Closure Activity (5 minutes)**
  - Tell students that they may have seen some ambiguity in the Tallinn Manual. What questions do they have? What seems to be a gray area? Allow students to share out. Remind students that as technology continues to change, the Tallinn Manual will too. For instance, espionage to view data and "do nothing" with it is considered legal.
    - If time permits, you may wish to explore the ethical question: "Should espionage be illegal in cyber warfare?"

Day Two: Protect, Defend, Attack: How countries engage in cyber warfare

- **Whole Group: Cyber Warfare Challenge (25 minutes)**
  - Ask students: "Of all the countries in the world, who do you think might be the most frequently cyberattacked?". Record student answers on the board.
  - Ask students to go to the *Cyberthreat Real-Time Map*. Instruct them to click on the country they guessed and see what number the country ranks. If no students guessed the correct country as the most attacked, let them continue clicking on different countries until someone in the class finds it.
  - Once the top countries are found, ask students to discuss with their partners why these countries might be targeted. Students may not know, but it could be that these countries have valuable information, secrets, or have posed a threat to other countries.
  - Tell students that cyberattacks occur all around the globe and can occur from anywhere, as they have just observed. How might a country engage in cyber warfare? How might a country defend itself? Who does the attacking and defending? Tell students they will engage in an online challenge in order to see how the U.S. might protect, defend, and attack in cyber warfare.
  - Allow students approximately 15 minutes to run the *Cybersecurity Challenge* (Department of Defense, n.d.). simulation. Tell students to answer the questions relating to each of the following sections as they play in the Cyber Challenge Student Handout.
    Teacher Note: It is reasonable for the timeframe to ask students to only attempt level one or two of each component of the cyber challenge. If you wish for students to attempt multiple levels, more time may be needed.
    - **Part One: Protect:** Students will build a secure server environment with the intent to prevent a cyberattack. Have students click on the different server components and record the purpose of each server component. Have them use the components to create secure servers.
    - **Part Two: Defend:** Students will evaluate attacks that are attempting to access their system, deciding if an attack is being made or if the attempt is legitimate.
    - **Part Three: Attack:** Students will use an analogous game to locate and track down potential threats (similar to IP addresses, but like a puzzle game). Now would be an appropriate time to review with students that an IP address is a numerical label that identifies a device on a network.
    - If some students finish before others, they can try the Ultimate Challenge while they wait for their peers.

- **Small Group/Individual: Careers (20 minutes)**
  - Tell students that they may be suited for a career in cybersecurity and that they will take a brief career survey from California CareerZone to determine the most compatible occupation for their interests.
    - Tell them that a brief (30 question) survey will show them some of their interests (called an interest profiler) and will try to match careers to those interests.
    - They will choose a career based on the interest profiler and take notes on this career.
    - They will choose a career in cybersecurity or information technology (close careers that can relate to cybersecurity) and take notes on a career of their choosing in this category.
    - They will compare careers for similarities and differences and discuss the careers with

their partners.

- Optional: Students may wish to research the careers linked from the game. Have students use the links below to investigate and research various cyber careers. They should report on the pathways, education, salary, daily duties, prerequisites, etc. Students should also explain which part of the game their career applies to.
  - Cyber Security Specialists
  - Cyber-Operations Officers
  - Cyber Security Officers
  - Network and Database Administrators
  - More Careers

Day Three: Cyber Warfare Case Studies

- **Whole Group (10 minutes)**
  - Tell students that cyberattacks might be categorized in order to assess their threats and in order to consider them as an act of war. For instance, causing harm to a civilian IS an act of war, while monitoring information, or espionage, is not.
    Cyberspace can be thought to have 3 layers: the physical layer (hardware, cables, equipment), the syntactic layer (software for operating the physical equipment), and the semantic layer (humans interacting with and perceiving the computer-generated information). Cyber attacks can be on any of these three layers and can be categorized as:
    - **Surprise Attack**: Massive and unexpected attack, usually with the intent to prepare for a physical attack later.
    - **Economic Disruption:** Targeted attack on economic establishments: stock market, payment systems, or banks with the intention of stealing money or blocking access to the money.
    - **Electrical Power Grid**: Disabling critical systems and infrastructure, potentially resulting in bodily harm with the intention of disrupting services and communication.
    - **Denial-of-service:** Flooding a website with fake requests (usually bots) to overwhelm the system, intending to shut down and block access to sensitive websites.
    - **Sabotage**: Stealing, destroying, or leveraging threats (ransomware) with the intent to shut down a system, receive funds, or for other malicious intent.

  - Have students watch the Solarwinds Attack video. Ask them to discuss with a partner what category they think the Solarwinds attack falls under. (Answer: sabotage, as the attack included government networks, could have resulted in destroyed/altered data and enabled hackers to impersonate people.)

- **Small Group (35 minutes)**
  - Students will work with a partner to learn about another cyberattack of their choice to determine which category the attack falls into and if it should be considered an act of war, using the Cyber Warfare Case Studies from the Student Handouts.
    Teacher Note: This activity has students completing a CER. If your class is unfamiliar with writing CERs, you may wish to use Claim, Evidence & Reasoning (CER): Writing Scientific Explanation as a review/introduction.
    Teacher Note: all the articles are from Wikipedia. You may wish to remind students that Wikipedia is a good first source of information, but should be verified using other, more trustworthy sources.
    - Pipeline Attack
    - Equifax Data Breach
    - Sony Pictures Hack
    - Ukraine Attacks

        - DDoS Attacks Against South Korea
        - WannaCry Attack
        - Democratic National Committee Cyber Attacks
        - Harris Federation Attack

    Teacher Note: You may opt to select cases that fit your student population better using this List of cyberattacks (Wikipedia, 2022).

- **Wiki Page**
    - If time permits, allow students to add the following to their Cybersecurity Wiki Outline. If not, assign for homework:
        - Does the attack you studied qualify as an act of war? Why or why not?
        - Images to help understand the concepts from the lesson
        - Key vocabulary words from the lesson defined

Day Four: Cyber Threat Defender Card Game

- **Small Group: Board Game (40 minutes)**
    - Tell students they will be playing a board game to simulate cyber warfare attacks and defenses. Each game will consist of two students who will take on the role of opposing nations.

    - Using the modified version of the Cyber Threat Defender:
        - Hand out decks to partners and tell students to look over the different types of cards.

        - Tell students to use the decks to try to figure out how to play/rules, writing down what they think on the board.

        - After students have had a chance to think of what the rules should be, call on a few students to volunteer their ideas. Review the following real rules with students and see how accurate they were in figuring out how to play. CTD Rules – The UTSA CIAS

        - Have students play a round with their partner.

- **Whole Group: Discussion and Closure (5 minutes)**
    - Reflection question: "Even with proper defense, are you always safe in the game? How is this similar to real life cybersecurity?"

Extension

Day One Closure Activity:

- Students may wish to apply what they've learned about the rules of cyber warfare to a more recent cyberattack. A discussion about the Ukraine attack of 2022 may be relevant. What is/was upheld or not in the Tallinn Manual? If this seems relevant to your class, more information can be found in *Russian Cyber Operations and Ukraine: The Legal Framework.* (Schmitt, 2022) and *Tech Companies Help Defend Ukraine Against Cyberattacks.* (Sanger et al., 2022).

CTE Alignment

3.4 Research the scope of career opportunities available and the requirements for education, training, certification, and licensure.

10.5 Understand the major software and hardware components of a computer and a network and how they relate to each other.

Resources

';--have i been pwned? (n.d.). Haveibeenpwned. https://haveibeenpwned.com/
California CareerZone. (n.d.). California CareerZone. https://www.cacareerzone.org/

CIAS Cyber Threat Defender. (n.d.). CIAS. https://cias.utsa.edu/ctd_cards.php

CIAS Cyber Threat Defender Instructors. (n.d.). CIAS. https://cias.utsa.edu/ctd_instructors.php

Claim, Evidence & Reasoning (CER): Writing Scientific Explanation. (n.d.). [E-book]. https://www.dvusd.org/cms/lib/az01901092/centricity/domain/5849/cer.pdf

Cyber Security Operations | Analyst — Today's Military. (n.d.). Today's Military. https://www.todaysmilitary.com/careers-benefits/careers/cyber-operations-officers

Cyber Security Specialists — Today's Military. (n.d.). Today's Military. https://www.todaysmilitary.com/careers-benefits/careers/cyber-security-specialists

Cyber Threat Defender: The Collectible Card Game. (n.d.). [E-book]. https://cias.utsa.edu/assets/CTD-Instructions_2022rulebook.pdf

Cyber Threat Defender (CTD) Custom Card Challenge. (n.d.). [E-book]. https://cias.utsa.edu/assets/CTD-Custom-Card-Challenge.pdf

Cyber Threat Defender Asset Quiz. (n.d.). [E-book]. https://cias.utsa.edu/assets/CTD_Quiz_Assets.pdf

Cyber Threat Defender Attacks Quiz. (n.d.). [E-book]. https://cias.utsa.edu/assets/CTD_Quiz_Attacks.pdf

Cyber Threat Defender Defense Quiz. (n.d.). [E-book]. https://cias.utsa.edu/assets/CTD_Quiz_Defense.pdf

Cyber Threat Defender Events Quiz. (n.d.). [E-book]. https://cias.utsa.edu/assets/CTD_Quiz_Events.pdf

Cyberthreat Real-Time Map. (n.d.). Https://Cybermap.Kaspersky.Com/. https://cybermap.kaspersky.com/

Department of Defense. (n.d.). *Cybersecurity Challenge*. https://www.cybermission.tech/#!/page/home

IT Cyber Security — Today's Military. (n.d.). Today's Military. https://www.todaysmilitary.com/careers-benefits/career-fields/cybersecurity-and-information-technology

IT Cyber Security Officers — Today's Military. (n.d.). Today's Military. https://www.todaysmilitary.com/careers-benefits/careers/cyber-security-officers

K-12 Classroom Box (Teachers). (n.d.). UTSA Marketplace. https://secure.touchnet.net/C21612_ustores/web/product_detail.jsp?PRODUCTID=293

List of cyberattacks. (2022, May 6). In *Wikipedia*. https://en.wikipedia.org/wiki/List_of_cyberattacks

McGuinness, B. D. (2017, April 27). *How a cyber attack transformed Estonia*. BBC News. https://www.bbc.com/news/39655415

Network and Database Administrators — Today's Military. (n.d.). Today's Military. https://www.todaysmilitary.com/careers-benefits/careers/network-and-database-administrators

Sanger, D. E., Barnes, J. E., & Conger, K. (2022, March 1). *Tech Companies Help Defend Ukraine Against Cyberattacks*. The New York Times. https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

Schmitt, M. (2022, January 16). *Russian Cyber Operations and Ukraine: The Legal Framework*. Lieber Institute. https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/

What is Cyber Warfare? (2018, August 15). [Video]. YouTube. https://www.youtube.com/watch?v=UxiWHGZxzWM

Estonia's Impact on Cyber War Answer Key

Part 1: Read about the Estonia Cyberattack of 2007 and answer the questions below as you read:

1. Who viewed the Bronze Soldier in Tallinn as a symbol of victory? Why?

   For Russian speakers in Estonia it represented the USSR's victory over Nazism.

2. Who viewed the Bronze Soldier in Tallinn as an offensive symbol? Why?

   For ethinic Estonians, Red Army soldiers weren't liberators, but occupiers, signifying Soviet oppression.

3. What decision by the Estonian government in 2007 sparked outrage and protests?

   To move the statue outside of the city

4. We have heard of "fake news" recently in the U.S. What kind of "fake news" was being reported in Estonia?

   Russian-language media reported the statue and Soviet war graves were being destroyed

5. What methods were used in a cyberattack on Estonia, and how did they harm the country? (Not the rioting and looting that took place, but specifically the cyberattacks).

   Banks, media, government bodies taken down by internet traffic
   Botnets and automated online requests swamped servers
   Cash machines/online banking froze, government employees couldn't communicate, broadcasters couldn't deliver the news.

6. What is cyber warfare?

   Disrupting society for military purposes

Part 2: Read through a summary of the Tallinn Manual and answer the questions below as you read.

7. What is the Tallinn Manual?

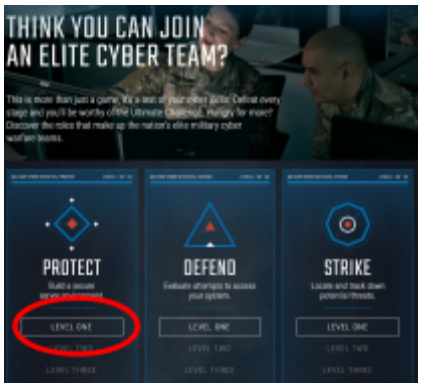
   It is a resource on how international law applies to cyber incidents, including conflicts and warfare.

8. How is the Tallinn Manual similar to the Geneva Convention?

   Both are international agreements to the ethical treatment of humans during warfare.

Cyber Challenge Answer Key

Go to the following website where you will simulate cyberwarfare:
https://www.cybermission.tech/#!/page/home



Protect: In this part of the cyber challenge simulation, you will work as a cyber protector who must build secure networks to transport information from a storage location to a database while preventing enemies from accessing your information.

1. Click on level 1 of "PROTECT" as seen in the image to the right.
2. Read the instructions on how to play.
3. Summarize the following infrastructure components, and decide with a 1-4 the order in which you think the data should flow:

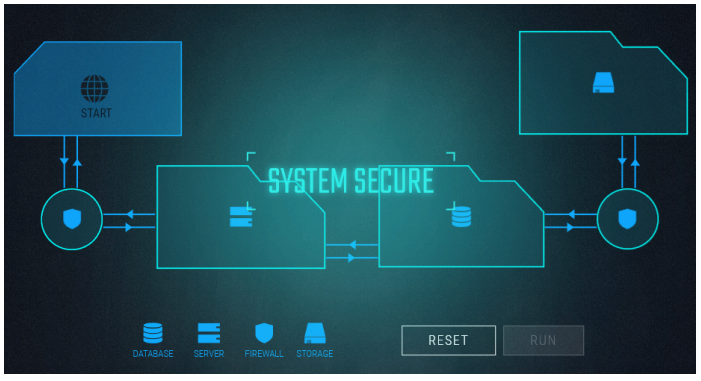
Component	What it is	Order of arrangement to try first
Firewall	Stopping point between infrastructure locations	1
Public Server	Main entry point for users	2
Data Base	A structure that holds user info and access data	3
Private Storage	Place to store secure data	4

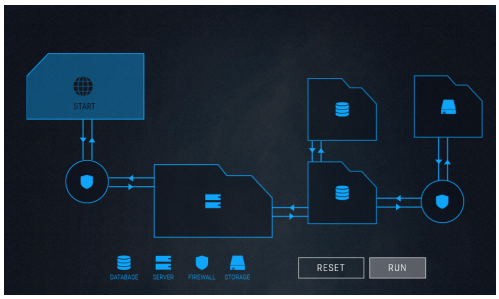
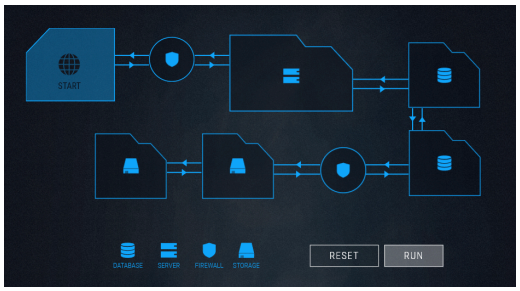
4. Click "PLAY NOW." Arrange the components in the order you chose above. It may not look exactly like you planned, so get as close to the plan as possible.
5. Rearrange the components until you obtain the "system secure" message.
6. What was one strategy you ultimately used to protect your database in the activity? It's ok if your first arrangement didn't work. This is asking what DID work.

Putting a firewall between components and having the private storage as the last point.

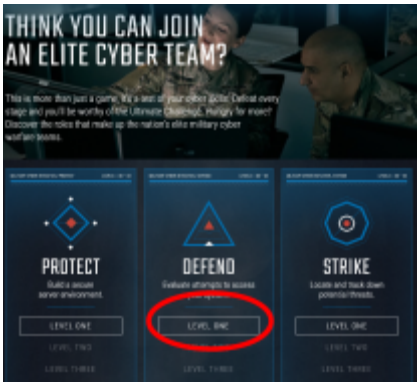
7. What surprised you about the simulation?

Connecting multiple databases was ok, but putting private storage between databases was not

Level 1 KEY	

Level 2 KEY	
Level 3 KEY	

Defend: Go back to the Home page by clicking HOME at the top of the website. You will now work as a cyber defender who must carefully review system logs to identify suspicious activity from users who do not have proper authorization.



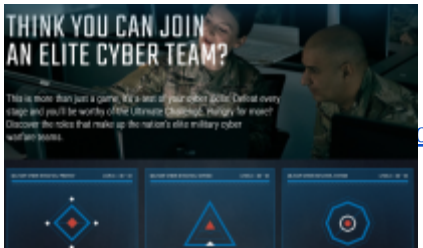
8. Click on level 1 of "DEFEND" as seen in the image to the right.
9. Read the instructions on how to play.
10. Summarize the following activities that will be used to evaluate user intentions.

Time Span	A large number of access attempts over a short period of time could be a denial-of-service attack.
Location	Have there been known attacks from certain locations?
Activity	SQL injections, .exe files, or unauthorized requests for sensitive data are signs of malicious intent.
Number of attempts	Repeated logins may mean someone is trying to guess a password.

11. Click "PLAY NOW." Continue to play until you are able to claim a badge.
12. What suspicious user activity was most difficult for you to detect?

Answers may be "file types," looking at the timing of multiple access attempts, etc.

Strike: Go back to the Home page by clicking HOME at the top of the website. You will now work as an offensive cyber operator who will track a target by matching binary codes.



Cyber

13. Click on level 1 of “STRIKE” as seen in the image to the right.
14. Read the instructions on how to play.
15. What exactly are you trying to figure out in this game (hint: look at step 3 of the instructions)?

    Revealing the IP address of a potential threat

16. What is an IP address?

    A numerical label that identifies a device on a network.

17. How can an IP address be used to track targets?

    If a location can be identified, it is easier to identify the user of the device during the timeframe of the attack

Extension: The Ultimate Challenge: You have been called to an undisclosed location and must now use your combined training to protect the United States from an imminent cyber attack! Play the ultimate challenge and try your best to complete the mission!