HACKERS \’ EPOCH™

Print-and-Play Cybersecurity Card Game

User Guide

Contents:

Download the cards for free at www.HackersEpoch.com

DC Collins

Modified January 7, 2021

Teach Cybersecurity Terminology with a Card Game

Hackers \' Epoch *Print-and-Play* Cybersecurity Card Game is a tool for teaching students many of the terms associated with threats and vulnerabilities within the scope of Cybersecurity. These cards gamify some aspects of cybersecurity training and provide the educator with a starting point for the discussion of cybersecurity principles with students.

As students play the game, they use the cards to build their own network infrastructure and defend it, while attempting to Deceive, Disrupt, Deny, Degrade, or Destroy systems and services belonging to other players. The goal is to add as many systems as possible to one's own infrastructure before the game ends.

The following "domains" are used within the card game:

- Malware
- Network Intrusion
- Social Engineering
- Web Exploitation
- SCADA Sabotage
- Physical Intrusion

Within those domains, the following cards represent the various threats, vulnerabilities, and mitigations:

- Advance Persistent Threat
- Antivirus
- Backup Power
- Blackout
- Botnet
- Cross-Site Request Forgery
- Deceive and Disrupt
- Degrade and Destroy
- Denial of Service
- Drive-By Download
- Encryption
- Footprinting
- Hacktivist
- Infiltrator
- Infrastructure Upgrade
- Lockdown
- Man in the Middle
- Network Breach
- Password Cracking
- Phishing
- Port Scan
- Ransomware
- Reimage
- Replay
- Session Hijacking
- Spam Filter
- Spear Phishing
- Spoofing
- Switch Attack
- Trojan Horse

- Unforeseen Circumstance
- Upgrade and Patch
- Validation
- Viral Worm
- War Driving
- Zero Day

This guide is provided as a free download on the website www.HackersEpoch.com .

HACKERS \' EPOCH™

Cybersecurity Card Game – Print & Play Edition

2-3 Players 30-60 Minutes Ages 12+

January 1, 1970 was the beginning of a new epoch – the digital age was born. What began as seemingly benign became a virtual battlespace that anchored itself into reality. At first, ragtag tribes of computer hackers exploited the unsuspecting users of this brave new world. Eventually, powerful organizations, governed by a select few, established themselves within the virtual realm to have greater influence over the real world. These Cyber Oligarchs, also called Cygarcs, are in a continuous battle for the hearts and minds of billions of people. Some wish only to bring peace to the world through freedom and equity. Others wish to control the world as they see fit. In this game, you are one of these Cygarcs. You must acquire Systems from your adversaries to reduce their capabilities and increase your own. Ultimately, you are fighting for the hearts and minds of humanity. Are your motives for good or for ill?

Objective

Build, protect and maintain your own infrastructure from hostile cyberattacks while strategically stealing from other infrastructures. Win by having the best infrastructure at the end of the game.

Components (100 Cards)

- 1 ***Instruction Sheet***
- 1 ***Layout Example Card*** (Setup and Infrastructure Examples)
- 3 ***Turn Procedure Cards***
- 24 ***FIREWALL Action Cards*** (SHIELD in the top-left corner)
- 42 ***ATTACK Action Cards*** (LIGHTNING BOLT in the top-left)
- 12 ***RAINBOW Action Cards*** (Rainbow-colored swirl on symbol)
- 18 ***SYSTEM Cards*** (2-sided with Warning symbol on back)

Systems, Domains and Enclaves

System cards can be one of 6 different colors. Each color represents a different Domain, which can be recognized by its own unique icon as listed below*.*

- ***Red*** - Network Intrusion Domain *(computer chip icon)*
- ***Orange*** - Physical Intrusion Domain *(padlock icon)*
- ***Yellow*** – Malware *Domain (insect icon)*
- ***Green*** – SCADA Sabotage Domain *(battery icon)*
- ***Blue*** – Web Exploitation Domain *(spider web icon)*
- ***Purple*** - Social Engineering Domain *(fishhook icon)*

Holding at least one System card of a color gives you capabilities within its Domain. For instance, if you have a System card from the Malware Domain (yellow), then you can attack with Malware Action cards. ***A set of all 3 System cards of a single Domain (color) is called an Enclave.***

Action Icons

Action Icons are found in the top left corner of each Action card. The icons inform the player on how the card is to be used.

- ***Shield*** – Firewall and Rainbow Defense Cards
- ***Lightning Bolt*** – Attack Cards
- ***Gear*** – Repair Cards

Action Numbers and the Skull and Crossbones

Each regular Attack Action card has a black circle in the top left corner with either a 1, 2, or ☠(skull and crossbones). Here are the meanings:

- ❶ Compromise 1 System
- ❷ Compromise 2 adjoined System
- ☠ Steal a System

Some attack cards also provide bonus attacks as specified on the card.

Rainbow Cards

Rainbow cards have a shield, lightning bolt, or gear with a rainbow-like swirl. These cards have special instructions written on them.

- Rainbow ATTACK cards can only be used by the attacker during their turn. They have a rainbow lightning bolt in the top left corner. They can only be stopped by an appropriate Rainbow Defense card.
- Rainbow DEFENSE cards can only be used by a player that is currently being attacked. They have a rainbow shield in top left corner. They are never placed in the Firewall.
- Rainbow REPAIR cards can be used by any player at any time.

Setting up the Game

1. Display the 18 System cards neatly in the center of the play area, each fully exposed and with the Warning Symbols (triangle with exclamation point) face-down.
2. Shuffle all Action cards into one deck and place it face-down near the System cards. This is the ACTION DECK.
3. Choose a Starting Player whose birthday is closest to the Epoch start date of January 1, 1970. Make sure that each player receives a Turn Procedure card that will serve as a reminder of the options they have during their turn.
4. Deal out 10 Action cards to each player, ensuring that the cards are kept hidden from other players. Give everyone a moment to look at their cards so that they can determine how they want to proceed in the next step.
5. Beginning with the Starting Player and then moving to their left (clockwise), each player selects a System card of their choice. They must place it down in front of them with the Warning Symbol face-down. Any other cards they receive must be placed next to a previously placed System card. Continue around the table until each player has received 3 System cards.

6. Each player must then place Firewall cards, one from each available Domain (color), into a horizontal row, from left to right, at the top of their play area, making sure to keep those cards within a card's width or less of each other. Only one of each color can be represented in the Firewall at any time. Any duplicates must remain in their hand. Up to 6 unique cards can be placed in the Firewall.

7. All Action Cards used during an attack are placed in the same discard pile, face-up. When the Action deck is depleted, simply shuffle the discard pile, and place it face-down to become the new Action deck. System cards are never discarded. They are only drawn or stolen. Additionally, a player may discard 2 action cards to receive 1 at any time.

Playing the Game

During each player's turn:

1. Draw 3 Action cards ***OR*** 1 System Card. A new System Card must be placed into an available position immediately. Any new Firewall cards must also be placed immediately.

2. Choose ONE Task: Attack ***OR*** Fortify.

   - ***Attack*** – You may attack one or more players as many times as you are able.

   - ***Fortify*** – Repair as many Systems as you are able by discarding a card of the same domain (color) as the compromised one. You may also rearrange System cards, as necessary.

Building the Infrastructure

Each player builds their own Infrastructure by placing System cards on the table in front of them, face-up (Warning symbol DOWN), at least one card's width below the Firewall row. As cards are added to the Infrastructure, they must be placed fully against another System card's edge. No more than one card may be touching any single edge of another card. Up to 4 System cards may touch any other System card.

Attacking and Defending

A player may only attack during their turn and only if they select to do the optional Attack task. ***Before a player can attack with an Action card from a certain domain (color), they must first possess a System from that same domain.*** The System can be either healthy or compromised. Also, the moment they receive the System, the new capability becomes active and they may then immediately use an Action card from the new domain in an attack. An attack is made by placing an Attack card on top of a Firewall or System card that is in a defender's Firewall or Infrastructure.

To attack a System card, the attacker must first get past the Firewall. If a player has an Attack card that is the same Domain (color) as a Firewall card, then the Attack card will be cancelled out and discarded along with the Firewall card that absorbed the attack. The defender must immediately replace any Firewall cards if they have duplicates available. If the Firewall does not have a Domain (color) of the same type as the Attack card, then the attack can bypass the Firewall and go straight to a System card. Rainbow Attack cards ALWAYS bypass the Firewall. They can only be stopped by an appropriate Rainbow Defense card.

An Attack card CANNOT be used on a ***healthy*** System card of the same Domain (*color*), nor on one protected by an adjacent healthy System card of the same Domain as the Attack card. Adjacent System cards protect each other unless they are compromised. Compromised System cards offer no protection and can be attacked by any Attack cards, even cards of the same Domain (color), unless they are being protected by an adjacent healthy System. A compromised System will have the Warning symbol facing up.

Attacking Healthy System Cards

To attack a healthy System card, place one attack card on top of it, face-up. If the attack cannot be stopped, the players follow the instructions on the attack card. Newly compromised System cards are turned over to reveal the Warning symbol. Stolen System cards are given to the attacking player to be immediately placed into an open position within their infrastructure.

Attacking Compromised System Cards

To steal a ***compromised*** System card, place any two attack cards from any domain (including Rainbow) on top of it, face-up, ***disregarding any instructions shown on the attack cards***. Both Attack cards must make it past the Firewall to be successful. If the attack cannot be stopped, the System card is given to the attacker, but it remains compromised in their infrastructure until repaired. If any one Attack card is stopped, then the whole attack fails. Once a system is stolen from a player, the victim can immediately draw a card from the Action deck.

Ending the Game

The game ends immediately when any of the following events occur:

- The last System card has been selected and placed
- Any player has less than 2 System Cards remaining.

All players may then use any Rainbow ***Repair*** cards they have in their possession. The player with the most Victory Points (VP) is the winner. If there is a tie, then the player with the greatest number of healthy systems wins. If there is still a tie, then the person with the most complete Firewall wins.

Calculating Victory Points (VP)

- Healthy System cards = 3 VP each
- Compromised System cards = 2 VP each
- Firewall cards = 1 VP for each ***placed*** Firewall card
- Enclave (All 3 System cards from a domain) = +4 VP
- Full Spectrum (1 System card from each domain) = +6 VP

HACKERS \’ EPOCH

Cybersecurity Terminology Glossary

DC Collins

www.HackersEpoch.com

Advance Persistent Threat — *An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender’s efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.*

“Advanced Persistent Threat.” Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/advanced_persistent_threat. Accessed 10 Apr. 2020.

Antivirus — *Used to protect a computer from viruses*

“Antivirus.” Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/antivirus. Accessed 20 Mar. 2020.

Blackout — *A period of darkness (as in a city) caused by a failure of electrical power*

“Blackout.” Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/blackout. Accessed 20 Mar. 2020.

Botnet *A network of computers that have been linked together by malware : a network of bots*

"Botnet." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/botnet. Accessed 20 Mar. 2020.

Breach *A gap in a wall, barrier, or defense, especially one made by an attacking army.*

"Breach." Lexico.com, https://www.lexico.com/en/definition/breach. Accessed 10 Apr. 2020.

Cross-Site Request Forgery *An attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.*

"Cross-Site Request Forgery." Owasp.org, OWASP, https://owasp.org/www-community/attacks/csrf. Accessed 20 Mar. 2020.

Deception *The act of causing someone to accept as true or valid what is false or invalid*

"Deception." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/deception. Accessed 10 Apr. 2020.

Degradation *A decline in quality or performance; the process by which the decline is brought about.*

"Degradation." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/Degradation. Accessed 10 Apr. 2020.

Denial of Service *The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided).*

"Denial of Service." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/denial_of_service. Accessed 10 Apr. 2020.

Destroy	*A method of erasing electronically stored data, cryptographic keys, and credentials service providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data.*

"Destroy." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/destroy. Accessed 10 Apr. 2020.

Disruption	*An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).*

"Degradation." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/Degradation. Accessed 10 Apr. 2020.

Drive-By Download	*A drive-by download refers to potentially harmful software code that is installed on a person's computer without the user needing to first accept or even be made aware of the software installation.*

"Drive-By Download." Webopedia.com, https://www.webopedia.com/TERM/D/drive-by-download.html. Accessed 10 Apr. 2020.

Encryption	*The act or process of encrypting something : a conversion of something (such as data) into a code or cipher*

"Encryption." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/encryption. Accessed 20 Mar. 2020.

Firewall	*Computer hardware or software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users (as of the Internet)*

"Firewall." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/firewall. Accessed 20 Mar. 2020.

Footprinting	*See **Reconnaissance**.*

Hacktivist *Computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism*

"Hacktivist." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/hacktivist. Accessed 20 Mar. 2020

Host *Any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices.*

"Host." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/host. Accessed 22 Apr. 2020.

Infiltrate *To enter or become established in gradually or unobtrusively usually for subversive purposes*

"Infiltrator." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/infiltrator. Accessed 20 Mar. 2020.

Infrastructure *The resources (such as personnel, buildings, or equipment) required for an activity*

"Infrastructure." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/infrustructure. Accessed 20 Mar. 2020.

Lockdown *An emergency measure or condition in which people are temporarily prevented from entering or leaving a restricted area or building (such as a school) during a threat of danger*

"Lockdown." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/lockdown. Accessed 20 Mar. 2020.

Malware *Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-*

	based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

"Malware." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/malware. Accessed 22 Apr. 2020.

Man in the Middle	*An attack on the authentication protocol run in which the Attacker positions himself or herself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.*

"Man in the Middle Attack." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/Glossary/Term/man_in_the_middle-attack. Accessed 20 Mar. 2020.

Scanning	*Sending packets or requests to another system to gain information to be used in a subsequent attack.*

"Scanning." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/scanning. Accessed 20 Mar. 2020.

Password Cracking	*The process of recovering secret passwords stored in a computer system or transmitted over a network.*

"Password Cracking." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/Password_Cracking. Accessed 10 Apr. 2020.

Patch	*A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.*

"Patch." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/patch. Accessed 10 Apr. 2020.

Phishing	*A scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly*

"Phishing." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/phishing. Accessed 20 Mar. 2020.

Ransomware — *A type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.*

"Ransomware." Csrc.nist.gov, NIST CSRC Glossary, https://www.us-cert.gov/Ransomware. Accessed 22 Apr. 2020.

Reconnaissance — *A preliminary survey to gain information*

"Reconnaissance." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/reconnaissance. Accessed 20 Mar. 2020.

Reimage — *To replace the contents of (a computer or hard drive) with a previously created disk image*

"Reimage." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/reimage. Accessed 20 Mar. 2020.

Replay Attack — *An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.*

"Replay Attack." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/replay-attacks. Accessed 20 Mar. 2020.

SCADA — *Supervisory Control and Data Acquisition*

"SCADA." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/SCADA. Accessed 22 Apr. 2020.

Session Hijacking — *An attack in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is*

	able to pose as a subscriber to the verifier or vice versa to control session data exchange. Sessions between the claimant and the RP can be similarly compromised.

"Session Hijacking." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/Session_Hijack_Attack. Accessed 10 Apr. 2020.

Social Engineering	*An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.*

"Social Engineering." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/social_engineering. Accessed 22 Apr. 2020.

Spam Filter	*Software that identifies and blocks spam*

"Spam Filter." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/spam%20filter. Accessed 20 Mar. 2020.

Spear Phishing	*The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.*

"Spear Phishing." Lexico.com, https://www.lexico.com/definition/spear_phishing. Accessed 20 Mar. 2020.

Spoofing	*DECEIVE, HOAX*

"Spoofing." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/spoofing. Accessed 20 Mar. 2020.

Switch	*A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination.*

"Switch." Csrc.nist.gov, NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/Switch. Accessed 10 Apr. 2020.

Trojan Horse *A seemingly useful computer program that contains concealed instructions which when activated perform an illicit or malicious action (such as destroying data files)*

"Trojan Horse." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/Trojan%20horse. Accessed 20 Mar. 2020.

Upgrade *To replace something (such as software or an electronic device) with a more useful version or alternative*

"Upgrade." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/upgrade. Accessed 22 Apr. 2020.

Validation *Before submitting data to the server, it is important to ensure all required form controls are filled out, in the correct format. This is called client-side form validation and helps ensure data submitted matches the requirements set forth in the various form controls.*

"Form Validation." Mozilla.org, https://developer.mozilla.org/enUS/docs/Learn/Forms/Form_validation. Accessed 20 Mar. 2020.

Virus *A computer program that is usually disguised as an innocuous program or file, that often produces copies of itself and inserts them into other programs, and that when run usually performs a malicious action (such as destroying data or damaging software)*

"Virus." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/virus. Accessed 20 Mar. 2020.

War Driving *The act of driving around in a vehicle with a laptop computer and an 802.11 wireless LAN adapter set to promiscuous mode .... in order to find and exploit existing, unsecured wireless networks.*

"War Driving." CollinsDictionary.com, https://www.collinsdictionary.com/us/submission/19345/War+Driving. Accessed 20 Mar. 2020.

Worm	*A usually small self-contained and self-replicating computer program that invades computers on a network and usually performs a destructive action*

"Worm." Merriam-Webster.com, Merriam-Webster, https://www.merriam-webster.com/dictionary/worm. Accessed 20 Mar. 2020.

Zero Day	*Deriving from or relating to a previously unknown vulnerability to attack in some software.*

"Zero Day." Lexico.com, https://www.lexico.com/definition/zero-day. Accessed 20 Mar. 2020.

Credits

DC Collins – *Creative Director*

Luke Edwards – *Card Illustrator*

Drew Purifoy – *Website Developer*

Eric Rothfeldt – *3D Render Artist*

Richard Archer – *Gameplay Consultant*

Keith Leonard – *Education Consultant*

Samuel Collins – *Graphic Design Intern*