Critical Infrastructure in Your Home Town

David I. Schwartz, Ph.D.
Jessica D. Bayliss, Ph.D.
Chris Schwartz, Ph.D.
Brian Tomaszewski, Ph.D.

Rochester Institute of Technology
College of Computing and Information Sciences
School of Interactive Games and Media
RSS:2025

General Questions

- Disclaimer
- Motivation
- Jack Voltaic®
- Resources and Q/A

Disclaimer

- I am not a representative of the Army Cyber Institute at West Point.
- I am the recipient of a grant from which my team and I have worked with the ACI.
- Full attribution and formal disclaimer near end of slides.

What could possibly go wrong?

- SolarWinds Attack & Details You Need To Know About It | Simplilearn
- Drinking Water Warning Issued Nationwide - Newsweek
- Amid ongoing cybersecurity crisis, workflows remain disrupted at Ascension Seton | KUT Radio, Austin's NPR Station
- East Palestine, Ohio, train derailment - Wikipedia
- Fukushima nuclear accident - Wikipedia
- 80 percent of organizations not ready for CISA rules on security practices | BetaNews
- Cybersecurity incident disrupts services in Newburgh
- Disinformation Fed Far-Right Riot in England After Deadly Stabbing - The New York Times
- Radioactive waste from atom bomb-making headed to Wayne Co. landfill
- Information Security vs. Cybersecurity
- Judge grants restraining order against cybersecurity expert who exposed extent of city's data breach
- Shipment of radioactive waste from Western New York halted before it starts | wgrz.com
- Cyber security expert calls ransomware attack on UMC a ‘national security issue’
- In the wake of Hurricane Helene, questions about government response emerge
- ‘It’s mindblowing’: US meteorologists face death threats as hurricane conspiracies surge
- 8/20→ FBI warns of Russian hacks targeting US critical infrastructure | Reuters
- And, unfortunately, so it goes

What if…?

- **Civilian, non-military, and private resources for military “stuff” and deployment**
- **What can hamper or block everything?**
  - physical, natural, cyber
  - what else?
  - are we all prepared for emergencies?
  - what if all these emergencies converge?
- **The Army Cyber Institute (ACI) asked those questions:**
  - short videos at cyber.army.mil/Our-Work/Jack-Voltaic/JV-Media
  - convergence of disasters affecting critical infraction (CI)

Jack Voltaic® (JV) History

- cyber.army.mil/Our-Work/Jack-Voltaic
  - series of tabletop exercises (TTXes)
  - researching critical infrastructure response
  - cyber.army.mil/Our-Work/Jack-Voltaic/Research-Reports
- **JV1–3, 2016–2020:**

  1.0: "first step in building a framework to prepare, prevent, and respond to multi-sector cyberattacks on major cities"

  2.0: "assembled critical infrastructure partners to study cybersecurity and protection gaps"

  2.5: "series of one day training workshops to share insights from JACK VOLTAIC® 2.0 and discuss how similar efforts have the potential to strengthen the cyber resiliency of DoD missions"

  3.0: "use a regionally-focused scenario where civilian infrastructure influences military deployment"
- **JACK VOLTAIC 3.0: JV3 fact sheet link summarizes JV1–3**

ARMY CYBER INSTITUTE AT WEST POINT

JACK VOLTAIC 3.0

Cyber Research Report

Prepare | Prevent | Respond

Increasingly Connected, Ready to Respond

cyber.army.mil/Our-Work/Jack-Voltaic

Boil it down for us

- When participants/players showed up, some passed around business cards.
- “If you need to know who you need to know when you need to know, you’ve already lost.”
- What could ACI do next?

?

JV 4.0

- **ACI is a research organization, not a TTX organization**
- **More funding appeared given JV1–3 success (Army Doctrine)**
- **JV 4.0 coalition built:**
  - cyber.army.mil/Our-Work/Jack-Voltaic
  - RIT, Stanford, Norwich, Indiana, Trends Global
  - Community development, media, research resources, TTX development
  - JV is research and a TTX

IGM

- What happens to a TTX or wargame given to the *other* game designers?
- What happens when game designers consider security and CI?
- School of Interactive Games and Media | igm.rit.edu
- Focus on entertainment games, serious games, gamification, …

RIT

Rochester
Institute of
Technology

Side Note: Convergence of Games and CI…

Could JV4 Be …

- Easy to install?
- Easy to play? Perhaps within an hour or less?
- Involve multiple players?
- Engage and encourage replay?
- Allow for customization?
- Convince stakeholders of CI to seek additional help?
- A self-adjudicating TTX or wargame that handles CI resilience against a convergence of attacks?

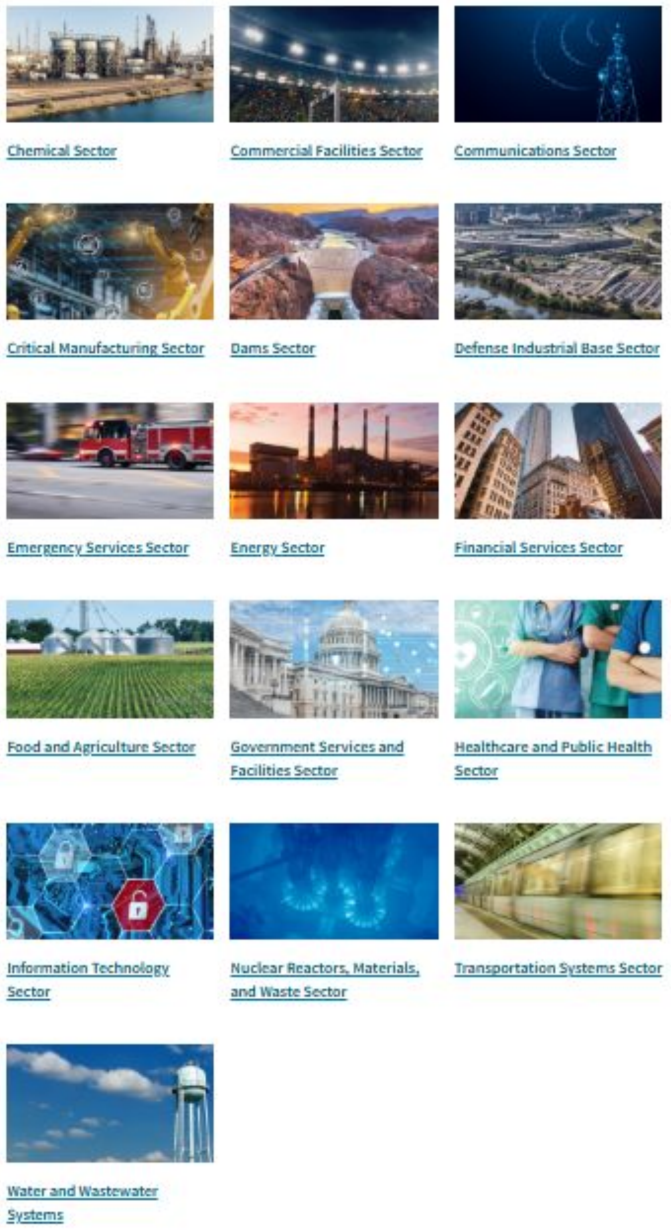
Resilience Games

- Wargaming focused on sustaining critical infrastructure and mitigating cascading failures under crisis conditions
- Decision-makers navigate systemic disruptions and ensure operational continuity

Disaster Resilience + Wargame

JV4: the game(s)

- **Digital card game framework**
  - MTG, Backdoors & Breaches, and many others
  - common format and platform
  - can go analog, too
- **CISA’s 16 CI sectors**
  - www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
  - Think “Model UN” or RPG



Chemical Sector

Commercial Facilities Sector

Communications Sector

Critical Manufacturing Sector

Dams Sector

Defense Industrial Base Sector

Emergency Services Sector

Energy Sector

Financial Services Sector

Food and Agriculture Sector

Government Services and Facilities Sector

Healthcare and Public Health Sector

Information Technology Sector

Nuclear Reactors, Materials, and Waste Sector

Transportation Systems Sector

Water and Wastewater Systems

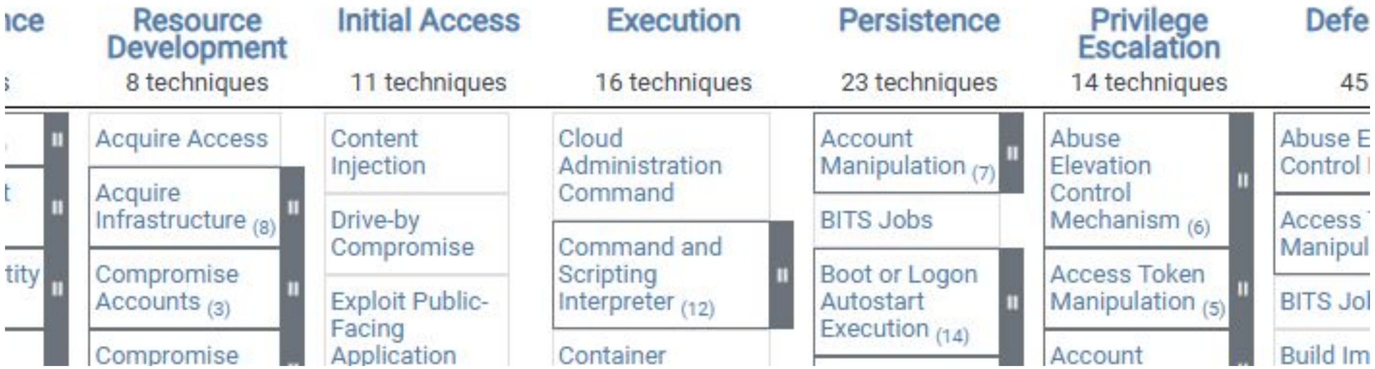
Multiple Products

- **ACI contracted for a modifiable game, and now:**
  - Sector Down: “Critical Instructure TTX: The LAN Party”
  - Access Denied: “Cybersecurity: The Card Game”
  - H4ckC0rps: “Cybersecurity meets Candycrush”
- **All open source and free**
  - Everything can be modified via GitHub (forking)
- **Sector Down and Access Denied can be edited**
  - They’re both games and rudimentary game engines
- **Still getting tweaked**
  - Need more testers!

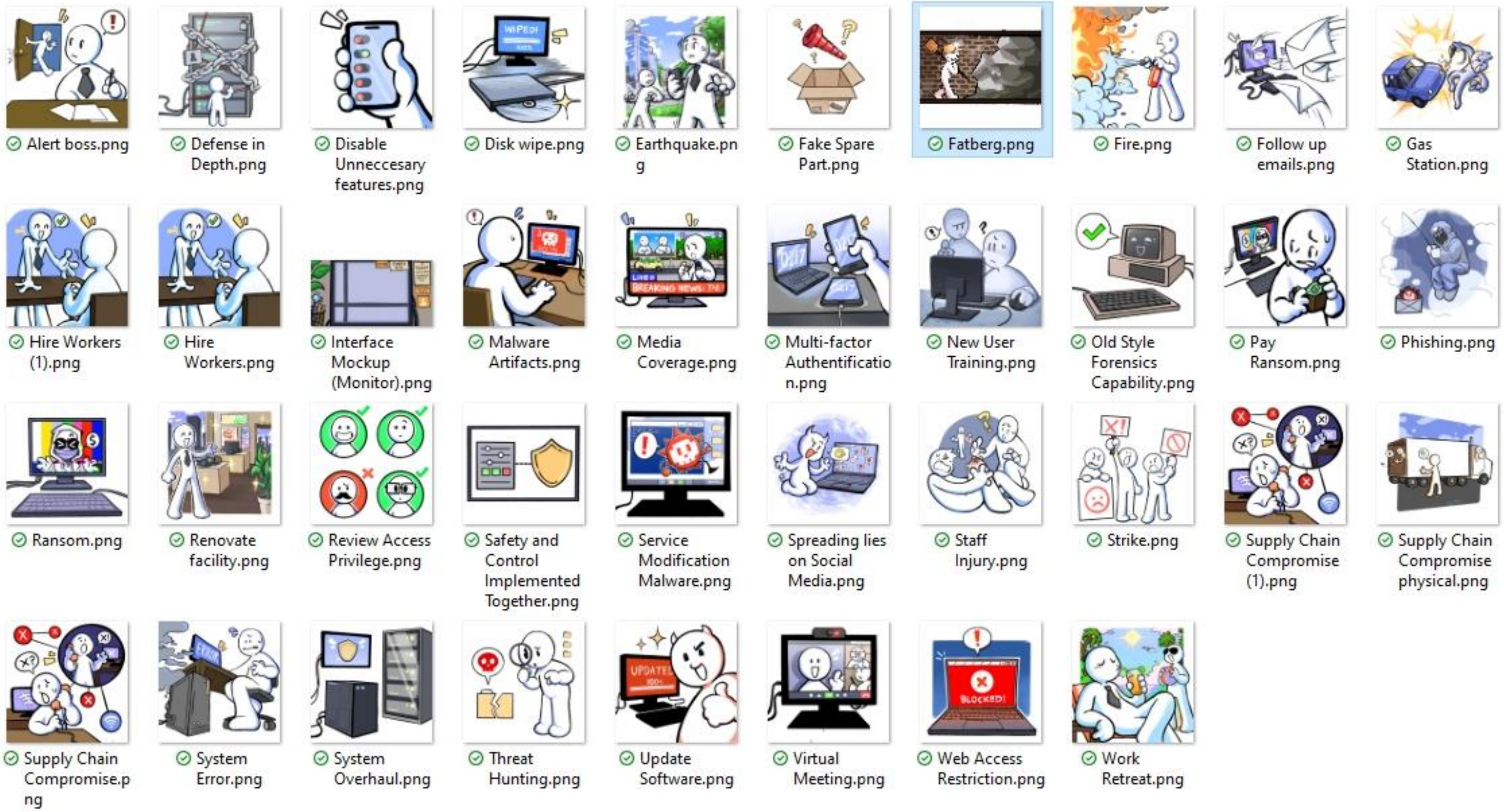
Access Denied Cards

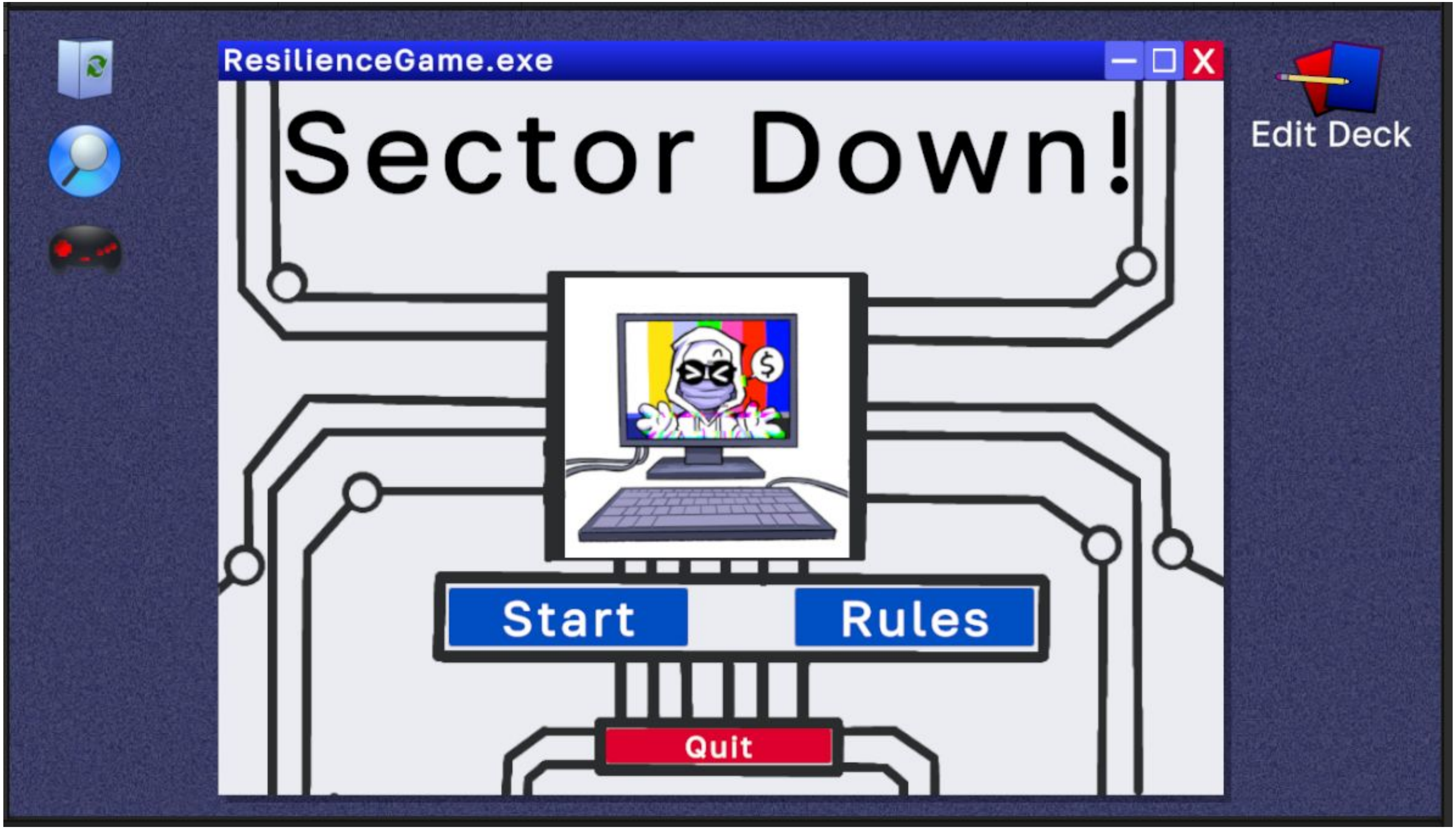
- Basis of AD and SD
- HC uses different art
- Everything leverages MITRE ATT&CK
- See attack.mitre.org for screen captures
- Physical and natural disasters inspired by news articles and hazards.colorado.edu

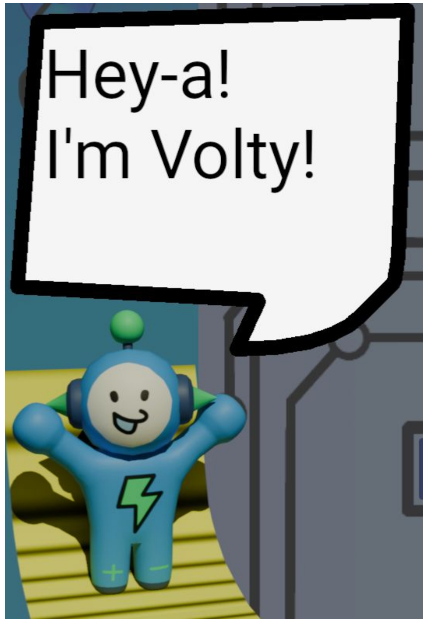
ATT&CK®

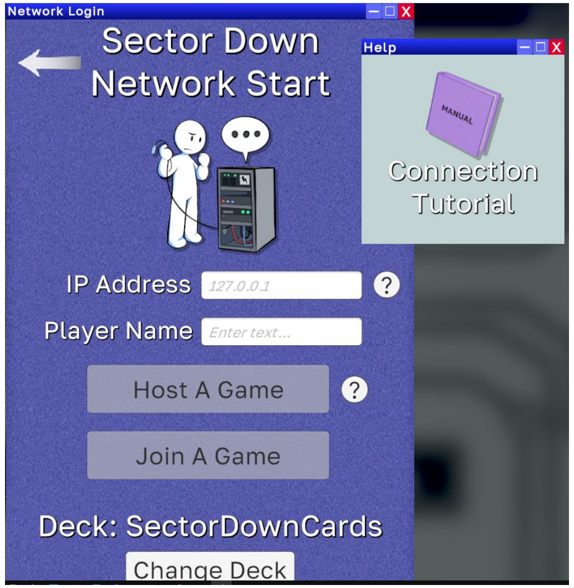


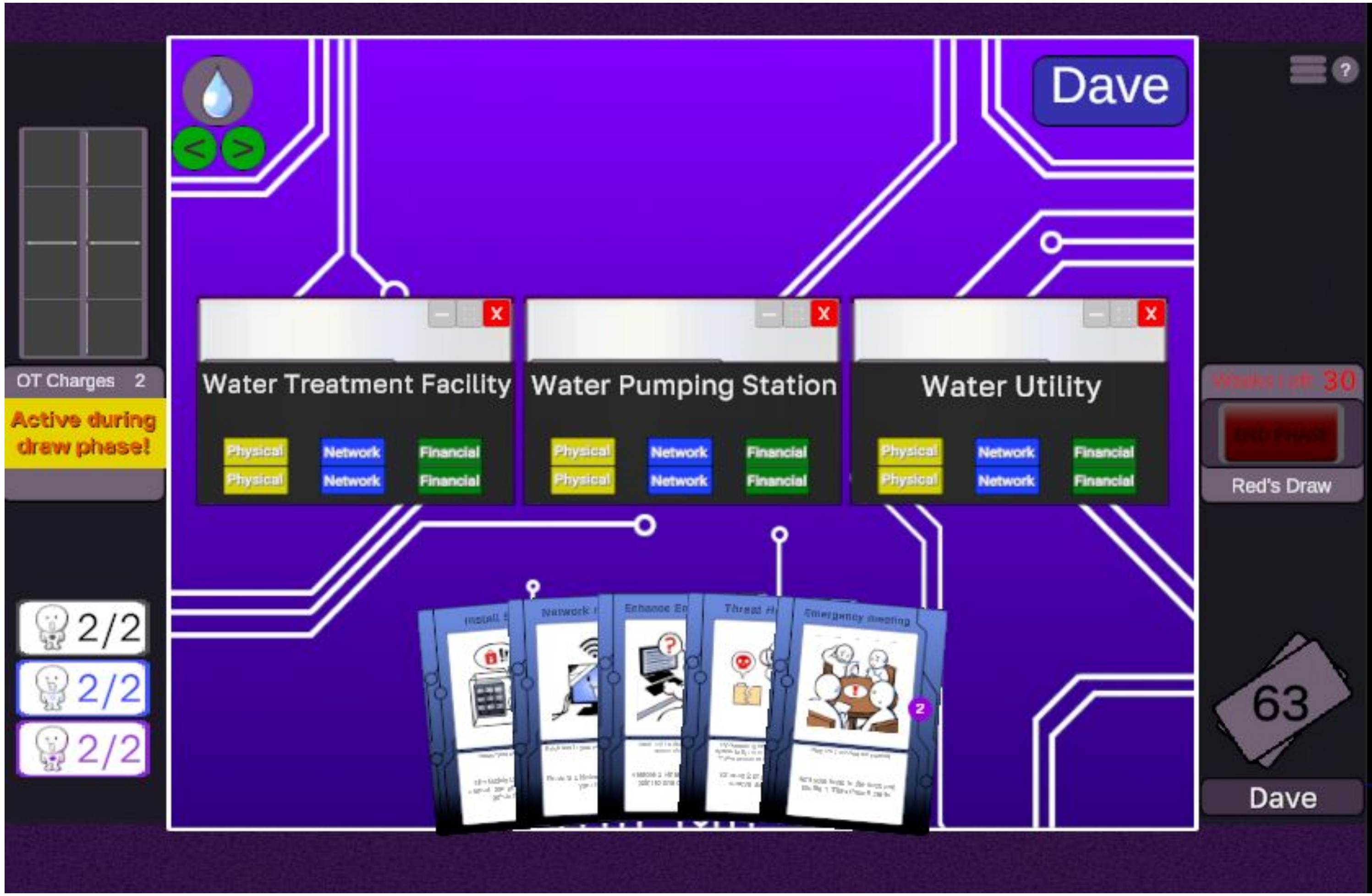
ıce ;	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defe 45
	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse E Control
t	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs	Access Token Manipulation (5)	Access Manipul
tity	Compromise Accounts (3)	Exploit Public-Facing Application	Container	Boot or Logon Autostart Execution (14)	Account	BITS Jol
	Compromise					Build Im

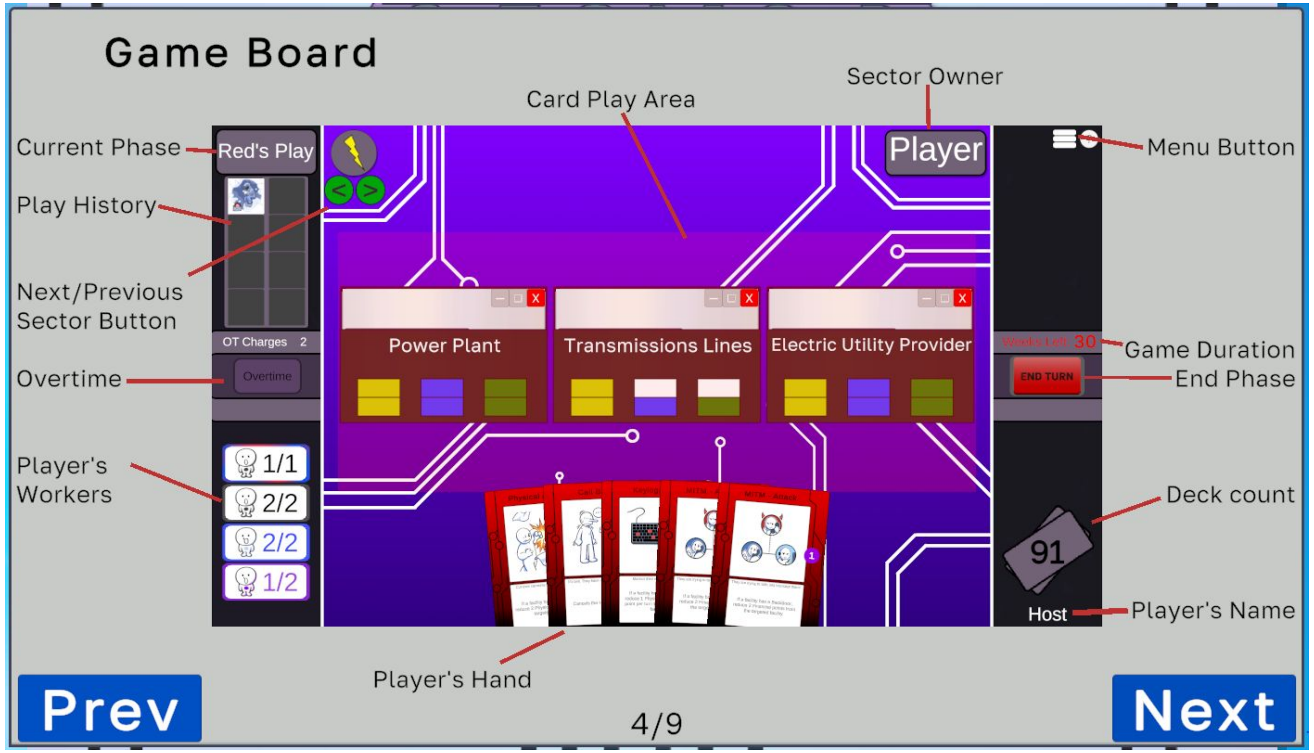

Alert boss.png
Defense in Depth.png
Disable Unneccesary features.png
Disk wipe.png
Earthquake.png
Fake Spare Part.png
Fatberg.png
Fire.png
Follow up emails.png
Gas Station.png
Hire Workers (1).png
Hire Workers.png
Interface Mockup (Monitor).png
Malware Artifacts.png
Media Coverage.png
Multi-factor Authentification.png
New User Training.png
Old Style Forensics Capability.png
Pay Ransom.png
Phishing.png
Ransom.png
Renovate facility.png
Review Access Privilege.png
Safety and Control Implemented Together.png
Service Modification Malware.png
Spreading lies on Social Media.png
Staff Injury.png
Strike.png
Supply Chain Compromise (1).png
Supply Chain Compromise physical.png
Supply Chain Compromise.png
System Error.png
System Overhaul.png
Threat Hunting.png
Update Software.png
Virtual Meeting.png
Web Access Restriction.png
Work Retreat.png

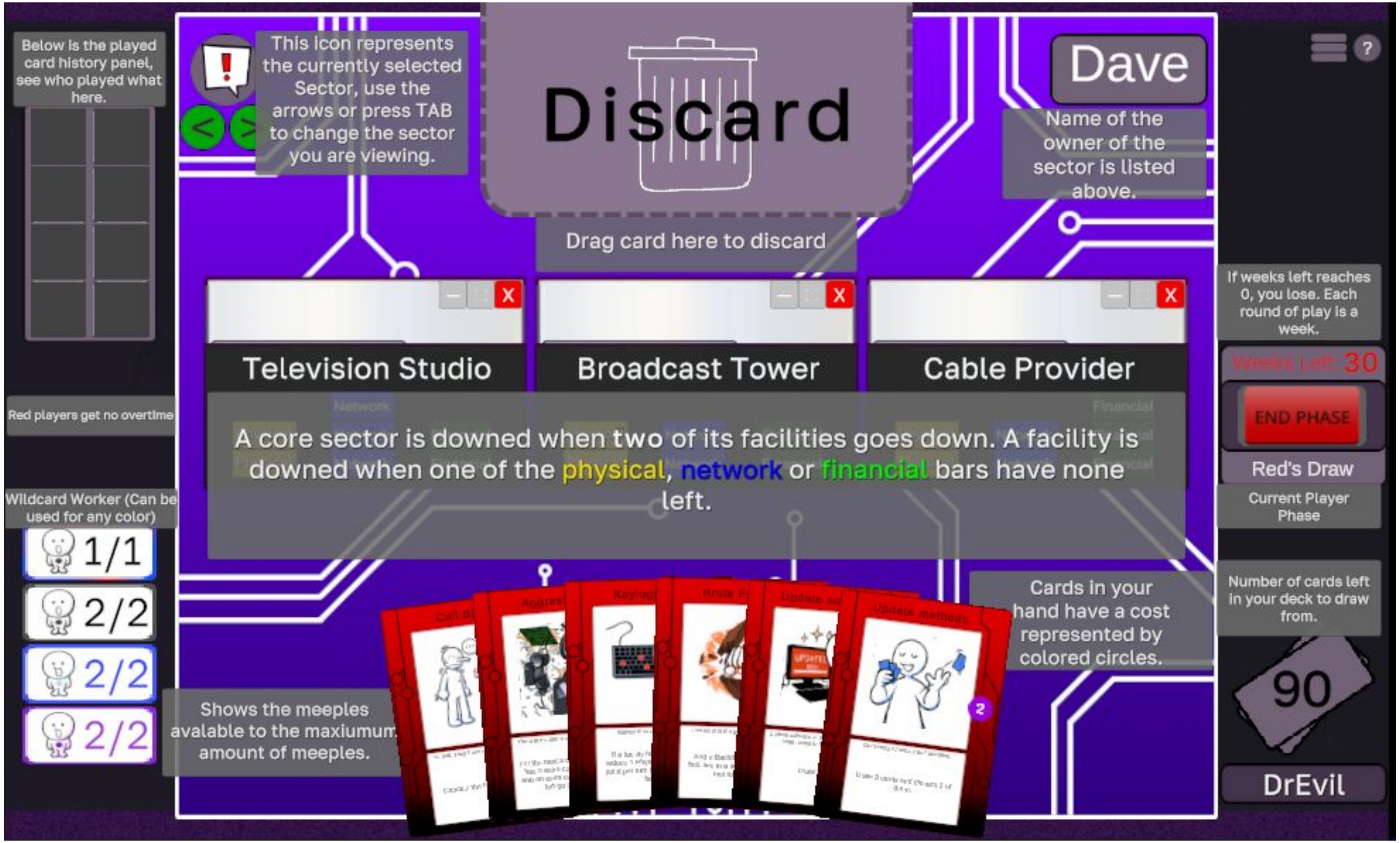

ResilienceGame.exe
Sector Down!
Edit Deck
Start
Rules
Quit


Hey-a!
I'm Volty!


Network Login
Sector Down
Network Start
Help
MANUAL
Connection
Tutorial
IP Address
127.0.0.1
?
Player Name
Enter text...
Host A Game
?
Join A Game
Deck: SectorDownCards
Change Deck


Dave
OT Charges 2
Active during
draw phase!
Water Treatment Facility
Water Pumping Station
Water Utility
Physical
Network
Financial
2/2
2/2
2/2
30
Red's Draw
63
Dave


Game Board
Card Play Area
Sector Owner
Current Phase
Red's Play
Play History
Next/Previous
Sector Button
OT Charges 2
Overtime
Overtime
Player's
Workers
1/1
2/2
2/2
1/2
Player
Power Plant
Transmissions Lines
Electric Utility Provider
Menu Button
Weeks Left 30
Game Duration
END TURN
End Phase
Deck count
91
Host
Player's Name
Player's Hand
Prev
4/9
Next



Below is the played card history panel, see who played what here.

This icon represents the currently selected Sector, use the arrows or press TAB to change the sector you are viewing.

Drag card here to discard

Name of the owner of the sector is listed above.

If weeks left reaches 0, you lose. Each round of play is a week.

Red players get no overtime

A core sector is downed when two of its facilities goes down. A facility is downed when one of the physical, network or financial bars have none left.

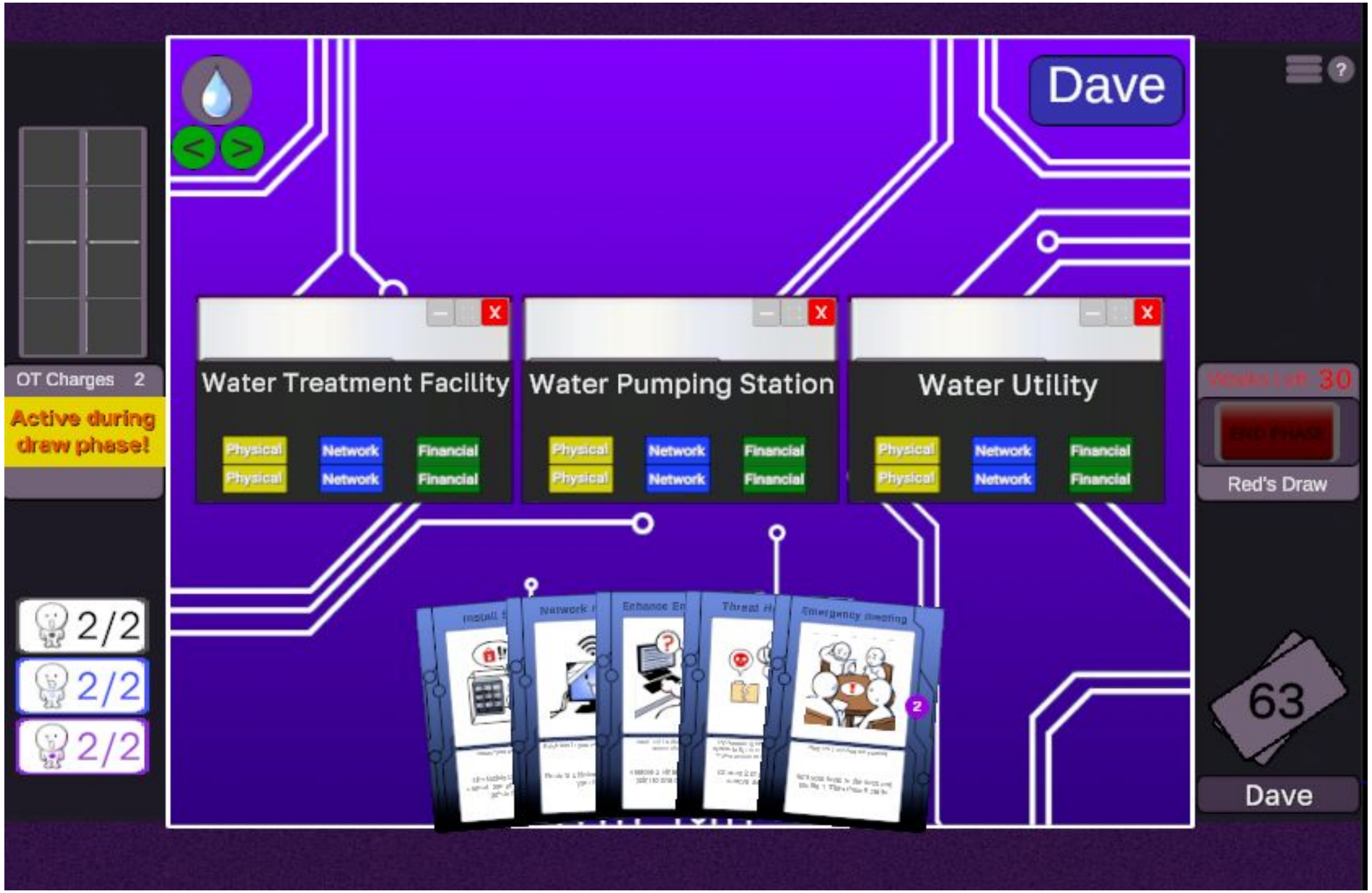
Wildcard Worker (Can be used for any color)

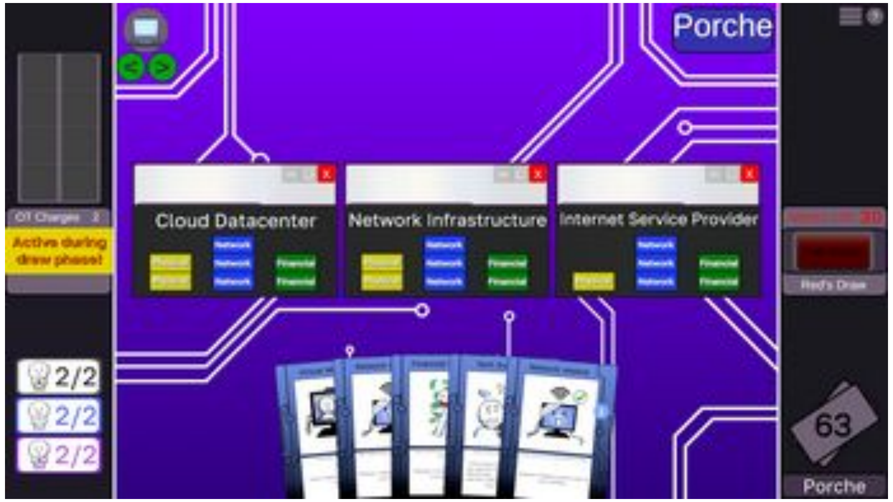
Current Player Phase

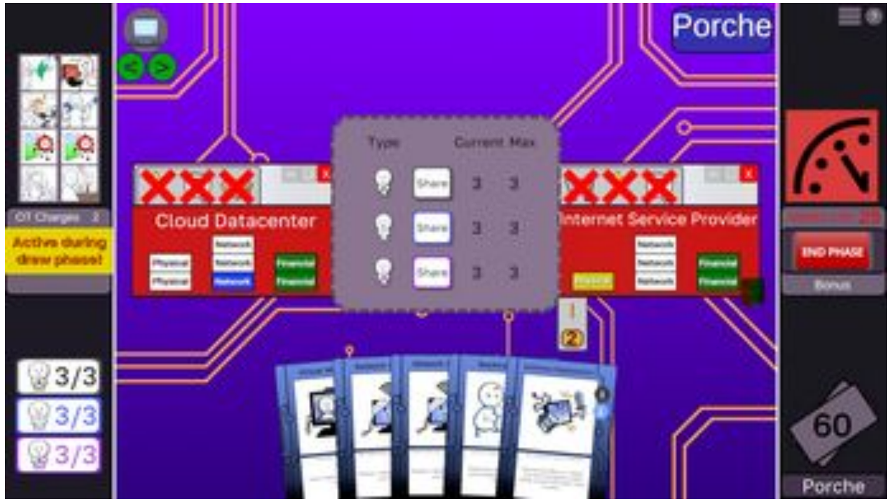
Cards in your hand have a cost represented by colored circles.

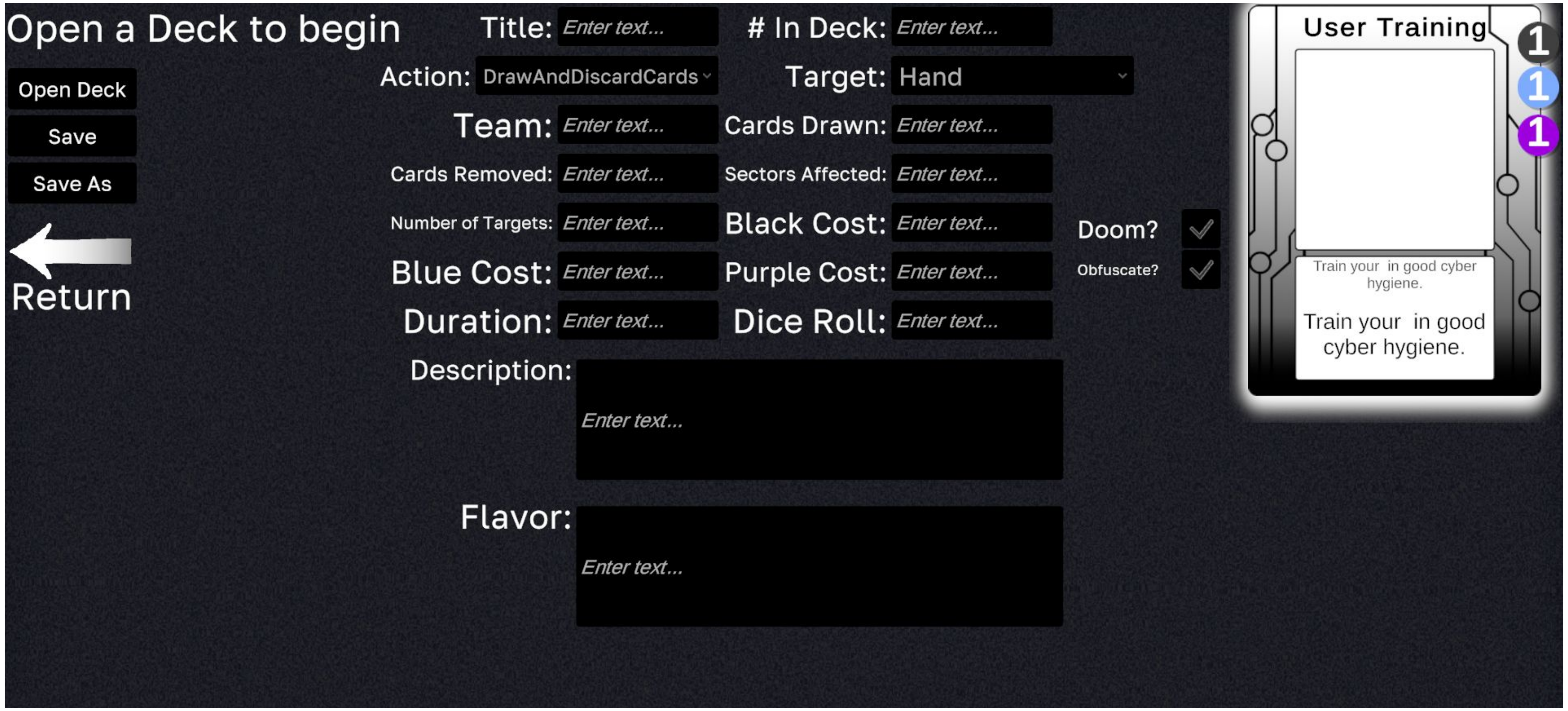
Number of cards left in your deck to draw from.

Shows the meeples avalable to the maxiumum amount of meeples.


Dave
OT Charges 2
Active during draw phase!
Water Treatment Facility
Water Pumping Station
Water Utility
Physical
Physical
Network
Network
Financial
Financial
Weeks Left 30
END PHASE
Red's Draw
2/2
2/2
2/2
Install S
Network
Enhance En
Threat H
Emergency meeting
63
Dave


Porche
OT Charges 2
Active during draw phase!
Cloud Datacenter
Network Infrastructure
Internet Service Provider
Network
Financial
Physical
Red's Draw
2/2
2/2
2/2
63
Porche


Porche
OT Charges 2
Active during draw phase!
Cloud Datacenter
Internet Service Provider
Type
Current
Max
Share
3
3
Physical
Network
Financial
END PHASE
Bonus
3/3
3/3
3/3
60
Porche



Open a Deck to begin

Title: *Enter text...*
In Deck: *Enter text...*
Action: DrawAndDiscardCards
Target: Hand
Team: *Enter text...*
Cards Drawn: *Enter text...*
Cards Removed: *Enter text...*
Sectors Affected: *Enter text...*
Number of Targets: *Enter text...*
Black Cost: *Enter text...*
Doom? ✓
Blue Cost: *Enter text...*
Purple Cost: *Enter text...*
Obfuscate? ✓
Duration: *Enter text...*
Dice Roll: *Enter text...*
Description: *Enter text...*
Flavor: *Enter text...*

User Training
1
1
1
Train your in good cyber hygiene.
Train your in good cyber hygiene.

Access Denied

- Digital and Analog
- Learn some basics about cybersecurity through learning attack and mitigation terms

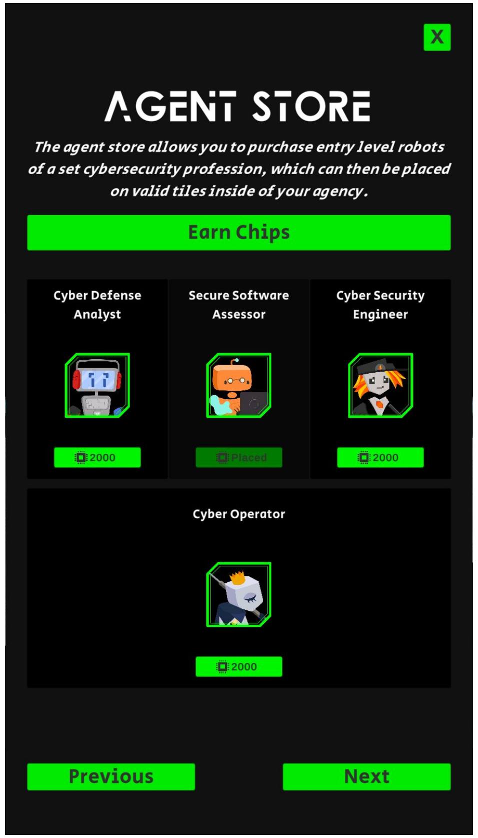
Draw Phase:

You can draw up to 6 cards and discard up to 2 cards to redraw

DEFCON a few weeks ago

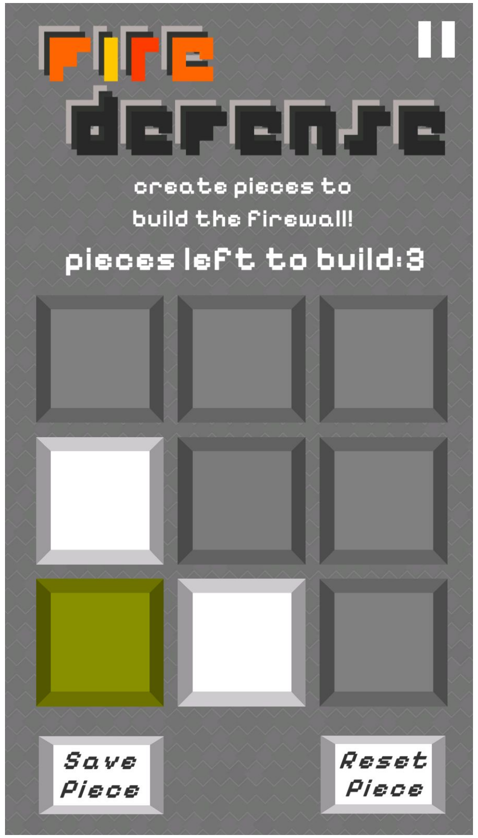
- Free! Open!
- We gave all the current decks away–more coming

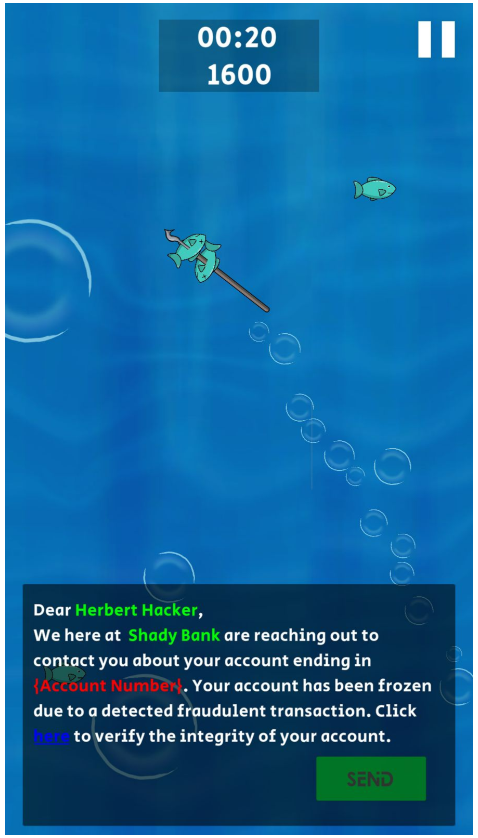
H4ckC0rps



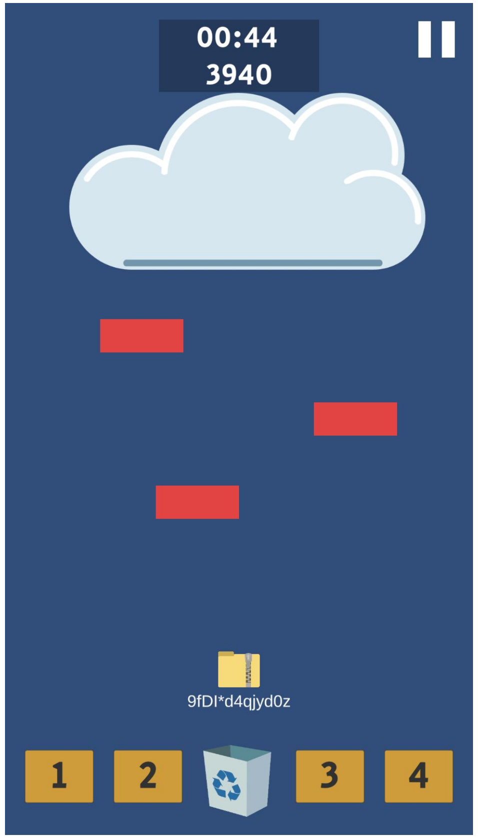
AGENT STORE

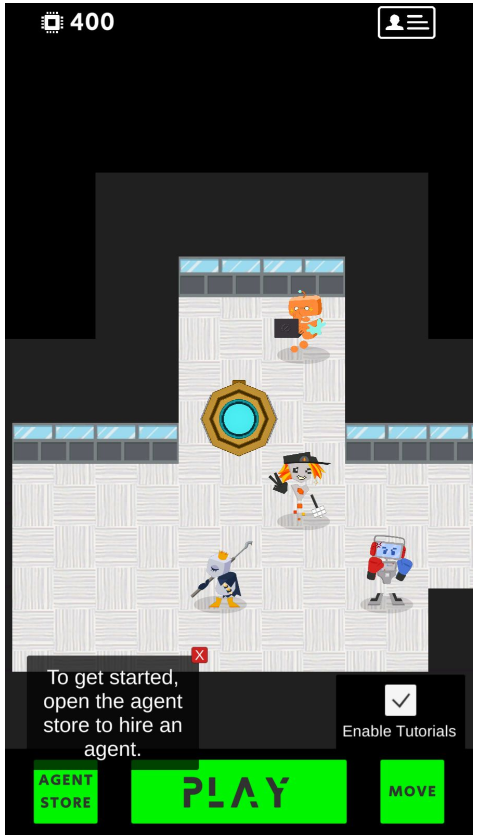
The agent store allows you to purchase entry level robots of a set cybersecurity profession, which can then be placed on valid tiles inside of your agency.





Dear Herbert Hacker,
We here at Shady Bank are reaching out to contact you about your account ending in {Account Number}. Your account has been frozen due to a detected fraudulent transaction. Click here to verify the integrity of your account.





To get started, open the agent store to hire an agent.

☑ Enable Tutorials

Help!

- We want to help you
- But we need help → testing!

Acknowledgements

THE ARMY CYBER INSTITUTE AT WEST POINT 2012

ARMY CYBER INSTITUTE AT WEST POINT

aeop ARMY EDUCATIONAL OUTREACH PROGRAM usaeop.com APPRENTICESHIPS & FELLOWSHIPS

RIT Golisano College of Computing and Information Sciences School of Interactive Games and Media

RIT ESL Global Cybersecurity Institute

ArcGIS

NSF

Unity®

This data was produced by Rochester Institute of Technology under United States Military Academy (USMA) Award Number W911NF-23-2-0036. USMA, as the Federal awarding agency, reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use this data for Federal purposes, and to authorize others to do so in accordance with 2 CFR 200.315(b).

A large team created this work and related products: **students** (Liam Andres, Diego Barilla, Sam Beckman, Lizhao Cao, Jye Crocker, Michael Eaton, Elad Flaison, Ben Garvey, Emmett McEvoy, Kevin LaPorte, Mukund Suresh, Emily Nack, Henry Orsagh, Dariel Ravelo-Ramos, Lee Smith, Heena Thadani, Huadong Zhang, James Zilberman), **faculty** (Jessica Bayliss, Chao Peng, David I. Schwartz, Brian Tomaszewski), a **research scientist** (Chris Schwartz), and **DoD representatives** (David Abitbol, Jason Brown, Karen Guttieri, Mark McElwain, Steve Whitham, Chris Wilkinson).

Current Resources | Q/A

Everything

- bit.ly/rit-jv (where we have posted everything, including this presentation)
- github.com/profjdbayliss/RIT-Resilience-Game (all builds)
- cyber.army.mil/Our-Work/Jack-Voltaic (official site)
- www.rit.edu/directory/disvks-david-schwartz (primary contact)

Access Denied

- github.com/profjdbayliss/accessDenied (everything for free!)
- See also: bit.ly/access-denied-game
- Order a copy! www.thegamecrafter.com/games/access-denied2

Sector Down

- voltyjv.itch.io/sd (direct download of DefCon build)
- bit.ly/sector-down-game (instructions and alternative build)
- github.com/profjdbayliss/RIT-Resilience-Game (source code)

Project “H4ckB0x”

- bit.ly/h4ckc0rps-game (Android APK) (supported in part by NSA)
- bit.ly/h4ckc0rps-images (game images)