Decisions & Disruptions

The Rulebook

March 14, 2017

Overview

Decisions & Disruptions (*D&D*) is a tabletop / role playing game about security in industrial control systems. *D&D* players are tasked with managing the security of a small utility company: they are given a budget that they can spend among different defensive options. Decisions have to be made, taking into account a number of potential threats, known vulnerabilities of the infrastructure, past and ongoing cyber attacks, and of course budget limitations.

The game is to be played with 3 to 5 players plus a Game Master who directs the players, enforces rules and tells the game's narrative. A *D&D* session is expected to last 2 hours maximum. The players need no preparation, and indeed, **players should not read the content of this rulebook**! Partial information and the element of surprise are key elements of *D&D*. But if you, the reader, want to be a Game Master, then keep on reading: this is the reference manual that will guide you through the process of mastering *D&D* sessions.

Table of contents

How to play *D&D*

Before the game

Before playing *D&D*, the Game Master (not the players!) gets familiar with the rules by reading this manual, and builds the game board as described in the **Assets and Defences** section (p. 13).

Structure of a *D&D* session

D&D is a turn-based game, where each turn represents approximatively 2 months in the *D&D* world. A complete *D&D* session lasts **4 turns**. Each turn follows the same structure:

1. The Game Master describes the game situation to the players: the state of their infrastructure, known threats and ongoing attacks.

2. The Game Master gives the players a budget (by default: £100,000) and presents a number of possible security investments such as firewall, antivirus or threat assessment.

3. The players debate which defences are more appropriate and decide by consensus where to spend their budget.

4. The Game Master tells the players about the consequences of their decisions: whether their defences deflect any attacks, and the effects of undefended attacks, such as data theft or equipment disruptions. In addition to technical consequences, the share price of the company can be affected by successful attacks. Then the next turn starts, with a fresh £100,000 budget plus any unspent money left from the previous turn.

The importance of a good narrative

D&D is a role-playing game, and as such, the immersion of players is an important success criteria. You, the Game Master, do not want your players to think that they are playing a game as if they were solving a riddle. Instead, players should think in terms of what they would do if the situation happened in real life: the decisions they take should be based on their common sense, experience, or gut instinct, not on trying to guess what is the content of the rule book.

To achieve a good immersive session, it is important that the Game Master tells a convincing story to the players. We provide a number of pre-written narratives that can be read out loud to the players, describing the *D&D* world, the infrastructure they defend, the effect of attacks and defences. These are provided for inspiration: ideally, after having studied the rule book and the game's environment, the Game Master should be able to describe *D&D*'s world and tell the game story in their own words. This will make the experience much more immersive for the players, and the Game Master will be able to better react to unexpected questions and decisions than if they were following the book. It is perfectly fine to change any description or rule provided in this book! As the Game Master, you have complete control over the game, and any customisation is more than welcome.

Turn One: how to start the session

At the start of the game, set up the game table: put the game board in the centre and dispose the first set of defence cards and figures besides it so that everyone can see them. This first set of defences includes (cf. the section on assets and defences, p. 13, for more details):

- two *Firewalls* (plant and offices)
- *Anti-Virus*

- *Security Training*
- *Asset Audit*
- *Threat Assessment*
- two *CCTV* (plant and offices)
- two *Network Monitoring* (plant and offices)

The other defence cards and figures (three *Patches* and two *Encryptions*) should stay hidden: the players should not know about these yet. They will be unlocked later when they invest in an *Asset Audit*.

TODO: Picture of the game board and cards at the start of the game.

Welcome address by the Board of Directors

You are now ready to start the game. You will be acting as the representative of the company's Board of Directors. Read the following text to the players, or if you feel confident enough, tell them a similar story in your own words:

> *Congratulations! You have been appointed to be the team in charge of managing the security of this company:* ***TODO:*** *CompanyName. I am representing the Board of Directors of* ***TODO:*** *CompanyName, from now on you will reporting directly to me. Security is a very new concern for us, we don't understand much about it. But we also follow the news, and we have seen a growing number of security incidents in utility companies just like us. This is why you have been hired: you are our security experts, and we trust you to keep us safe and secure.*

Your task is therefore to minimise the number of security incidents. As the Board of Directors, our task is to take care of the company's share price. We have high hopes in your ability to defend us against malicious attackers: we wouldn't want the press to learn that we have been hacked, would we? Our share price would certainly be negatively affected. I will be giving you regular updates on how our stocks are doing. Hopefully, nothing will happen, and our shareholders and customers will be happy, right?

At ***TODO:*** *CompanyName, we work on a 2-months financial cycle. I will therefore give you right now your budget for our first cycle: £100,000. Use this money wisely. We have already identified a number of potential investments in defences, represented by these cards and figures. Since the money is limited, and there is a lot of options to choose from, you will have to prioritise the most important defences for this cycle, and delay less urgent investments to the next cycles. Any unspent money will carry over to the next cycle.*

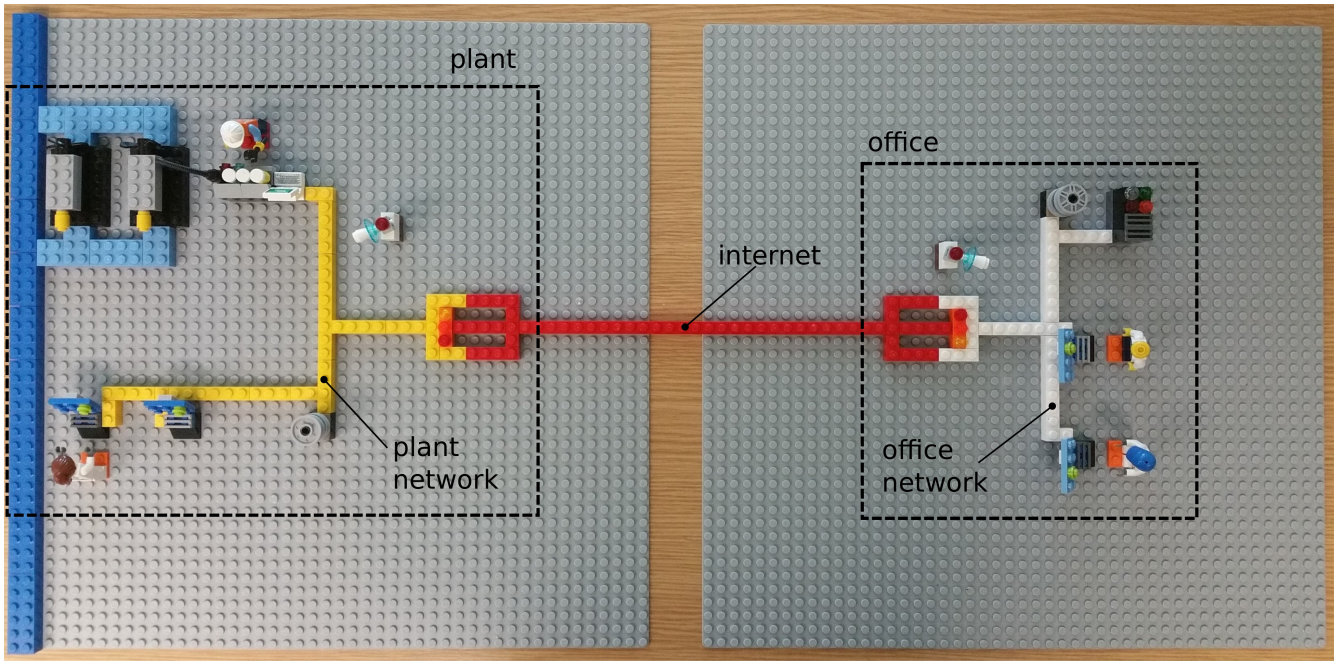
At this stage, interrupting the narrative can be a good idea to ask the players whether they have questions. We have compiled a number of frequently asked questions at the end of this section. When all questions have been answered, you can resume the narrative and show the players around their new company.

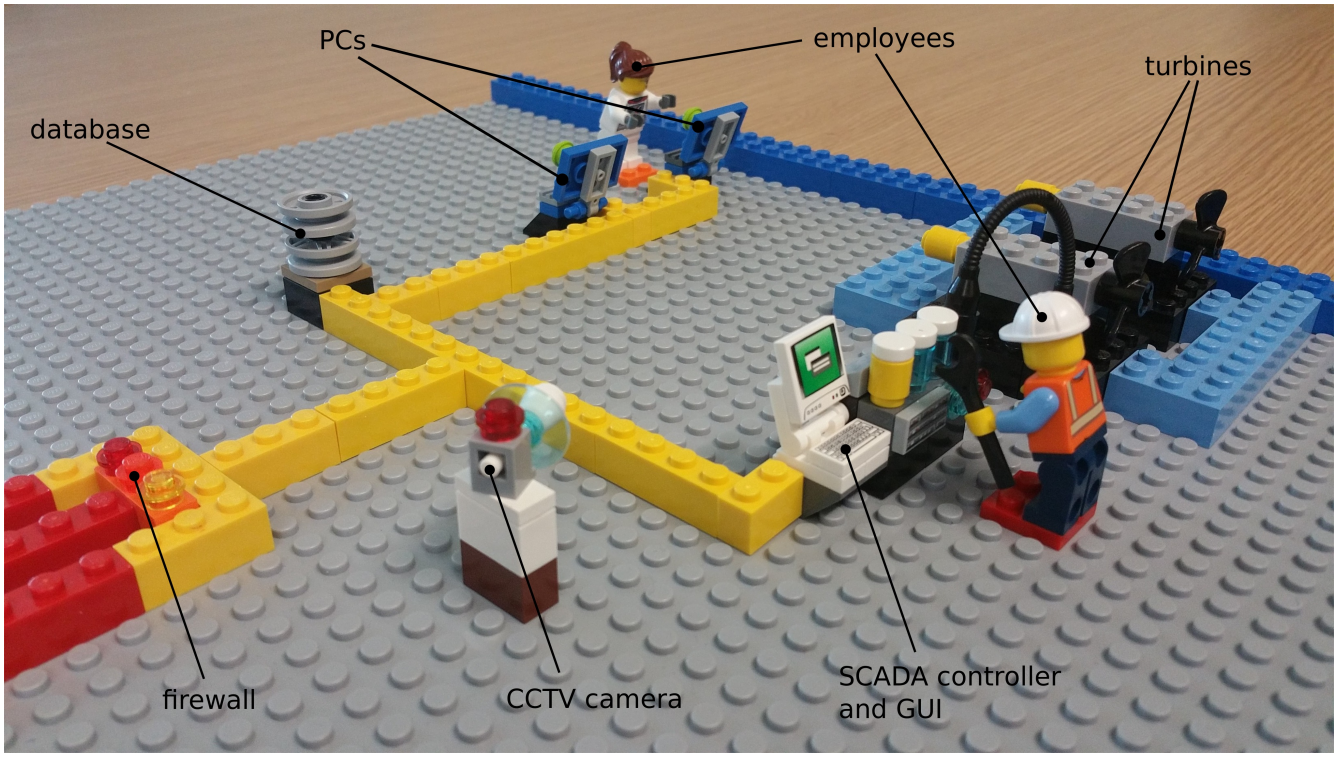
Describing the game board

The game board is a physical representation of the infrastructure that the players are defending. We provide the following description as a reference, with important elements to point on the board highlighted in **bold**:

I will now walk you through our premises and show you around our infrastructure. First is the ***plant*** *which hosts power generators: you can see a* ***river*** *in blue at the back and two* ***turbines*** *driven by the stream. The turbines are controlled by a* ***SCADA controller****, maintained by this* ***technician*** *with the wrench, and connected to the* ***local network*** *in yellow. This local network also hosts a number of* ***PCs*** *for* ***local engineers and technicians****, and a* ***database*** *that stores monitoring values produced by the SCADA controller: water debit, power production, etc. The plant's network (in yellow) is connected to the* ***Internet*** *(in red) via this* ***router****.*

The second site is the ***remote offices****, also connected to the Internet its own* ***router****. The offices'* ***local network*** *(in white) also hosts a number of* ***PCs*** *for employees:* ***managers, Human Resources, engineers, analysts****. The company runs its own* ***email and web server****, connected to a local* ***database*** *for storing emails, HR records, technical and financial data, etc.*





TODO: polish pictures + offices picture

Describing the defences

After showing the game board to the players and answering their questions, the Game Master should present them with available defences. Take the time to show the cards one by one, read the description text on the cards and present the associated figures. Refer again to the Frequently Asked Questions section if need be.

Supervising player decisions

The players should be now ready to start taking their first decisions and debating what defences are the most appropriate. As the Game Master, you should try not to influence their discussions: you know about the attack scenario and which defences are indeed the most important. The players should be left ignorant of what will happen precisely, although investing in a threat assessment will give them precious clues regarding the threats they are facing.

Try therefore to answer their questions in a neutral way and not to give indices regarding what would be right or wrong player decisions. Making mistakes is a valid way of learning, and the final debriefing phase of the game will be the occasion for them to understand what went wrong.

Some groups of players have a hard time taking decisions and keep debating forever. A simple and neutral way of speeding things up is to organise a quick vote: ask each player to mention the one defence they think is the most important, and to justify it briefly. Optionally, the player can also point out one defence that they think is not a priority. A round of vote like this can help identifying clear favourites among the defences, especially at the beginning of turn 1 when many options are available. Do not hesitate to organise several such voting rounds. The actual decision, however, should always follow player consensus: voting for important defences is simply a way to speed up the debates and eliminate unlikely candidates for an investment.

End of turn 1: deployment, attacks, consequences

Once the players have decided wich defences to invest in, remove their cards from the table, and deploy the corresponding figures on the game board. The **Defences** section (p. 14) contains text descriptions of what happens when the defences are deployed in the infrastructure: read them to the players.

It is now time to run the attacks for turn 1. Refer to the **Attacks** section (p. 22) and describe to the players what happens during the two months following their investments. This (usually grim) phase ends the turn.

After turn 1: the game goes on

For the following turns, the players are already familiar with the infrastructure and defences. They are, however, likely to be surprised by the attacks that just happened at the end of the previous turn. Start again the process of debating which defences should be invested in, with a fresh budget plus any leftovers from the previous turn. In general, players take their decisions much more quickly after the first turn. They should be careful however: sticking to one's initial ideas is not always the optimal decision. Good players will be able to understand the threats behind the attacks and adapt their decisions accordingly.

Turn four: how to end the session

At the end of the game, i.e. after turn 4, the Game Master reveals to the players the full range of attackers they were facing, which attacks they deflected successfully and which ones beat their defences. This is an occasion for everyone to reflect on their decisions and evaluate their cyber-defence strategies.

Frequently Asked Questions (by the players)

Players will often ask questions as the Game Master describes the board and defences, but also later during the game. We have compiled the most frequent ones. Some of these can be answered directly by the Game Master, some will require the players to first invest in an Asset Audit (see **Defences** section p. 14). In case a unexpected question comes, the Game Master must make up their own answer. Providing answers that are both realistic and consistent is important for players to immerse in the world of *D&D*, think in terms of what they would do in real life and forget that they are actually playing a game.

Q: Where are these sites situated?
A: The field site is somewhere in a mountainous area of the UK (e.g. the Lake District). The offices occupy one floor of a corporate building somewhere in a city centre, a few dozen miles from the field site (e.g. Barrow in Furness).

Q: How many employees does the company have?
A: The company has a few dozen employees: around 20 in total working in the field site, and a little bit more working in the offices. The company is an independent branch of a larger, national utility, which explains why they have their own clients, IT infrastructure, management, etc.

Q: How old is the company? The infrastructure?
A: The company has been running for a few decades already. Some legacy parts of the infrastructure (for instead, the canal derivating water from the river) date back to the early days. The IT infrastructure has not been updated in years. For more details (OS versions, controller firmware, server software, known vulnerabilities), invest in an Asset Audit!

Q: What are the current cyber-security defences?
A: The company has been taking cyber-security into account only very recently. You (the players) are the very first to implement any sort of security. You can therefore expect to start from the ground up. For instance: there is no firewalls, no antivirus, no security updates for the software and operating systems.

Q: Is there any communications between the two sites?
A: Employees from both sites communicate constantly via our email server, who is publicly visible on the Internet. Other than that, monitoring data is pulled every day from the plant's database to the offices for strategic analysis: how much are we producing, what is the performance

of the generators, etc. This is used to make predictions about the future, for maintenance planning, and to decide strategic investments such as an equipment replacement. There is no direct control of the generators from the offices: the plant's controller is the only one that can stop the physical process in case of an emergency, for instance.

Q: What if we don't spend all our budget?
A: Any money left will carry over to the next turn. For instance, if there is £20,000 left at the end of this turn, then the budget for the next turn will be £120,000.

Q: Can we have more budget?
A: This is a classic: almost every group will ask for a bigger budget. It is important to reply to this query in-game, as the board of directors, and *not* as the Game Master. A typical way of handling this situation is to ask the players to make a case justifying why they want more budget. Then, the boards of directors grants or refuses this extra budget, based for instance on their (potentially flawed) perception of the threats on the company. An easy way of dismissing the query is to use stonewalling along the lines of: *The board of directors has taken your demand into careful consideration. Given that you have been doing an excellent job so far (for instance, there has been no detected attacks) they fully trust you to carry your mission within the limits of your current allocated budget.*

Q: What OS / firmware / software runs on the PCs? Server? Database? Controller?
Q: Are there known vulnerabilities in the infrastructure?
Q: Can we update the PCs? Server? Database? Controller?
Q: Is anything encrypted? Can we encrypt it?
A: All these require the players to invest first in an Asset Audit for the

Game Master to provide answers. New defences will be unlocked that will allow the players to defend the vulnerabilities the Audit revealed, cf. **Defences** section p. 14.

Q: TODO
A:

Assets & Defences

The Game Board (Assets)

TODO: Pictures of all figures + descriptive text

Defences

Defences are represented by cards with an associated lego figure. Each card displays information such as:

- Defence name
- Defence cost
- A short description

In this section, we provide additional information for the Game Master (players should not read this!):

- A description of what happens when the defence is deployed in the infrastructure, to be read to the players after they invest in it.
- A description of the defence's effect when it stops an attack, to be read when the attack is countered (not when describing the defence to the players!).

Initially the players have access to the following defences only:

- all *Firewalls*
- *Anti-Virus*
- *Security Training*
- *Asset Audit*
- *Threat Assessment*
- all *CCTV*
- all *Network Monitoring*

CCTV Surveillance (Offices) : 50k
Description: A set of surveillance camera and alarms that will automatically warn security guards of an intrusion in the offices.
Deployment: **TODO:**
Defence effect: Counters *On-site Infiltration (Offices)*: An intruder is detected entering the offices and trying to open some doors. The moment the security guard comes and ask them what they are doing around, they run away.

CCTV Surveillance (Plant) : 50k
Description: A set of surveillance camera and alarms that will automatically warn security guards of an intrusion in the field site.
Deployment: **TODO:**
Defence effect: Counters *On-site Infiltration (Plant)*: An intruder is detected entering the plant perimeter and trying to access the buildings. The moment the security guard comes and asks them what they are doing around, they run away.

Firewall (Office) : 30k
Description: A software and hardware solution that monitors and filters unauthorized traffic coming from the Internet to the office network.
Deployment: **TODO:**
Defence effect: Counters *Network Scan (Offices)*: The firewall intercepts a number of scanning attemps from all over the world. Apparently, there is people out there very interested in knowing more about your servers.

Firewall (Plant) : 30k
Description: A software and hardware solution that monitors and filters unauthorized traffic coming from the Internet to the plant network.
Deployment: **TODO:**
Defence effect: Counters *Network Scan (Plant)*: The firewall intercepts a number of scanning attemps from all over the world. Apparently, there is people out there very interested in knowing more about your infrastructure.

Software Patches (PCs) : 30k
Description: A brand new, up-to-date OS and software suite for all your Personal Computers, including continuous support and security patches.
Deployment: **TODO:**
Defence effect: Counters *Remote Vulnerability Exploit (PCs)*: This defence is silent, unless the players have deployed a Network Monitor in the corresponding network. In that case, the Network Monitor shows in its logs failed attempts at exploiting the remote vulnerabilities on PCs: good thing that the OS were up to date.

Software Patches (Servers & DB) : 30k
Description: A brand new, up-to-date OS, web server and database management system, including continuous support and security patches.
Deployment: **TODO:**
Defence effect: Counters *Remote Vulnerability Exploit (Servers & DBs)*: The logs of the server show that someone on the Internet tried to use an SQL injection to compromise the server. This would have affected the old version of the software, by fortunately, the vulnerability has been patched.

Software patches (Controller) : 30k
Description: An update to the firmware of the SCADA controller.
Deployment: **TODO:**
Defence effect: Counters *Remote Vulnerability Exploit (Controller)*: This defence is silent, unless the players have deployed a Network Monitor in the field site network. In that case, the Network Monitor shows in its logs failed attempts at accessing an old, insecure remote access facility that has been disabled in the new version of the firmware.

Anti-virus : 30k
Description: A recent, decent professional anti-virus from a reputable provider, good enough to stop common malware. Support and continuous updates are included in the price.
Deployment: **TODO:**
Defence effect: Counters *Trojan-infected Thumb Drive, Phishing Attack*: Upon pluging in a thumb drive / opening an attachment, the anti-virus fires an alert and announces that a malicious program has been stopped from running on the computer. Upon closer inspection, it was indeed a real threat, and the PC was properly protected: disaster averted!

Security Training : 30k
Description: A quick yet thorough one-day formation on security essentials for all employees: Do not click on random links while browsing the Web. Do not open email attachments from unknown sources. Do not bring personal thumb drives to work, especially when you don't know where they come from! Here is how to design a secure, easy to remember password. And do not put it on a sticky note on your monitor! Etc.
Deployment: **TODO:**
Defence effect: Counters *Phishing Attack & Trojan-Infected Thumb Drive*. Upon receiving an email with an attachment from an unknown source / finding a thumb drive in the parking lot, an employee reports it directly to you (the players). Upon close inspection, the attachment / thumb drive did indeed contain malware. Good thing the employee knew better than opening it themselves!

Network Monitoring (Offices) : 50k
Description: A sophisticated piece of hardware and software that will record everything that is going on in the office network: web browsing, email, remote access, etc. An advanced detection system will signal any suspicious activity: malware signatures on the network, unexpected remote access, data being exfiltrated, etc. This big, shiny piece of bleeding-edge technology is quite expensive but also very effective: it will indeed detect any kind of attack going on in the office network and allow immediate measure to be taken, such as isolating infected machines, blocking unauthorized traffic, and telling exactly what is going on.
Deployment: **TODO:**
Defence effect: Detects??? *Remote Control ??? & Data Theft ???*:

Network Monitoring (Plant) : 50k
Description: A sophisticated piece of hardware and software that will record everything that is going on in the plant network: web browsing, email, remote access, etc. An advanced detection system will signal any suspicious activity: malware signatures on the network, unexpected remote access, data being exfiltrated, etc. This big, shiny piece of bleeding-edge technology is quite expensive but also very effective: it will indeed detect any kind of attack going on in the plant network and allow immediate measure to be taken, such as isolating infected machines, blocking unauthorized traffic, and telling exactly what is going on.
Deployment: **TODO:**
Defence effect: Detects??? *Remote Control ??? & Data Theft ???*:

Encryption (PCs) : 20k
Description: A robust, proven encryption mechanism for the hard drives of all PCs (plant and offices), protecting technical documentation, client information, and other sensitive data from being stolen.
Deployment: **TODO:**
Defence effect: Counters *Data Theft*:

Encryption (DBs) : 20k
Description: A robust, proven encryption mechanism for the hard drives of the two databases (plant and offices), protecting the technical data, email, client information, and other sensitive data from being stolen.
Deployment: **TODO:**
Defence effect: Counters *Data Theft*:

Asset Audit : 30k
Description: The entire infrastructure is thoroughly assessed for vulnerabilities. The following additional defences are unlocked: all *Software Patches* and *Encryption*. In addition, an unsecured Wi-Fi network on the plant is detected and closed (counters *Unsecured Wi-Fi Infiltration*).
Deployment: **TODO:**
Defence effect:

Threat Assessment : 20k
Description: Reveals existing threats to the company, the attack vectors they use, and the possible effects of their attacks (*Disruption* and *Data Theft*). Script kiddies with low skill but numerous, and therefore very likely (*Network Scans*, *DoS Attacks*, *Phishing*); organised crime, with high skill and highly motivated, quite likely (*Infected Thumb Drive*); nation states, with the highest techniques and technologies, but quite unlikely (*On-Site Infiltration*).
Deployment: **TODO:**
Defence effect:

Attackers & Attacks

			× Encryption DB	× Encryption DB
Phishing Kiddie	Phishing offices (trojan) × Training × Antivirus × Patches PCs	Disruption PC offices × Antivirus × Patches PCs	Disruption PC offices × Antivirus × Patches PCs	Disruption PC offices × Antivirus × Patches PCs
Mafia APT PC Offices	Infected USB offices × Training × Anti-virus PC	Remote Control PC offices × Anti-virus PC × Network monitoring offices	Data exfiltration PC offices × Anti-virus PC × Encryption PCs × Network monitoring offices	Data exfiltration PC offices × Anti-virus PC × Encryption PCs × Network monitoring offices
Mafia APT Server Offices	Phishing offices (credentials) × Training	Remote Control Server offices × Network monitoring offices	Data exfiltration DB offices × Network monitoring offices × Encryption DB	Data exfiltration DB offices × Network monitoring offices × Encryption DB
Mafia APT Server Plant	Vulnerable Wi-Fi plant × Asset Audit	Remote Control DB plant × Patch server × Network monitoring plant	Data exfiltration DB plant × Network monitoring plant × Encryption DB	Data exfiltration DB plant × Network monitoring plant × Encryption DB
Mafia Disruption Controller	Scan plant × Firewall plant	Remote control Controller	Disruption controller × Patch con-	Disruption controller × Patch con-

After the Game