port:1010

1 HIT

Persistent Malware

Obfuscated code saved to the Common Log File System

port:1010

2 HIT

Signed Driver

Signed Razer mouse driver privilege escalation

port:1010

3 HIT

Browser Plugin

Malicious Chrome extension supply chain attack

port:1010

4 HIT

Malicious Driver

Malicious driver deployed for keyboard input interception

port:1010

5 HIT

New Service

Persistence using Windows service disguised as EDR updater

port:1010

6 HIT

Cloud Bucket

Data exfiltration through public cloud storage bucket

port:1010

7 HIT

New User Added

New user assetmgt created with administrator access

port:2472

1 HIT

Cloud Metadata

Cloud access through Instance Metadata Service exfiltration

port:2472

2 HIT

MFA Bypass

Office 365 MFA bypass using named location access

port:2472

3 HIT

Watering Hole

Redirected to malicious website through Facebook Messenger

port:2472

4 HIT

Cloud Account

Endpoints compromised through O365 Ruler payload delivery

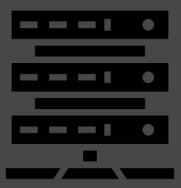
port:2472

5 HIT

Credential Stuffing

Citrix internal network access through reused credentials

port:2472



6 HIT

Web Shell

Persistent access to web server with isolated code

port:2472

7 HIT

Malicious Kubelet

Kubernetes takeover with malicious kubelet deployment

port:3800

1 HIT

Fake Installer

Gain access through a fake installer

port:3800

2 HIT

O365 Macro

Command execution through O365 Excel document macro

port:3800

3 HIT

Sysmon Reporting

Malicious PowerShell invocation detected

port:3800

4 HIT

Shadow Copy

Access protected SAM database using Volume Shadow Copy

port:3800

5HIT

Password Audit

DPAT reveals systemic password selection exposure

port:3800

6HIT

Sinkhole Domain

Malicious activity identified through a sinkhole DNS response

port:3800

7HIT

Log Analysis

SIEM logging analysis identifies APT activity

port:4545

1HIT

Persistent Malware

Obfuscated code saved to the Common Log File System

port:4545

2HIT

Signed Driver

Signed Razer mouse driver privilege escalation

port:4545

3HIT

Browser Plugin

Malicious Chrome extension supply chain attack

port:4545

4HIT

Malicious Driver

Malicious driver deployed for keyboard input interception

port:4545

5HIT

New Service

Persistence using Windows service disguised as EDR updater

port:4545

6HIT

Cloud Bucket

Data exfiltration through public cloud storage bucket

port:4545

7 HIT

New User Added

New user assetmgt created with administrator access

port:5600

1 HIT

Cloud Metadata

Cloud access through Instance Metadata Service exfiltration

port:5600

2 HIT

MFA Bypass

Office 365 MFA bypass using named location access

port:5600

3 HIT

Watering Hole

Redirected to malicious website through Facebook Messenger

port:5600

4 HIT

Cloud Account

Endpoints compromised through O365 Ruler payload delivery

port:5600

5 HIT

Credential Stuffing

Citrix internal network access through reused credentials

port:5600

6 HIT

Web Shell

Persistent access to web server with isolated code

port:5600

7 HIT

Malicious Kubelet

Kubernetes takeover with malicious kubelet deployment

port:6834

1 HIT

Fake Installer

Gain access through a fake installer

port:6834

2HIT

O365 Macro

Command execution through O365 Excel document macro

port:6834

3HIT

Sysmon Reporting

Malicious PowerShell invocation detected

port:6834

4HIT

Shadow Copy

Access protected SAM database using Volume Shadow Copy

port:6834

5HIT

Password Audit

DPAT reveals systemic password selection exposure

port:6834

6HIT

Sinkhole Domain

Malicious activity identified through a sinkhole DNS response

port:6834

7 HIT

Log Analysis

SIEM logging analysis identifies APT activity

exposed

PORT:1010

exposed

PORT:2472

exposed

PORT:3800

exposed

PORT:4545

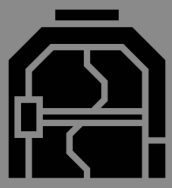
exposed

PORT:5600

exposed

PORT:6834

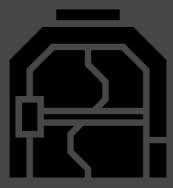
1



win to infiltrate

PORT:1010

2



wins to infiltrate

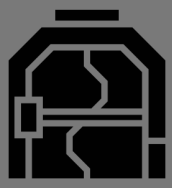
PORT:2472

3

wins to infiltrate

PORT:3800

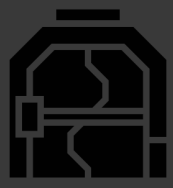
4



wins to infiltrate

PORT:4545

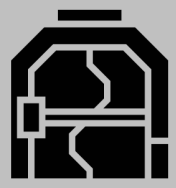
5



wins to infiltrate

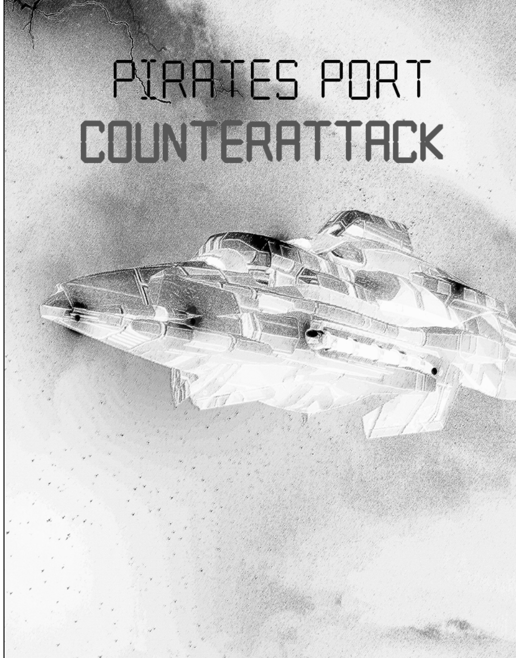
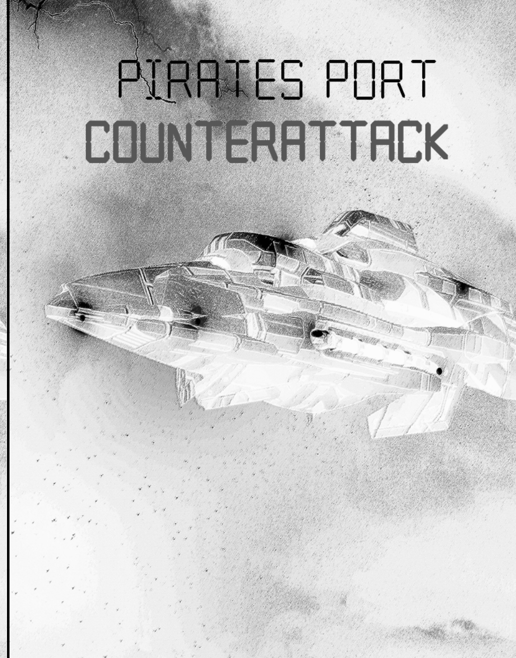
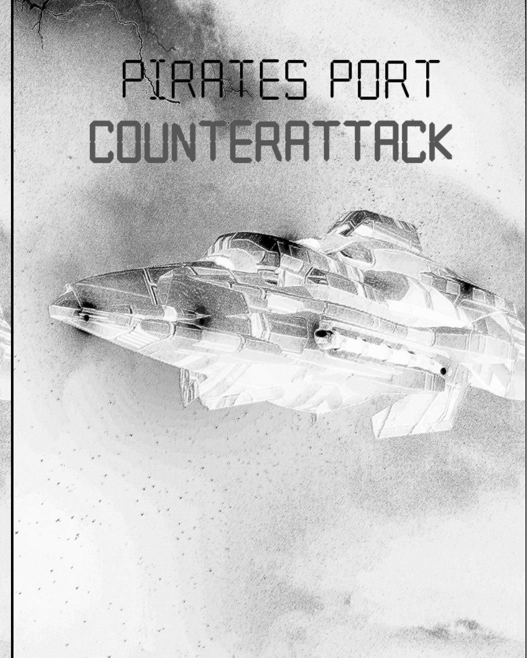
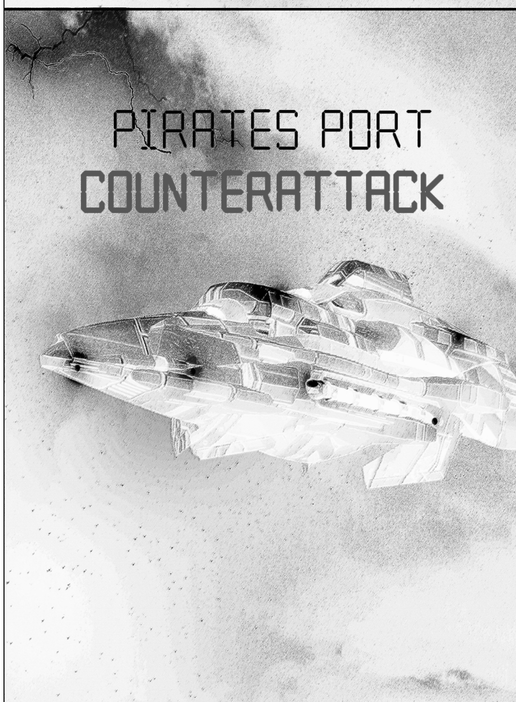
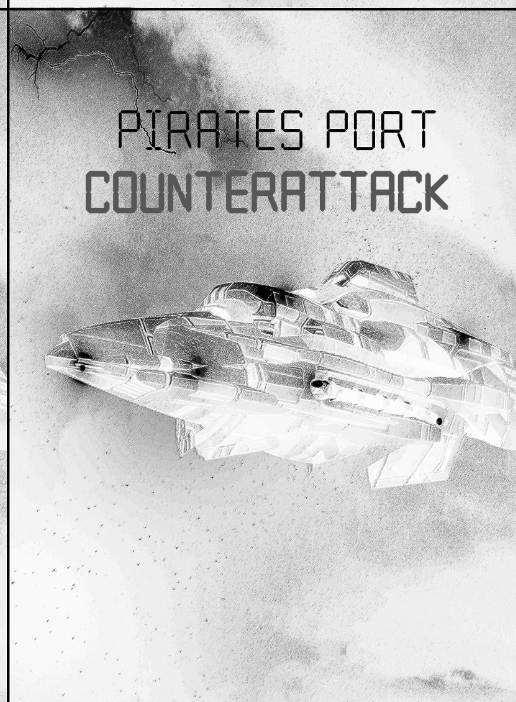
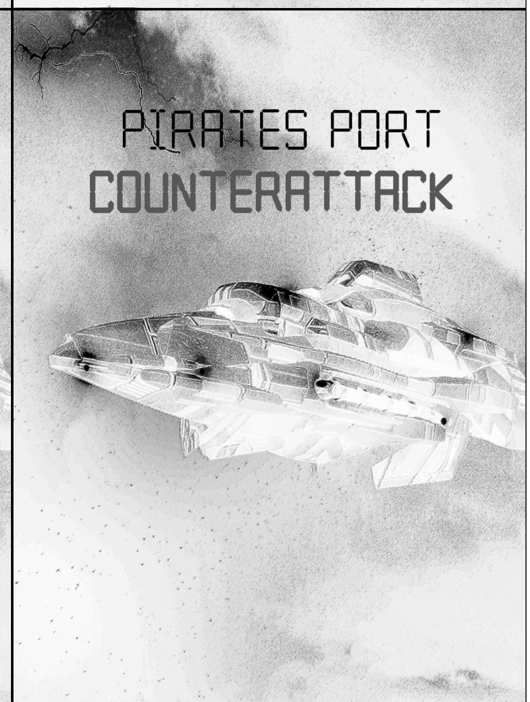
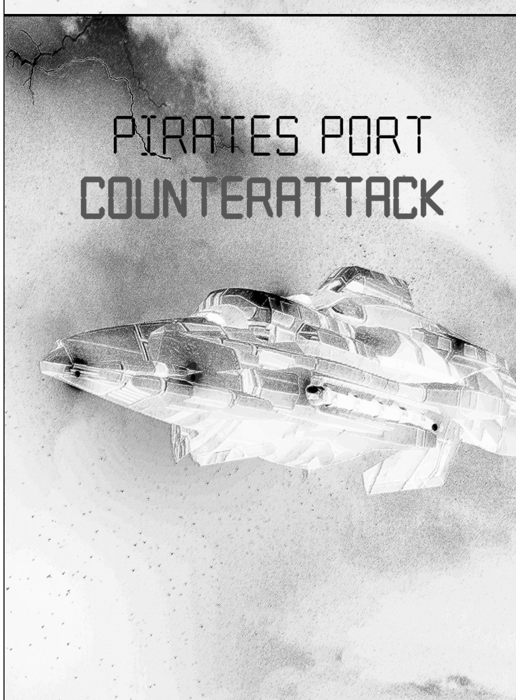
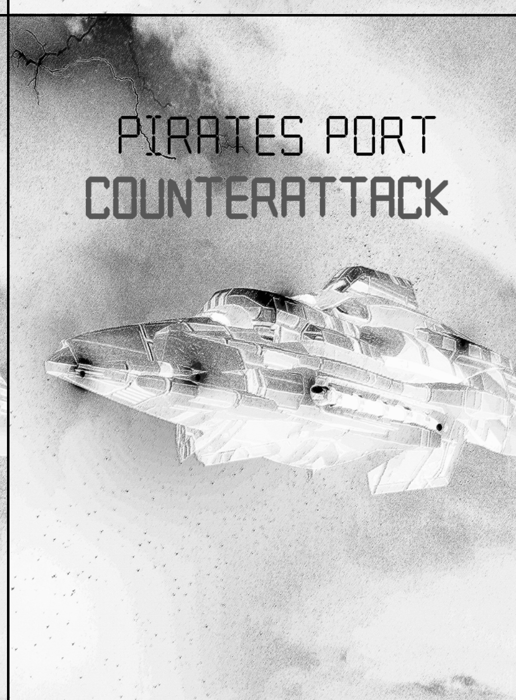
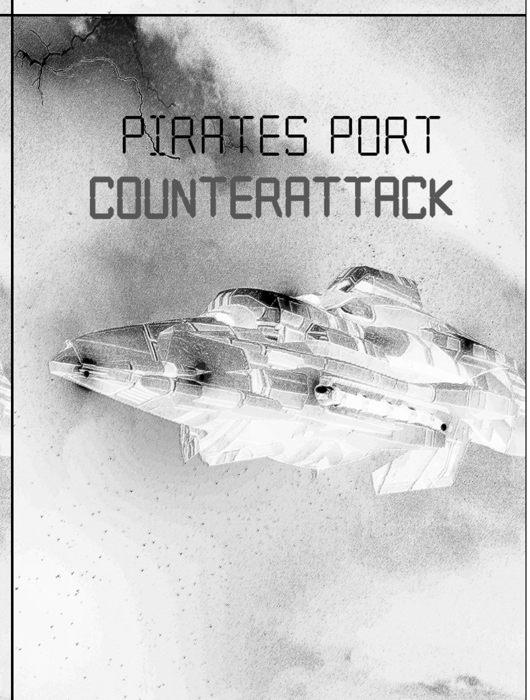
PORT:5600

6

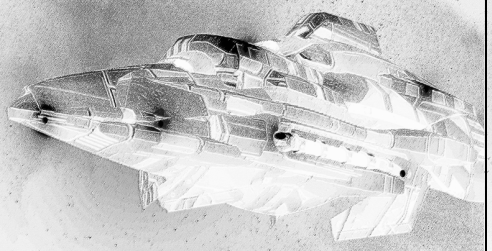


wins to infiltrate

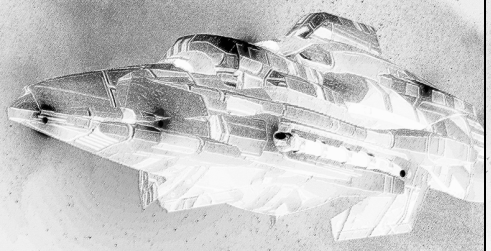
PORT:6834


PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

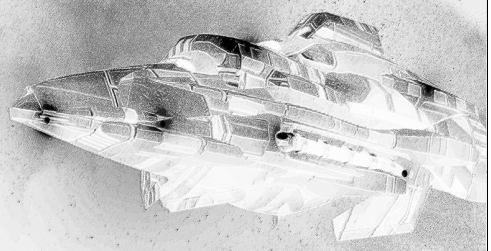

PIRATES PORT
COUNTERATTACK



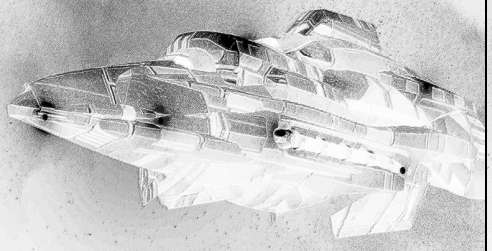
PIRATES PORT
COUNTERATTACK



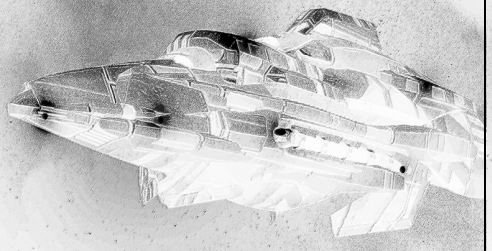
PIRATES PORT
COUNTERATTACK



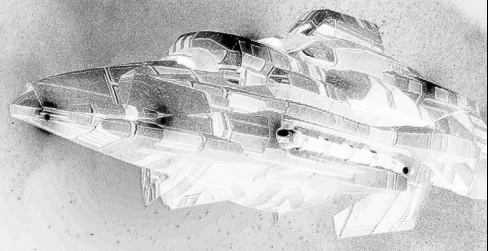
PIRATES PORT
COUNTERATTACK



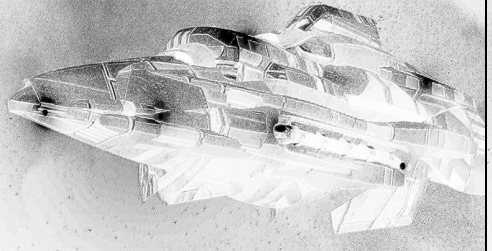
PIRATES PORT
COUNTERATTACK



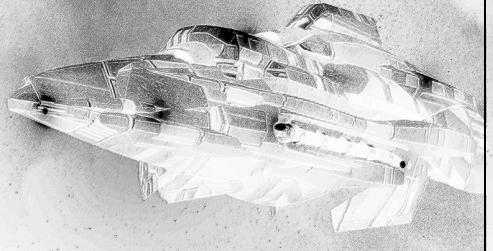
PIRATES PORT
COUNTERATTACK



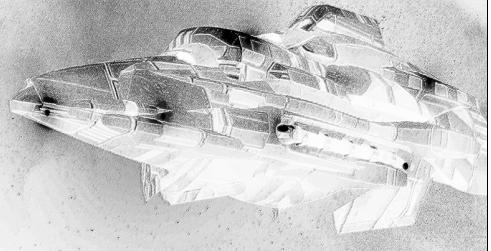
PIRATES PORT
COUNTERATTACK

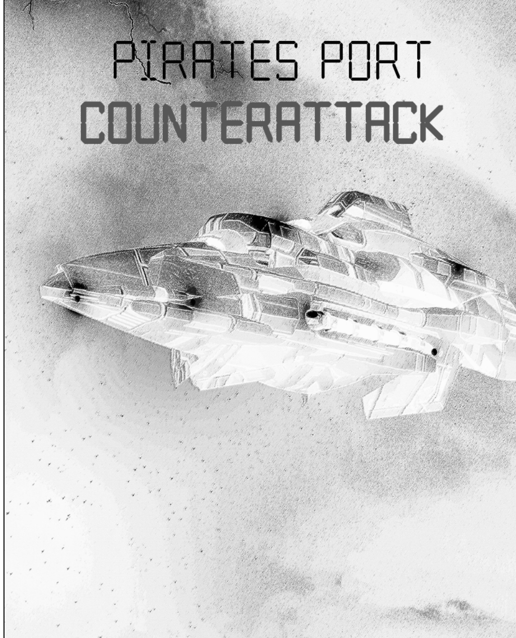
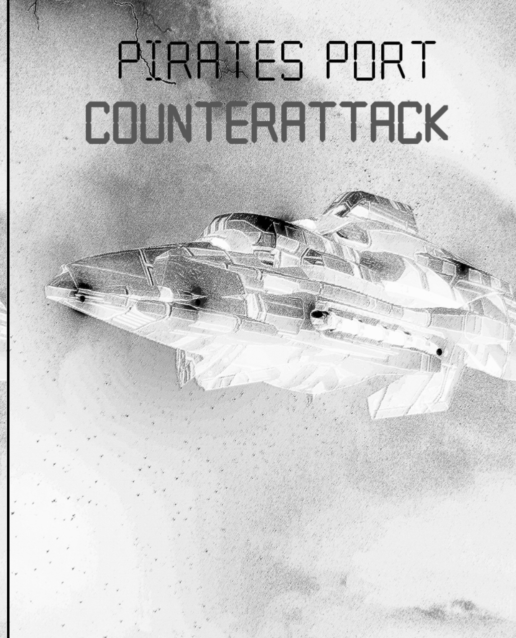
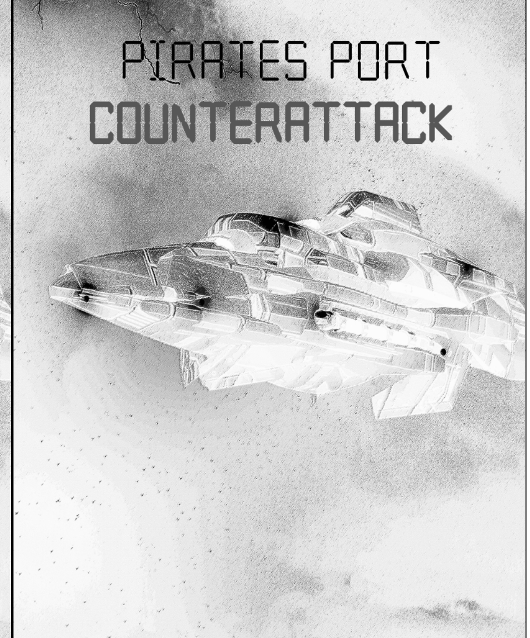
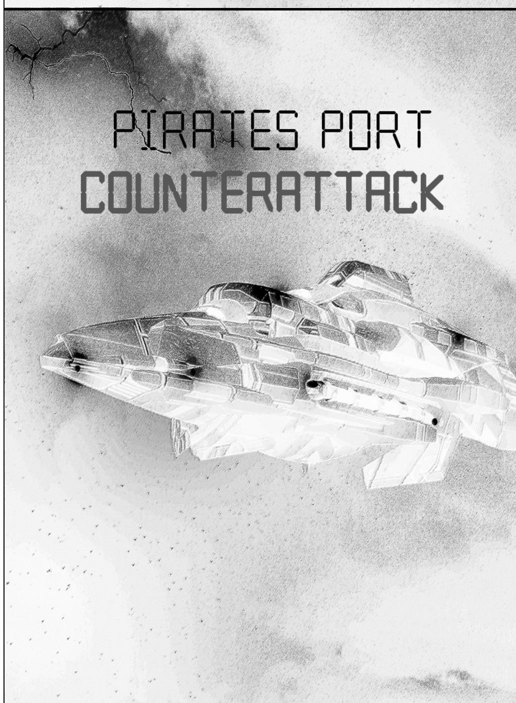
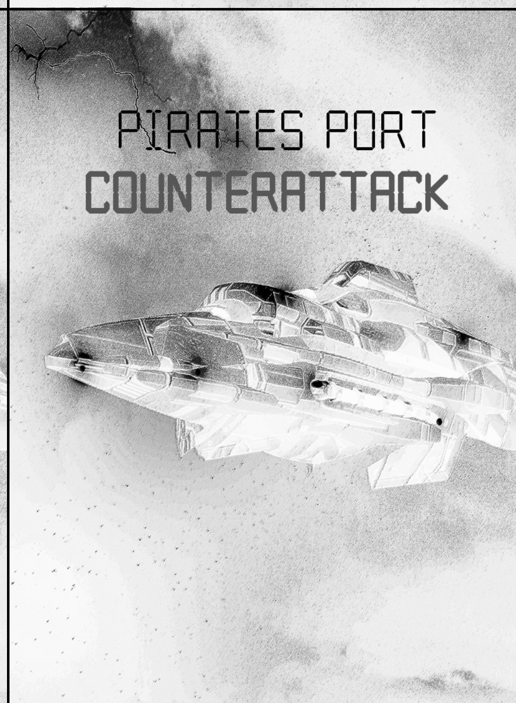
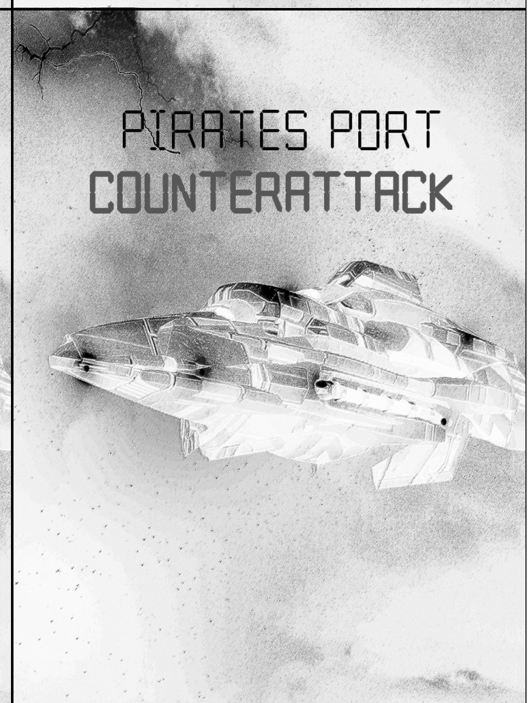
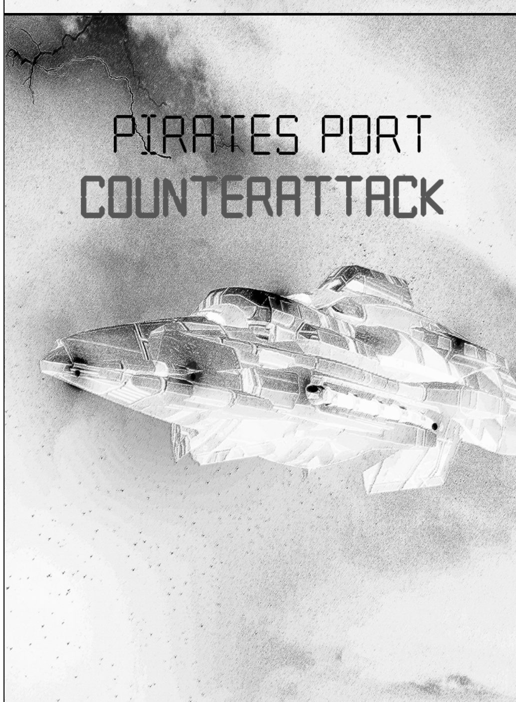
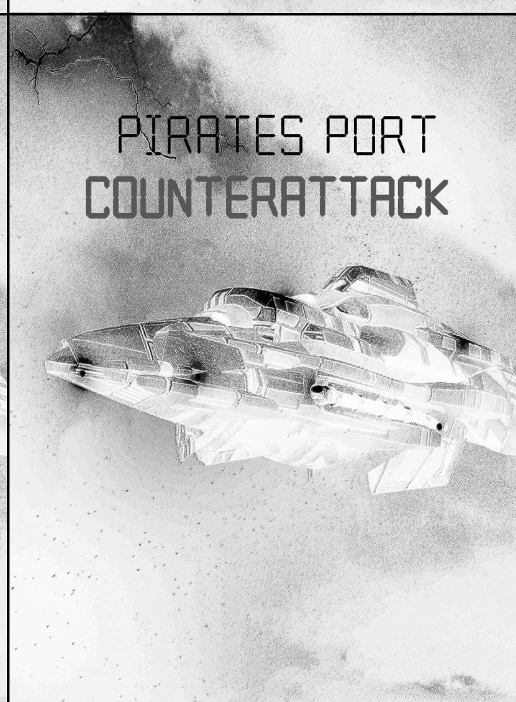
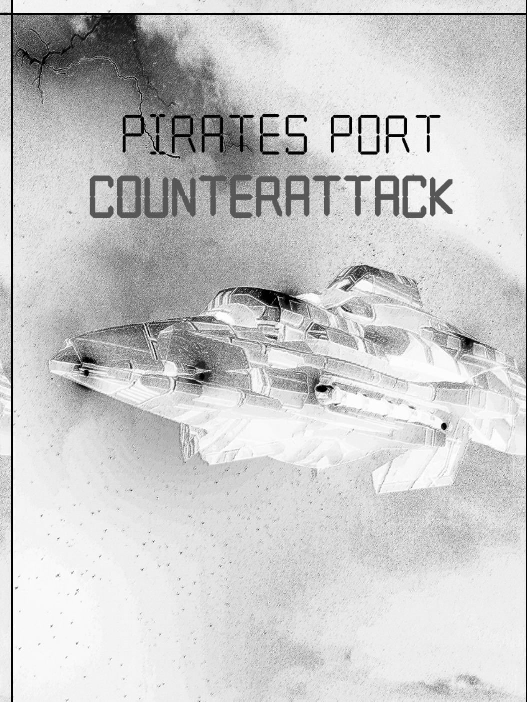


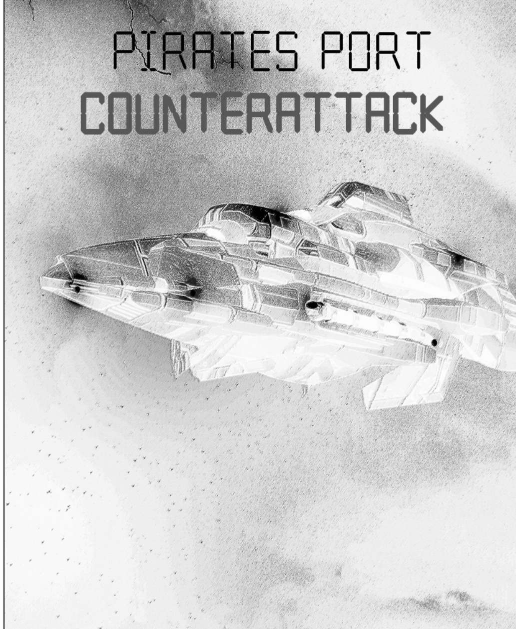
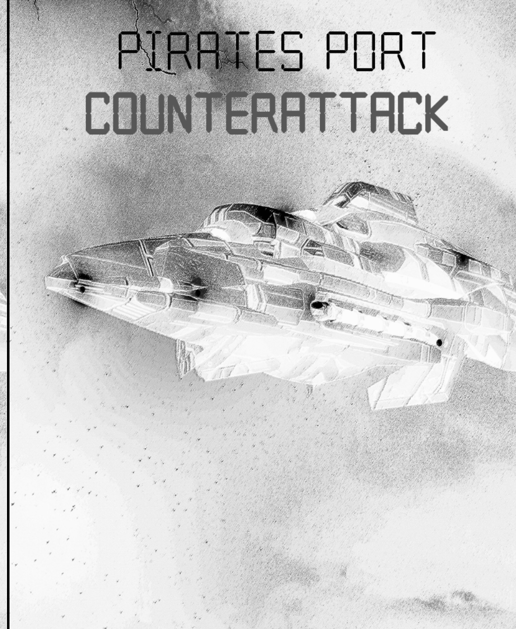
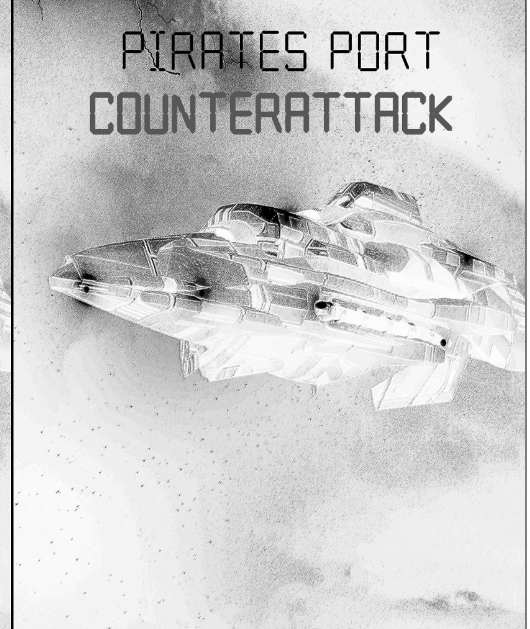
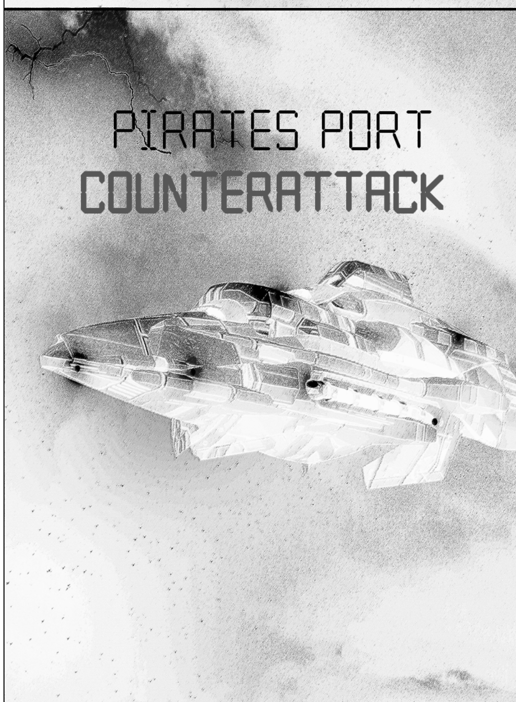
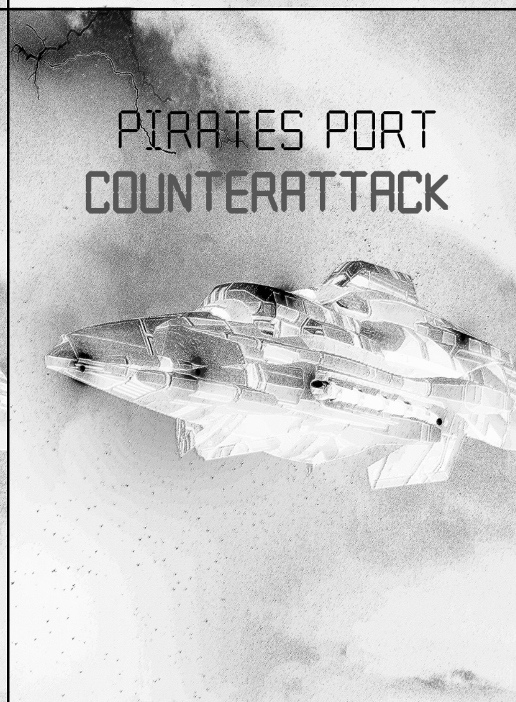
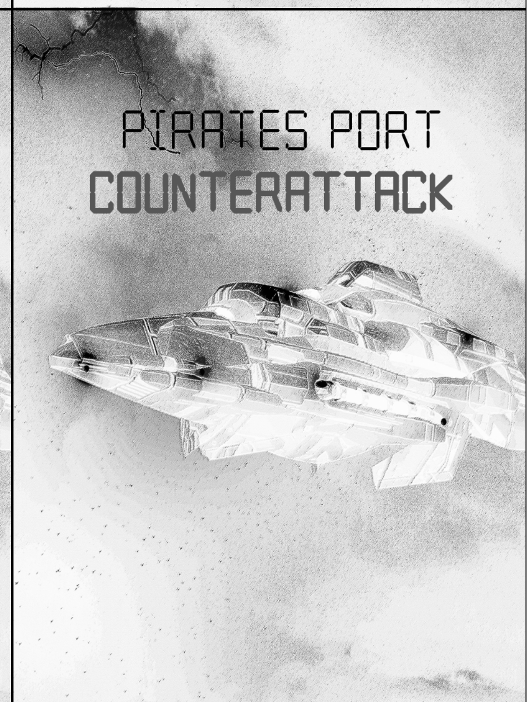
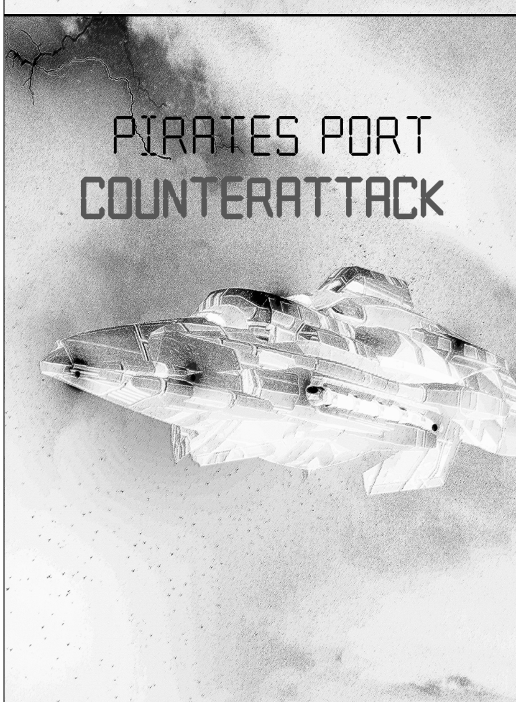
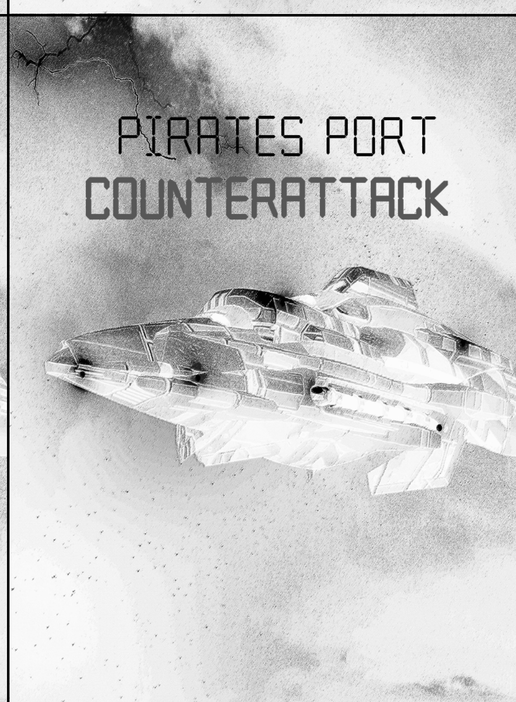
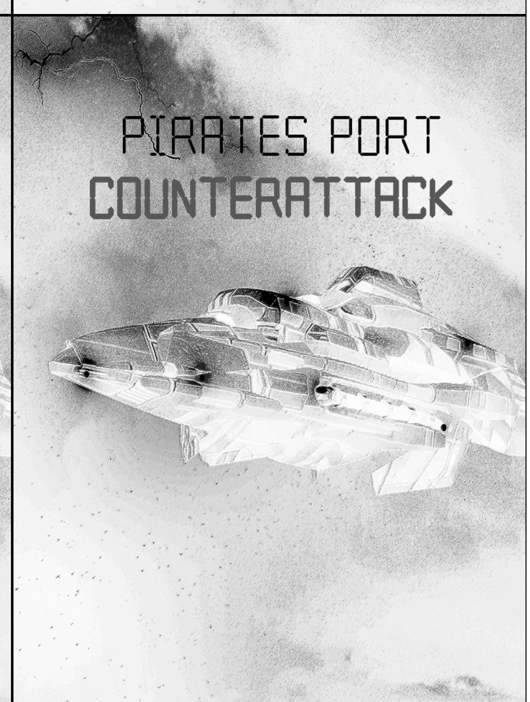
PIRATES PORT
COUNTERATTACK



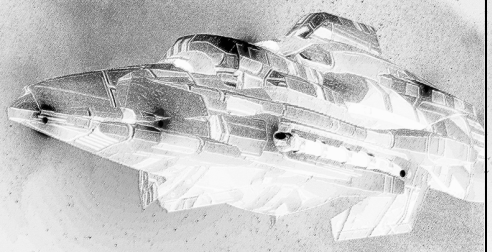
PIRATES PORT
COUNTERATTACK



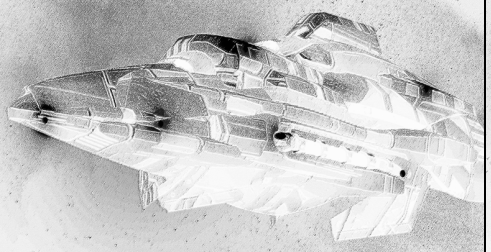

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK



PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

PIRATES PORT
COUNTERATTACK

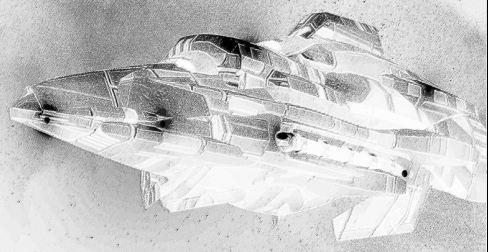

PIRATES PORT
COUNTERATTACK



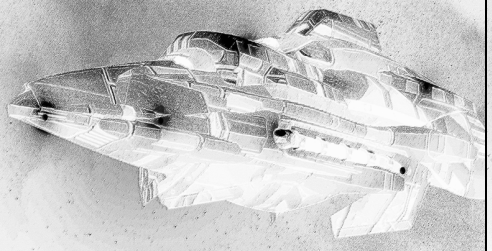
PIRATES PORT
COUNTERATTACK



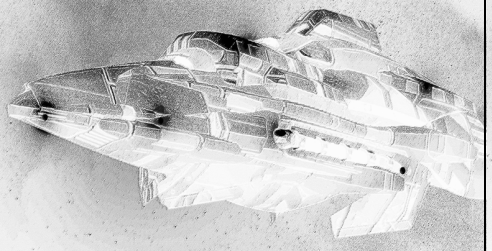
PIRATES PORT
COUNTERATTACK



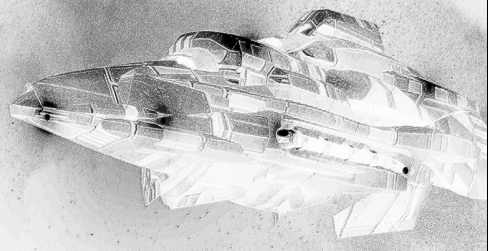
PIRATES PORT
COUNTERATTACK



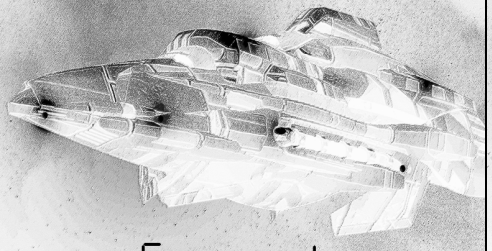
PIRATES PORT
COUNTERATTACK



PIRATES PORT
COUNTERATTACK

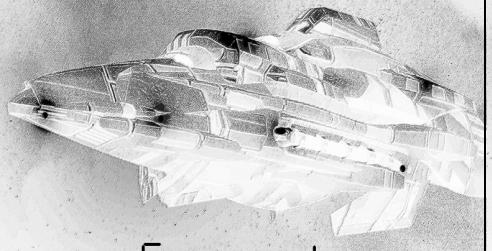


PIRATES PORT
COUNTERATTACK



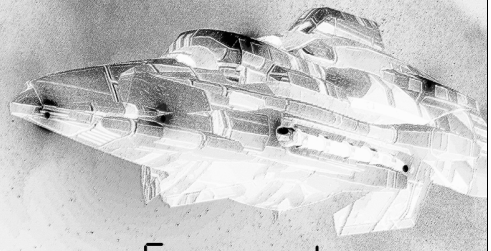
Exposed
Port

PIRATES PORT
COUNTERATTACK

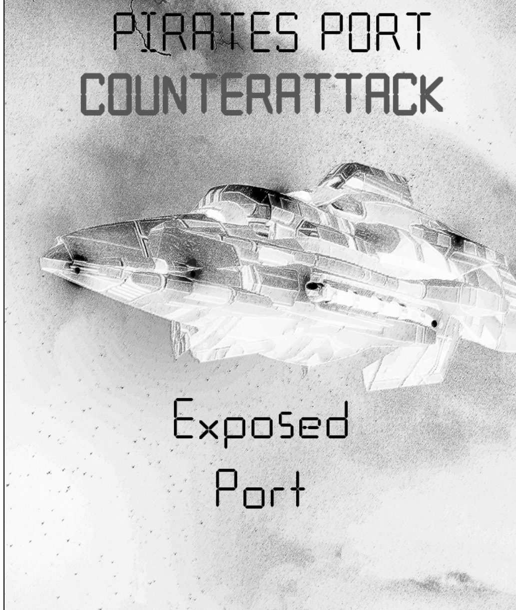


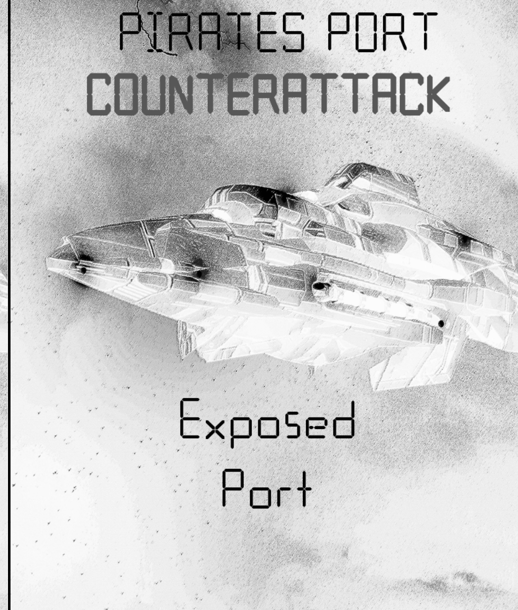
Exposed
Port

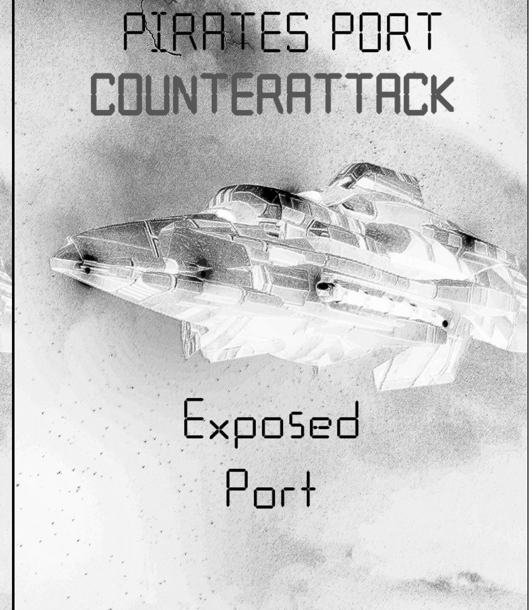
PIRATES PORT
COUNTERATTACK

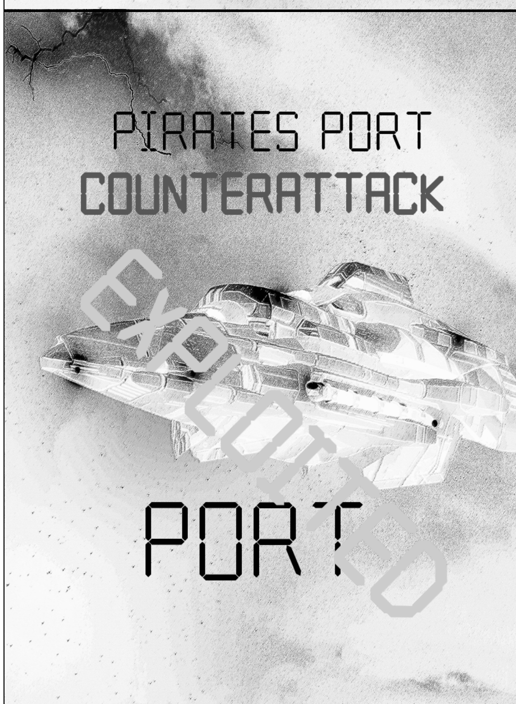


Exposed
Port

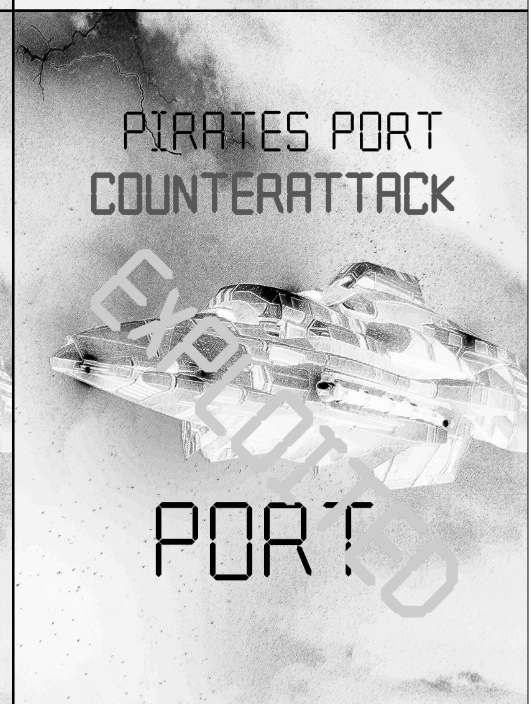

PIRATES PORT
COUNTERATTACK
Exposed
Port

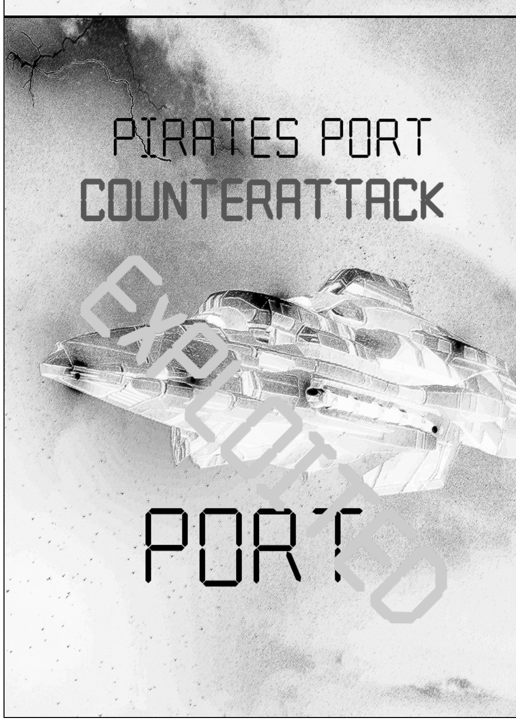

PIRATES PORT
COUNTERATTACK
Exposed
Port


PIRATES PORT
COUNTERATTACK
Exposed
Port

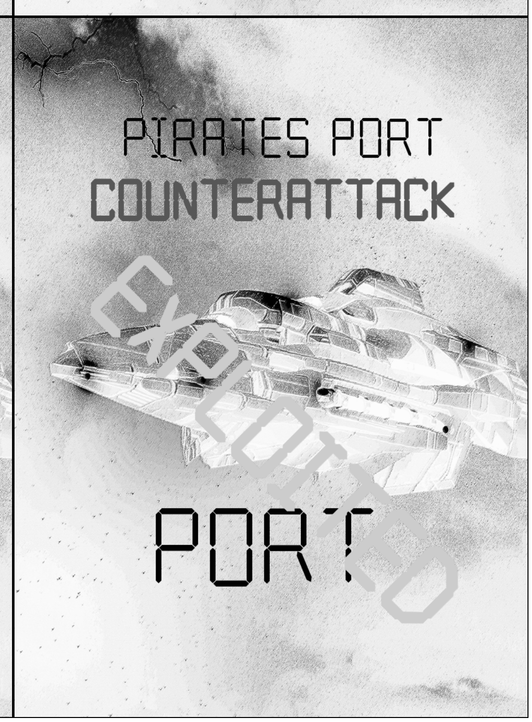

PIRATES PORT
COUNTERATTACK
EXPLOITED
PORT


PIRATES PORT
COUNTERATTACK
EXPLOITED
PORT


PIRATES PORT
COUNTERATTACK
EXPLOITED
PORT


PIRATES PORT
COUNTERATTACK
EXPLOITED
PORT


PIRATES PORT
COUNTERATTACK
EXPLOITED
PORT


PIRATES PORT
COUNTERATTACK
EXPLOITED
PORT