

Cyber Defenses Table

	Defense: Diplo	Defense: Info	Defense: Military	Defense: Econ
Australia (Starting Def: 5)				
Canada (Starting Def: 4)				
China (Starting Def: 9)				
France (Starting Def: 3)				
Japan (Starting Def: 5)				
Philippines (Starting Def: 3)				
Taiwan (Starting Def: 5)				
UK (Starting Def: 4)				
US (Starting Def: 7)				
Commercial	2	2	3	1

CLASSIFIED GREYSCALE//GREYSCALE



UNITED STATES CYBER COMMAND

Sea Shadow

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.
3. *Target:* Any friendly naval unit.
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: USCYBERCOM

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)

CLASSIFIED GREYSCALE//GREYSCALE



UNITED STATES CYBER COMMAND

Nietzschean Abyss

Brigade Headquarters Wiper Capability

1. *Scope:* Operational
2. *Effect:* Utilize access to an enemy headquarters to deploy wipers to wipe information and render computers inoperable.
Unit has -1 Colum Shift in Combat Until Resolved
3. *Target:* Any chosen PLA Brigade [Military]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: USCYBERCOM

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)

To Target: _____ [Brigade]



UNITED STATES CYBER COMMAND

Sharp Blindness

Command and Control (C2) Vulnerability Exploit

1. *Scope:* Strategic
2. *Effect:* Covert exfiltration of information from Chinese Eastern Theater Command (ETC) systems. The vulnerability may be used to deploy an offensive payload to seriously degrade enemy C2.
If used passively, may get one answer to 1 question within ETC's purview.
If used Actively, ETC may issue no new orders until resolved.
3. *Target:* PLA Eastern Theater Command [Military]
4. *Projected Chance of Success Against an Undefended Target*
70% (Active), 90% (Passive)

Requiring Authorization By: POTUS (Active)

(Severe Risk of Escalation in Multiple Scenarios)

Requiring Authorization By: Commander, CYBERCOM (Passive)

(Risk of Valuable Vulnerably Loss)

Authorized: _____ (POTUS)



UNITED STATES CYBER COMMAND

Stop Loss

Narrative Bombardment

1. *Scope:* Operational
2. *Effect:* Ramp up political leaning and induce action in Chinese dissident populations across Pacific and CONUS.
Move the World Public Opinion tracker by 1.
3. *Target:* Global English-Speaking Populations [Information]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: USCYBERCOM
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)



UNITED STATES CYBER COMMAND

Blinding Nobody

PLA ISR Satellite Vulnerability

1. *Scope:* Operational
2. *Effect:* Degrade and disrupt PLA ISR satellite constellations to remove their ability to detect US and allied forces and conduct battle damage assessment.
Reduce Chinese detection rolls by 1 until resolved. No dynamic targeting with long range missiles allowed past the first island chain.
3. *Target:* PLA ISR Constellations [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: USCYBERCOM
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)



UNITED STATES CYBER COMMAND

Dead Exchange

PLA Communications Satellite Vulnerability

1. *Scope:* Operational
2. *Effect:* Degrade and disrupt PLA communication satellite constellations to remove their coordinate and direct action.
PLA may issue no orders to units at sea more than 3 hexes away from China until resolved.
3. *Target:* PLA Comms Constellations [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: USCYBERCOM
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)



UNITED STATES CYBER COMMAND

Clouded Vision

Brigade Headquarters Wiper Capability

1. *Scope:* Operational
2. *Effect:* Utilize access to a enemy headquarters to deploy wipers to wipe information and render computers inoperable.
Unit has -1 Colum Shift in Combat Until Resolved
3. *Target:* Any chosen PLA Brigade [Military]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: USCYBERCOM
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)

To Target: _____ [Brigade]



UNITED STATES CYBER COMMAND

Violent Awdry

Rail Infrastructure Vulnerability Exploit

1. *Scope:* Strategic
2. *Effect:* Exploit vulnerabilities to target singling systems and timetables to disrupt the enemies rail network.
Chinese units may not conduct rail movement, -1 to PLA units mobilizing to Green readiness, and no PLA days of supply are accrued until resolved.
3. *Target:* Chinese Civilian Rail Infrastructure [Economic]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: POTUS

(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (POTUS)



UNITED STATES CYBER COMMAND

Rushing Water

Hydrophone Spoofing Attack

1. *Scope:* Operational
2. *Effect:* Inject fake contacts and discard real contacts into PLA Hydrophone Data to degrade enemy ASW efforts.
Place 4 decoys. The PLA gains no bonus from Hydrophones to ASW Detection until resolved.
3. *Target:* PLA Hydrophone Arrays [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: USCYBERCOM

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)



UNITED STATES CYBER COMMAND

Evasive Heights

IADS Degradation Capability

1. *Scope:* Operational
2. *Effect:* Disrupt, degrade, and destroy enemy systems and equipment to reduce sensor coverage and communication between SAM batteries, aircraft, and command nodes.
All Chinese IADS are reduced by 1 until resolved.
3. *Target:* PLA Integrated Air Defense System [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: USCYBERCOM

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOM)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Full Docket

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.

3. *Target:* Any friendly naval unit.

4. *Projected Chance of Success Against an Undefended Target*

90%

Requiring Authorization By: Commander, PLACF

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, PLACF)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Bottled Lightning

Brigade Headquarters Wiper Capability

1. *Scope:* Operational
2. *Effect:* Utilize access to an enemy headquarters to deploy wipers to wipe information and render computers inoperable.
Unit has -1 Colum Shift in Combat Until Resolved
3. *Target:* Any chosen ROC or Philippines Brigade [Military]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: Commander, PLACF
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, PLACF)

To Target: _____ [Brigade]



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Shining Star

IADS Degradation Capability

1. *Scope:* Operational
2. *Effect:* Disrupt, degrade, and destroy enemy systems and equipment to reduce sensor coverage and communication between SAM batteries, aircraft, and command nodes.
Taiwanese IADS is reduced by 1 until resolved.
3. *Target:* Taiwanese Integrated Air Defense System [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: Vice Chairman, CMC
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Vice Chairman, CMC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Blind King**Command and Control (C2) Vulnerability Exploit**

1. *Scope:* Operational
2. *Effect:* Covert exfiltration of information from US Pacific Air Force (PACAF) systems. The vulnerability may be used to deploy an offensive payload to seriously degrade enemy C2.

If used passively, may get one answer to 1 question within PACAF's purview. If used actively, PACAF may only generate ½ normal sorties and Tanker costs for Reinforcement are increased by 1 until resolved.

3. *Target:* US PACAF [Military]
4. *Projected Chance of Success Against an Undefended Target*
80% (Active), 90% (Passive)

Requiring Authorization By: Vice Chairman, CMC
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Vice Chairman, CMC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Deep Echo**Hydrophone Spoofing Attack**

1. *Scope:* Operational
2. *Effect:* Inject fake contacts and discard real contacts into US Hydrophone Data to degrade enemy ASW efforts.
Place 4 decoys. US Hydrophones have a 50% chance to fail to detect until resolved.

3. *Target:* US Hydrophone Arrays [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: Vice Chairman, CMC
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Vice Chairman, CMC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Lighted Whispers**Command and Control (C2) Vulnerability Exploit**

1. *Scope:* Operational
2. *Effect:* Covert exfiltration of information from Republic of China Army (ROCA) systems. The vulnerability may be used to deploy an offensive payload to seriously degrade enemy C2.
If used passively, may get one answer to 1 question within ROCA's purview. If used actively, ROCA units have -1 column shift and move 1 hex less until resolved.
3. *Target:* ROCA [Military]
4. *Projected Chance of Success Against an Undefended Target*
80% (Active), 90% (Passive)

Requiring Authorization By: Vice Chairman, CMC
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Vice Chairman, CMC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Confused Retainers**US Logistics Vulnerability Exploit**

1. *Scope:* Operational
2. *Effect:* Exploit vulnerabilities in the US Military's logistics systems to create issues to disrupt the flow of reinforcements and supplies into theater.
On the Reinforcement Track tanker costs are doubled and all dice rolls to move units roll twice and use the lower result until resolved.
3. *Target:* US Military Logistics Systems [Military]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: Vice Chairman, CMC
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Vice Chairman, CMC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Blank Look

Narrative Bombardment

1. *Scope:* Operational
2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.
Move the Filipino, Japanese Will to Fight, or the World Public Opinion tracker by 1.
3. *Target:* Global English-Speaking Populations [Information]
4. *Projected Chance of Success Against an Undefended Target*

90%

Requiring Authorization By: Commander, PLACF

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, PLACF)



MINISTRY OF STATE SECURITY

国家安全部

Dial Tone

**Taiwanese Contracted Commercial Communications Satellite
Vulnerability**

1. *Scope:* Strategic
2. *Effect:* Degrade, disrupt, and destroy Taiwanese contracted communication satellites to remove their ability to direct and coordinate action on their outlying islands.
If undersea cables are cut, Taiwanese forces may issue no orders or have no communication to forces on outlying islands until resolved.
3. *Target:* Commercial Comms Constellations [Commercial Military]
4. *Projected Chance of Success Against an Undefended Target*

80%

Requiring Authorization By: Minister of State Security

(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Minister of State Security)



MINISTRY OF STATE SECURITY

国家安全部

Rolling Darkness

UK CNI Vulnerability

1. *Scope:* Strategic
2. *Effect:* Use known vulnerabilities in the UK's power grid to cause mass blackouts.
The UK must discard 3 Will/Morale cards. 50% chance to reduce UK Will to Fight by 2.
3. *Target:* UK CNI [Economic]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: President of the PRC

(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (President of the PRC)



MINISTRY OF STATE SECURITY

国家安全部

Tropical Dusk

Philippines CNI Vulnerability

1. *Scope:* Strategic
2. *Effect:* Use known vulnerabilities in the Filipino power grid to cause mass blackouts in major cities in the Philippines.
The Philippines must discard 3 Will/Morale cards. 75% chance to reduce Filipino Will to Fight by 1, 25% chance to increase it by 2.
3. *Target:* Philippines CNI [Economic]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: President of the PRC

(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (President of the PRC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Lengthening Shadow

Taiwanese CNI Vulnerability

1. *Scope:* Strategic
2. *Effect:* Use known vulnerabilities in the Taiwanese power grid to cause mass blackouts on Taiwan.
Taiwan must discard 1 Will/Morale card. 25% chance to reduce Civilian, Politician, and Military Will to Fight by 1.
3. *Target:* Taiwanese CNI [Economic]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: Chairman, CMC

(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (Chairman, CMC)



PLA CYBERSPACE FORCE

中国人民解放军网络空间部队

Silent Waters

US CONUS Port Vulnerability Exploit

1. *Scope:* Operational
2. *Effect:* Exploit vulnerabilities in US commercial ports in the Continental United States (CONUS) to create issues to disrupt the flow of reinforcements and supplies into the Pacific.
US ground units may not embark via Sea Ports of Embarkation (SPOE) until resolved.
3. *Target:* US CONUS Port Systems [Economic]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: Vice Chairman, CMC

(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Vice Chairman, CMC)



MINISTRY OF STATE SECURITY

国家安全部

Under Dark

Australia CNI Vulnerability

1. *Scope:* Strategic
2. *Effect:* Use known vulnerabilities in the Australian power grid to cause mass blackouts in major cities in Australia.
Australia must discard 2 Will/Morale cards. 75% chance to reduce Australian Will to Fight by 1, 25% chance to increase it by 2.
3. *Target:* Australian CNI [Economic]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: President of the PRC

(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (President of the PRC)



MINISTRY OF STATE SECURITY

国家安全部

Thickened Ichor

US CONUS Oil Infrastructure Vulnerability

1. *Scope:* Strategic
2. *Effect:* Exploit vulnerabilities in US oil distribution networks in the Continental United States (CONUS) by targeting programmable logic controllers to create a major issue for the US government.
US discards 5 Will/Morale cards as messaging resources must be redirected. 75% chance to reduce US morale by 1, 25% chance to increase it by 2.
3. *Target:* US Oil Distribution Systems [Economic]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: President of the PRC

(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (President of the PRC)



MINISTRY OF STATE SECURITY

国家安全部

Echoing Abyss

Undersea Cable Vulnerability

1. *Scope:* Strategic
2. *Effect:* Exploit vulnerabilities in undersea cables to cut 95% of Taiwan's bandwidth to the rest of the world
Taiwanese non-diplomatic players may communicate only by note with other teams until resolved.
3. *Target:* Undersea Cables to Taiwan [Commercial Economic]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: President of the PRC
(Severe Risk of Economic Disruption and Escalation Risk)

Authorized: _____ (President of the PRC)



MINISTRY OF STATE SECURITY

国家安全部

Screaming Harlan

STRACOM Denial Operation

1. *Scope:* Strategic
2. *Effect:* DDOS government websites, impersonate, fake, or hack politician and government spokespeople's social media, and spread fake news to deny the Taiwanese Government the ability to clearly and effectively message their people or the world.
DRM-2 on Taiwanese World Public Opinion Cards this turn.
3. *Target:* Taiwan [Information]
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: Minister of State Security
(Risk of Valuable Operation Loss)

Authorized: _____ (Minister of State Security)



**INFORMATION COMMUNICATIONS AND
ELECTRONIC FORCE COMMAND**

通信電子資訊參謀次長室

Marine Haze

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.

3. *Target:* Any friendly naval unit.

4. *Projected Chance of Success Against an Undefended Target*

90%

Requiring Authorization By: Commander, ICEFC

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, ICEFC)



INFORMATION COMMUNICATIONS AND
ELECTRONIC FORCE COMMAND

通信電子資訊參謀次長室

Earthbound Eagle
Headquarters Wiper Capability

1. *Scope:* Operational
2. *Effect:* Utilize access the PLAAF Airborne Corps headquarters to deploy wipers to wipe information and render computers inoperable.
PLAAF Airborne Corps units have -1 Colum Shift in Combat until Resolved
3. *Target:* PLAAF Airborne Corps [Military]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Chief of the General Staff
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Chief of the General Staff)



INFORMATION COMMUNICATIONS AND
ELECTRONIC FORCE COMMAND

通信電子資訊參謀次長室

Burning Letter
Narrative Bombardment

1. *Scope:* Operational
2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.
Increase Taiwanese's Civilians Will to Fight by 1. If discovered, potential negative effects to government and will to fight.
3. *Target:* The Taiwanese People [Information]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: President of Taiwan
(Clear Violation of Peacetime Laws and Norms)

Authorized: _____ (President of Taiwan)



INFORMATION COMMUNICATIONS AND
ELECTRONIC FORCE COMMAND

通信電子資訊參謀次長室

Silent Night

Australia CNI Vulnerability

1. *Scope:* Strategic
2. *Effect:* Use vulnerabilities in the Chinese power grid to cause mass blackouts in Fujian Province (directly across from Taiwan).
China must discard 1 Will/Morale card. Chinese logistics flows to Taiwan are reduced by 5% until resolved.
3. *Target:* Fujian Province [Economic]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Chairman, CMC
(Severe Risk of Economic Disruption, Civilian Harm, and Escalation Risk)

Authorized: _____ (Chairman, CMC)



INFORMATION COMMUNICATIONS AND
ELECTRONIC FORCE COMMAND

通信電子資訊參謀次長室

Lonesome Fish

Chinese Port Vulnerability Exploits

1. *Scope:* Operational
2. *Effect:* Exploit vulnerabilities in Chinese commercial ports to create issues to disrupt the loading of supplies and units.
50% chance to delay each Chinese ground unit loading at a port, and Chinese logistics flows to Taiwan are reduced by 50% until resolved.
3. *Target:* Chinese Port Systems [Economic]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Chief of the General Staff
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Chief of the General Staff)



SELF-DEFENSE FORCES CYBER DEFENSE UNIT

自衛隊サイバー防衛隊

Fleeting Darkness

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.
3. *Target:* Any friendly naval unit.
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: SDF CDU

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, SDF CDU)



SELF-DEFENSE FORCES CYBER DEFENSE UNIT

自衛隊サイバー防衛隊

Shattered Iron

Port Infrastructure Attack

1. *Scope:* Operational
2. *Effect:* Use access to port infrastructure to disable cranes, lock gates, and other actions to cause disruption.
-1 PLA unit may attempt to move from Green to Black readiness.
3. *Target:* Shantou, China [Economic]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Chief of the Joint Staff
(Some Risk to Civilians Posted, Some Economic Risk)

Authorized: _____ (Chief, Joint Staff)



SELF-DEFENSE FORCES CYBER DEFENSE UNIT

自衛隊サイバー防衛隊

Soft Bunk

Narrative Bombardment

1. *Scope:* Operational
2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.
Increase Japanese Will to Fight by 1. If discovered, extremely serious effects to government and will to fight.
3. *Target:* The Japanese Civilian Population [Information]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Prime Minister of Japan
(Clear Violation of Peacetime Laws and Norms)

Authorized: _____ (Prime Minister of Japan)



SELF-DEFENSE FORCES CYBER DEFENSE UNIT

自衛隊サイバー防衛隊

Whisperer in Shadow

Hydrophone Spoofing Attack

1. *Scope:* Operational
2. *Effect:* Inject fake contacts and discard real contacts into PLA Hydrophone Data to degrade enemy ASW efforts.
Place 4 decoys. The PLA gains no bonus from Hydrophones to ASW Detection until resolved.
3. *Target:* PLA Hydrophone Arrays [Military]
4. *Projected Chance of Success Against an Undefended Target*
80%

Requiring Authorization By: Chief of the Joint Staff
(Major Capability Important to Joint Warfighting)

Authorized: _____ (Chief, Joint Staff)



SELF-DEFENSE FORCES CYBER DEFENSE UNIT

自衛隊サイバー防衛隊

Open Waters

Chinese Port Vulnerability Exploits

1. *Scope:* Operational
2. *Effect:* Exploit vulnerabilities in Chinese commercial ports in Guangzhou to disrupt the loading of supplies and military units.
-1 PLA unit may attempt to move from Green to Black readiness, PLA loses 1 day of supply.
3. *Target:* Chinese Port Systems in Guangzhou [Economic]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Chief of the Joint Staff
(Major Capability Important to Joint Warfighting)

Authorized: _____ (Chief, Joint Staff)



CYBER COMMAND, JOINT CAPABILITIES GROUP

Stark Light

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.
3. *Target:* Any friendly naval unit.
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: CYBERCOMD

(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, CYBERCOMD)



CYBER COMMAND, JOINT CAPABILITIES GROUP

Right Pattern

Narrative Bombardment

1. *Scope:* Operational
2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message to the populations of the Pacific Small Islands Developing States (PSIDS).

Shift World Public Opinion by 1. If discovered, serious effects to governmental relations.

3. *Target:* PSIDS Population [Civilian Information]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Chief of the Defence Force
(Violation of Norms and Risk to Relations with Target States)

Authorized: _____ (Chief of the Defence Force)



CYBER COMMAND, JOINT CAPABILITIES GROUP

Reverse Inference

Chinese Port Manifest Vulnerability Exploit

1. *Scope:* Operational
2. *Effect:* Exploit vulnerabilities in PLA-Civilian maritime manifest management systems to create issues to disrupt the flow of reinforcements and supplies to Taiwan.
-1 PLA unit may attempt to move from Green to Black readiness, PLA loses 1 day of supply.

3. *Target:* PLA-Civilian Manifest System [Military/Economic]
4. *Projected Chance of Success Against an Undefended Target*
60%

Requiring Authorization By: Chief of the Defence Force
(Major Capability Important to Joint Warfighting)

Authorized: _____ (Chief of the Defence Force)



CYBER COMMAND, JOINT CAPABILITIES GROUP

Full Null

Stock Exchange Vulnerability

1. *Scope:* Strategic
2. *Effect:* Exploit vulnerabilities in the Beijing Stock Exchange to stop trading, destabilizing the economic system.
The Chinese must discard 1 Will/Morale card. Economic effects may result.
3. *Target:* Beijing Stock Exchange [Economic]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Prime Minister of Australia
(*Severe Risk of Economic Disruption and Escalation Risk*)

Authorized: _____ (Prime Minister of Australia)



CYBER SECURITY COMMAND

Open Blue

Narrative Bombardment

1. *Scope:* Strategic
2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.
Move the World Public Opinion Tracker by 1.
3. *Target:* Anti-PRC populations in SE Asian States [Civilian Information]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: President of the Philippines
(*Strategic Manipulation of Countries with which the Philippines Maintains Relations*)

Authorized: _____ (President of the Philippines)



CYBER SECURITY COMMAND

Sea Salt

Command and Control (C2) Vulnerability Exploit

1. *Scope:* Operational
2. *Effect:* Utilize access to headquarters in the Spratly Islands to covertly exfiltrate information. The vulnerability may be used to deploy an offensive payload to seriously degrade enemy C2.
*If used passively, may get an answer to 1 question within the HQ's purview.
If used Actively, Spratly Islands HQ may issue no new orders until resolved.*
3. *Target:* Spratly Islands HQ's [Military]
4. *Projected Chance of Success Against an Undefended Target*
80% (Active), 90% (Passive)

Requiring Authorization By: President of the Philippines (Active)

(Severe Risk of Escalation in Multiple Scenarios)

Requiring Authorization By: Commander, CYBERCOM (Passive)

(Risk of Valuable Vulnerably Loss)

Authorized: _____ (POTUS)



FRENCH CYBERSECURITY AGENCY (ANSSI)

Old Goose

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.
3. *Target:* Any friendly naval unit.
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: Director General, ANSSI

(No Undue Risk to Civilians Posted)

Authorized: _____ (Director General, ANSSI)



FRENCH CYBERSECURITY AGENCY (ANSSI)

Wise Lobster

Narrative Bombardment

1. *Scope:* Strategic
2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.

Move the World Public Opinion Tracker by 1.

3. *Target:* French Speaking Populations [Civilian Information]

4. *Projected Chance of Success Against an Undefended Target*

70%

Requiring Authorization By: President of France

(Strategic Manipulation of Countries with which the Philippines Maintains Relations)

Authorized: _____ (President of France)



FRENCH CYBERSECURITY AGENCY (ANSSI)

Wise Rooster

Stock Exchange Vulnerability

1. *Scope:* Strategic
2. *Effect:* Exploit vulnerabilities in the Shanghai Stock Exchange to stop trading, destabilizing the economic system.
The Chinese must discard 1 Will/Morale card. Economic effects may result.

3. *Target:* Shanghai Stock Exchange [Economic]

4. *Projected Chance of Success Against an Undefended Target*

70%

Requiring Authorization By: President of France

(Severe Risk of Economic Disruption and Escalation Risk)

Authorized: _____ (President of France)



National
Cyber Force

NATIONAL CYBER FORCE

Last Dusk

AIS Spoofing Capability

1. *Scope:* Tactical
2. *Effect:* Spoof Automatic identification Systems to create false ships and sea-clutter making it seem that the ship(s) are somewhere else.
Places a decoy with any naval unit that lasts for one turn.
3. *Target:* Any friendly naval unit.
4. *Projected Chance of Success Against an Undefended Target*
90%

Requiring Authorization By: Commander, National Cyber Force
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, NCF)



National
Cyber Force

NATIONAL CYBER FORCE

Full Out

Narrative Bombardment

1. *Scope:* Strategic

2. *Effect:* A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.

Move the World Public Opinion Tracker by 1.

3. *Target:* Global Human Rights Activists [Civilian Information]

4. *Projected Chance of Success Against an Undefended Target*

70%

Requiring Authorization By: Commander, National Cyber Force
(No Undue Risk to Civilians Posted)

Authorized: _____ (Commander, NCF)



National
Cyber Force

NATIONAL CYBER FORCE

Blinded Astronomer

Chinese Space Tracking Systems Vulnerability

1. *Scope:* Operational

2. *Effect:* Degrade and disrupt Chinese space tracking systems and data fusion to remove their ability to detect positions and movement of satellites.

Chinese forces may not launch kinetic ASAT attacks until resolved.

3. *Target:* Chinese Space Tracking Systems [Military]

4. *Projected Chance of Success Against an Undefended Target*

80%

Requiring Authorization By: Chief of the Defence Staff
(Risk of Valuable Vulnerably Loss)

Authorized: _____ (Chief of the Defence Staff)



CANADIAN ARMED FORCES CYBER COMMAND

Blind Harper

Narrative Bombardment

1. Scope: Strategic

2. Effect: A narrative bombardment involves the coordinated use of as many means as possible to push a select message for a specific target demographic.

Move the World Public Opinion Tracker by 1.

3. Target: Chinese Speaking Populations [Civilian Information]

4. Projected Chance of Success Against an Undefended Target

70%

Requiring Authorization By: Commander, CAFCYBERCOM

(No Undue Risk to Civilians or Diplomatic Relations)

Authorized: _____ (CO, CAFCYBERCOM)



CANADIAN ARMED FORCES CYBER COMMAND

Brilliant Leper

Chinese Telecoms Vulnerability

1. *Scope:* Strategic
2. *Effect:* Use known vulnerabilities in the Xinjiang Telecoms Infrastructure to disrupt and degrade general and specific targets to weaken the ability of the CCP to police the region.
Coordination of actions in Xinjaing becomes more difficult until resolved.
3. *Target:* Xinjiang Telecoms Infrastructure [Economic]
4. *Projected Chance of Success Against an Undefended Target*
70%

Requiring Authorization By: Prime Minister of Canada
(*Severe Risk of Significant Retaliation*)

Authorized: _____ (Prime Minister of Canada)