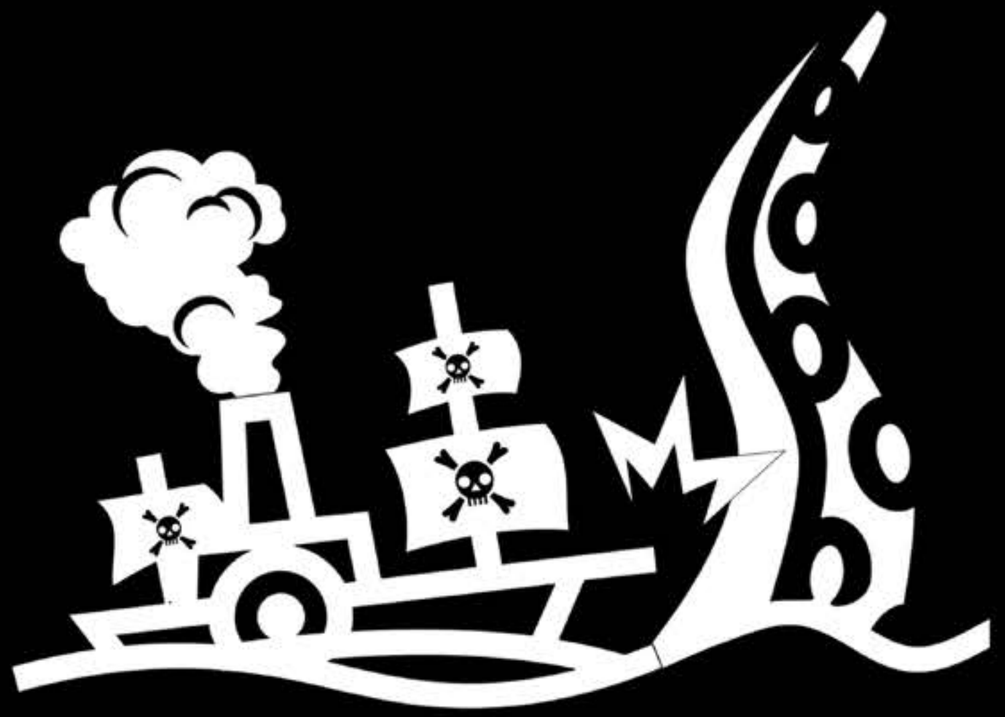
DAMN THE EXPLOITS!

FULL SPEED AHEAD!

HOW NAVAL FLEET TACTICS CAN REDEFINE CYBER OPERATIONS



1917

BRITISH BLOCKADE AROUND GERMANY

WORLD WAR 1

starving

AND RUNNING SHORT ON SUPPLIES, THE GERMANS REMOVED THE POLICY RESTRICTIONS PLACED ON SUBMARINE WARFARE

hopeful

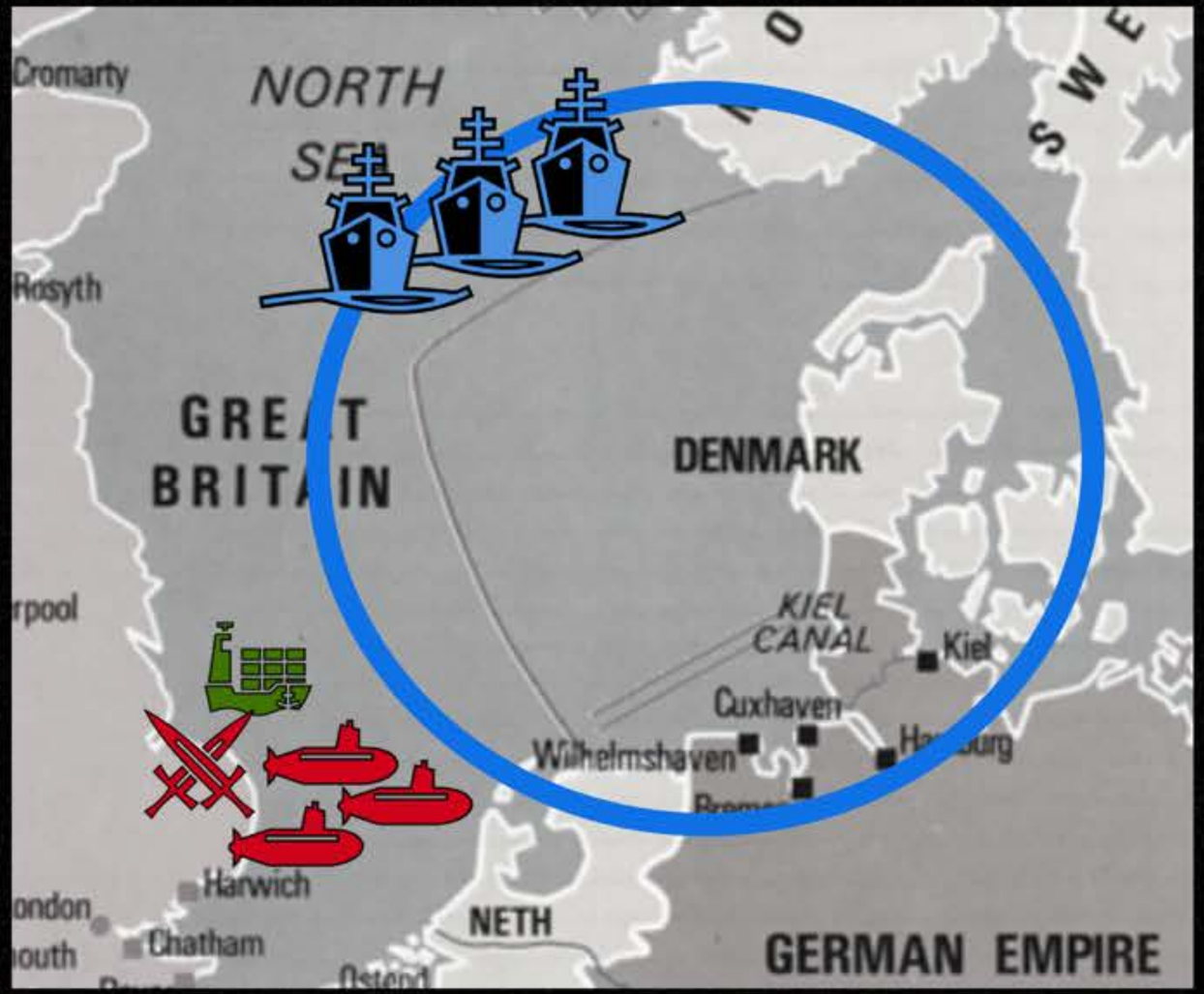
THAT SINKING AS MANY BRITISH SUPPLY SHIPS AS POSSIBLE WOULD FORCE THEM OUT OF THE WAR

unrestricted

SUBMARINE WARFARE TARGETED MERCHANT SUPPLY SHIPS AND LIGHTLY ARMORED COMBAT SHIPS

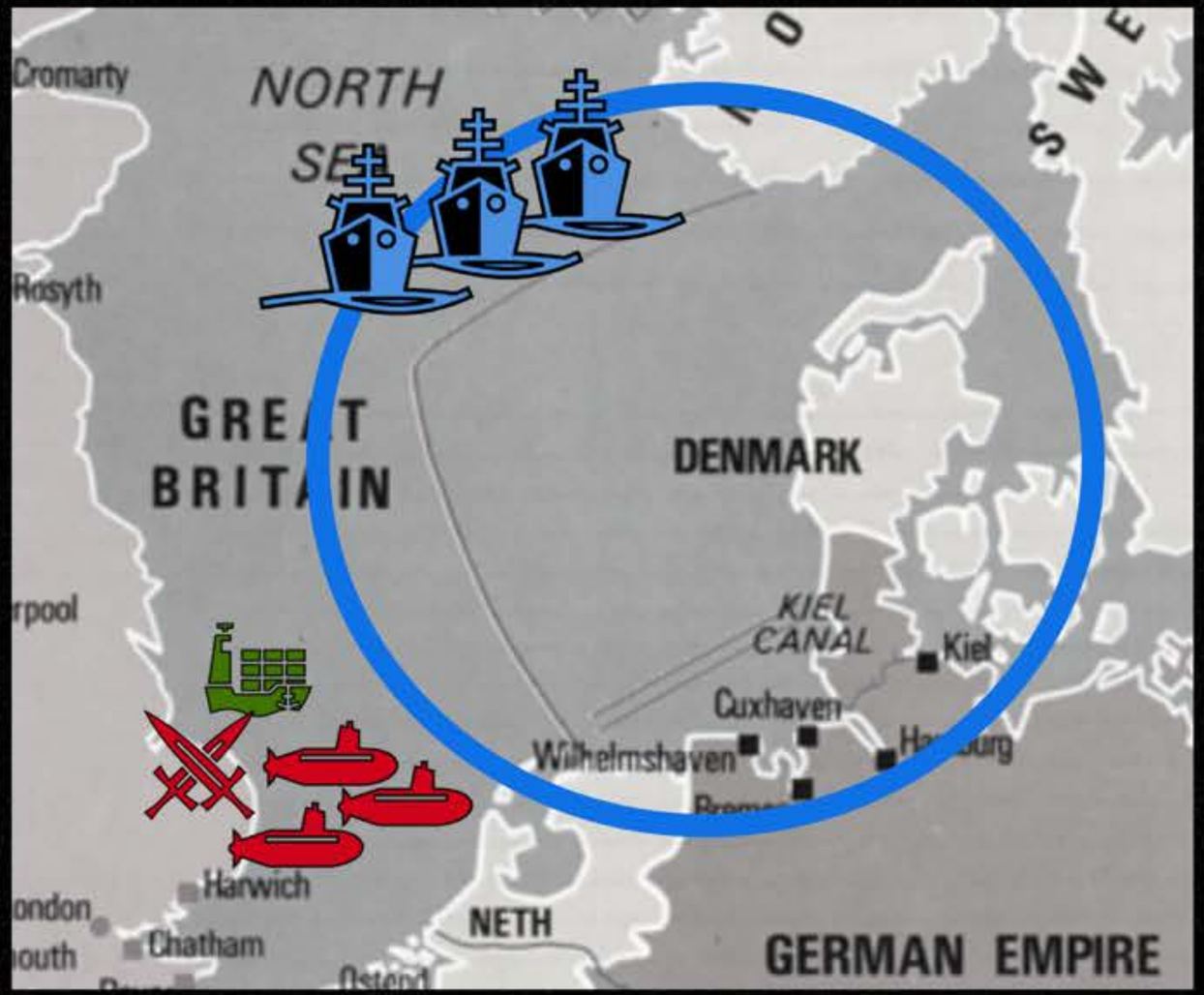
SUBMARINES EVADED THE BLOCKADE TO TAKE THE FIGHT TO SOFTER TARGETS

MUCH TO THE HORROR OF THOSE THAT FOLLOWED THE ESTABLISHED RULES OF WAR



breakthrough

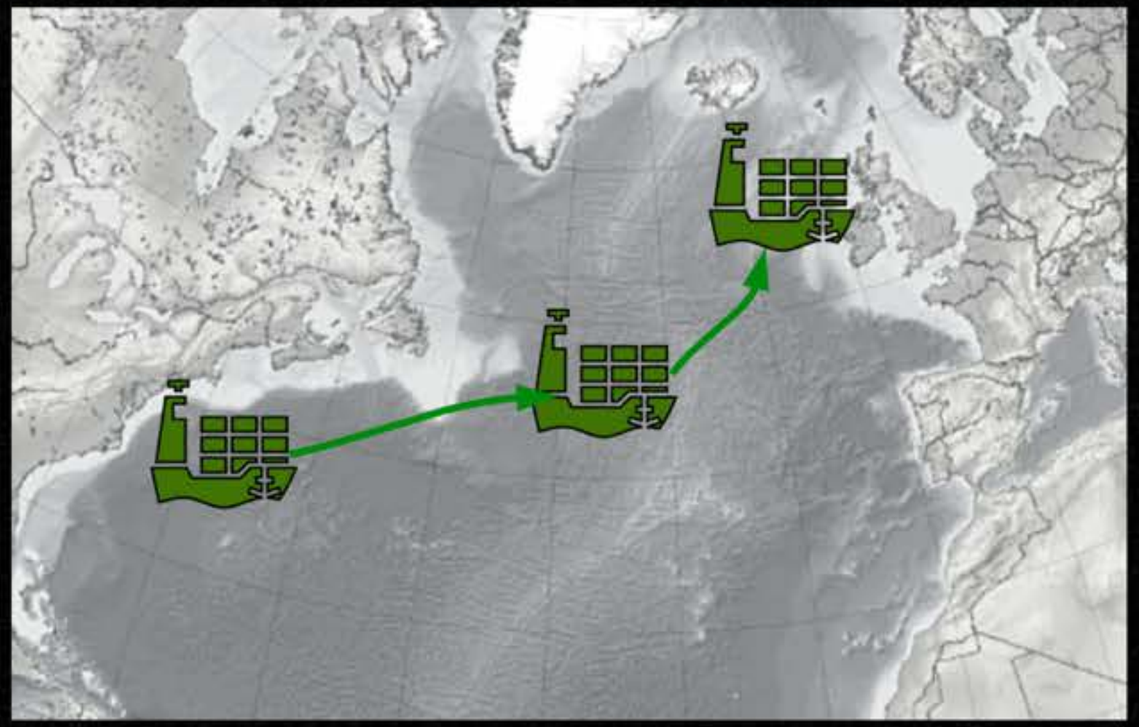
OF TACTICS CHANGED THE COURSE OF SUBMARINE USAGE IN FLEET OPERATIONS FOREVER



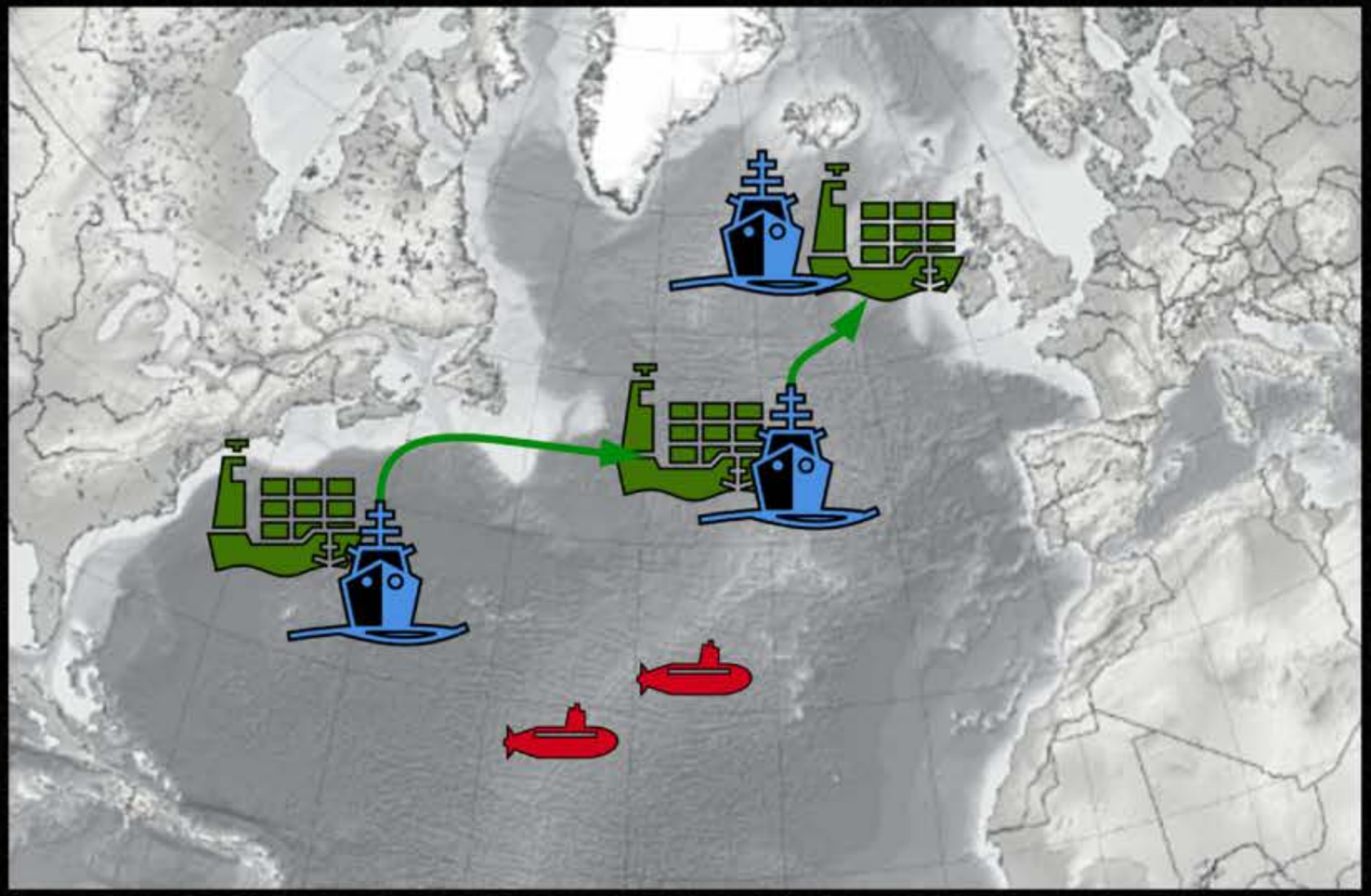
BREAKING THE RULES

to attack an enemy supply line ushered in a new theater of war, permanently changing how cargo and merchant ships transit the ocean

UNRESTRICTED SUBMARINES TURNED SUPPLY ROUTES FROM THIS...



...INTO THIS



RUMORS

of submarines were enough to scare merchants into requesting convoys.

Transiting the Atlantic was never the same.

Even if the submarines weren't active in an area, rumors were enough to divert combat resources to form armed convoys.

SUBMARINES

are Red Teams

whispers

OF A RED TEAM AT A COMPANY ARE ENOUGH TO FOREVER ALTER THE SECURITY POSTURE AT THE COMPANY

precedent

MUST EXIST ALREADY OF THE LETHALITY OF THE RED TEAM FOR THE RUMORS TO HAVE MAXIMUM EFFECTIVENESS

LETHALITY

How can a Red Team establish lethality?

by being submarines...

... and doing what submarines were meant to do

find soft targets

attack soft targets

ONE THING

IF THERE IS ONLY ONE THING
REMEMBERED FROM THIS
PRESENTATION...

RED TEAMS

MUST

DO THIS

this is the nature of a submarine

RED TEAMS

MUST NOT

DO THIS

this is not the nature of a submarine

INTRO

Name: Christopher Cottrell

Title: Senior Manager, Information Security
at NVIDIA

Job: Manager of Hackers and Hunters

icebearfriend

cyberseneca

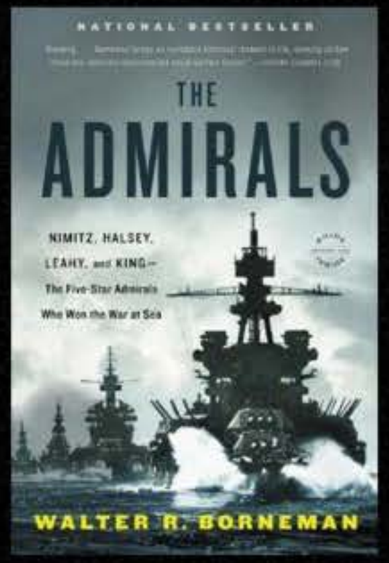
linktr.ee/cyberseneca

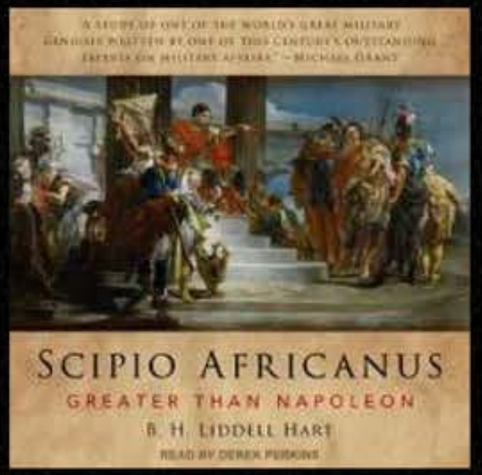
"I am, however, discussing with you troubles which concern us both, and sharing the remedy with you, just as if we were lying ill in the same hospital. **Listen to me, therefore, as you would if I were talking to myself.** I am admitting you to my inmost thoughts, and am having it out with myself, merely making use of you as my pretext."

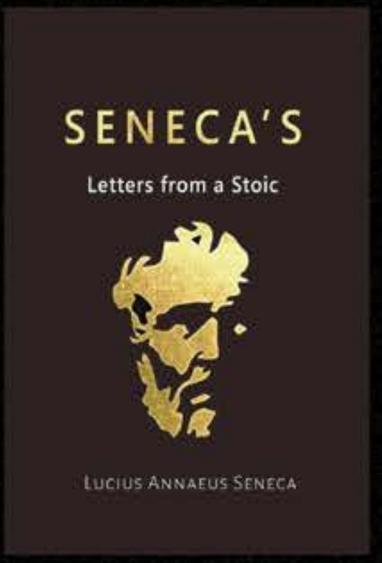
Seneca the Younger, Moral Letters to Lucilius, Letter 27 'On the Good which Abides'

HACKER PHILOSOPHY

Ancient wisdom applied to something I care about: HACKING!







HAPPY EVER AFTER

One year from now, sitting at your desk on a sunny day, your efforts to steer the cyber fleet towards into fair winds have:

- Earned you the respect of your peers
- Grown you into a leader
- Given you poise under stress
- Given you the knowledge of purpose
- Given you a trustworthy career roadmap
- The fleet is being led by those that should lead it

OUR STORY ENDS ON A HAPPY NOTE, BUT FOR NOW...

OUR STORY BEGINS...

EARLY 1900S

NAVIES THE WORLD OVER.

THE PATH TO ADMIRALTY GOES THROUGH THE BATTLESHIP.

AS SUCH, THE BATTLESHIP IS THE CENTER OF THE FLEET.

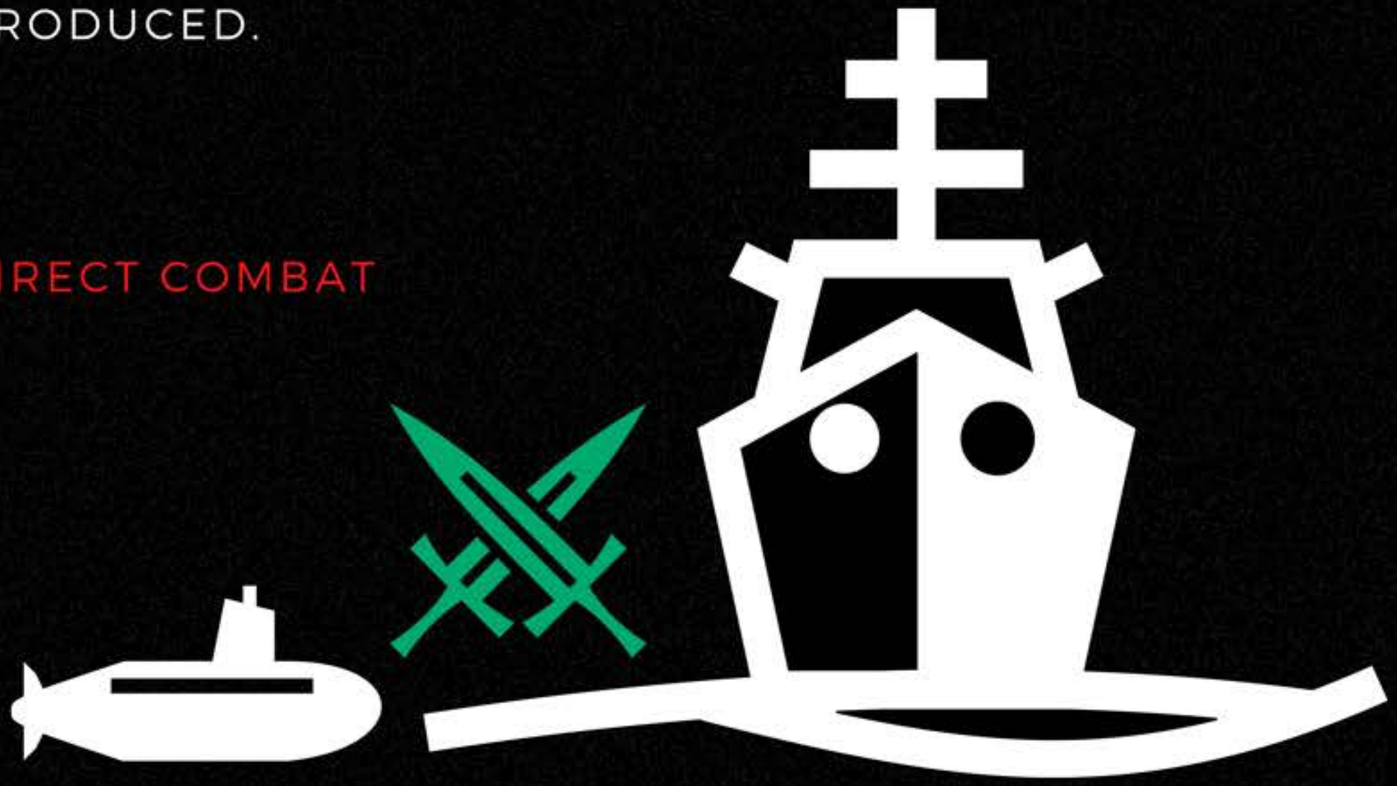
THEN...

EARLY 1900S

A NEW CONCEPT OF SUBMARINES INTRODUCED.

INITIALLY MOCKED.

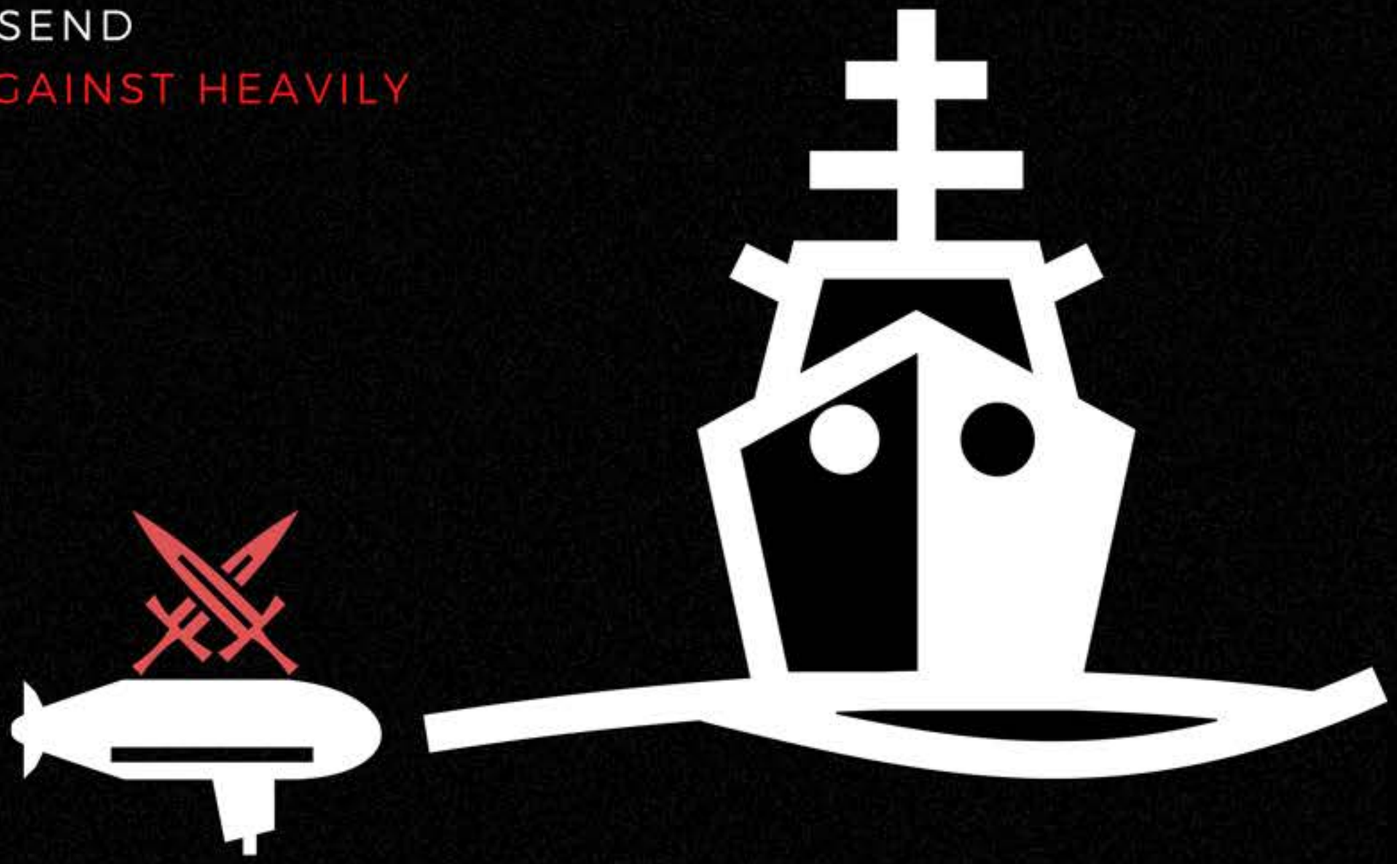
SUBMARINES WERE NO MATCH FOR DIRECT COMBAT AGAINST SURFACE SHIPS.



WHY..

...WOULD ADMIRALS AND TACTICIANS SEND SUBMARINES INTO DIRECT COMBAT AGAINST HEAVILY ARMED SHIPS...

...ON THE *SURFACE*?



WARFARE

Warfare had changed, but those in charge had not considered, explored, or researched new ways of combat.

Battles at sea are fought on the surface.

Submarines told to come to the surface to fight.

Submarines lost many fights.

NOW...

EARLY ~2007-2011

CYBERSECURITY TEAMS START TO FORMALIZE, AND THE PATH TO CISO GOES THROUGH THE SOC.

AS SUCH, THE SOC IS THE CENTER OF THE CYBERSECURITY TEAM.

THIS IS TRUE TO THIS DAY.

RED TEAMS

EARLY ~2007-2011

...FORM AS PENETRATION TESTING STARTS TO TEST MORE THAN APPLICATIONS, SPAWNING A NEW CLASS OF SECURITY ASSET.

RED TEAMS ARE PITTED DIRECTLY AGAINST THE DEFENSIVE CAPABILITIES OF THE CYBERSECURITY TEAM.

HISTORY

repeats itself

For the same reason as before.

promoted to CISO

burned out of profession

WHAT CAUSED THIS?

Fleets being Battleship centric

TIMES CHANGE

and we have a historical example of naval fleet tactics forcefully upended over the course of 40 years...**for the better.**

Security fleets cannot wait 40 years to evolve.

Our tactics must evolve now.

LET'S DIG IN

and discover how to evolve our fleets from Battleship centric...

...into Carrier centric

and our story starts with submarines...

doing what submarines are good at

Meet the Fleet

IT'S TIME TO MEET THE FLEET AND FIGURE OUT WHAT PART WE EACH PLAY AS SECURITY SAILORS

Drawing on the tactics, history, and best practices for each element of a Fleet

Destroyer
SOC (Modern)

Cruiser
SOC (Mature)

Battleship
SOC+IT (Obsolete)

Carrier
Hunt

Submarine
Offsec

Mine Hunter
Risk

Amphibious
IR

SUBMARINES

AND RED TEAMS

Similarities and effective tactics

SUBMARINES

PHILOSOPHY

Most effective when allowed to attack soft targets or supply chain

Even though they are part of the fleet, roaming and hunting to find, engage, and attack supply chain targets can WIN WARS

1945 Imperial Japan was no longer able to conduct war as a direct result of Allied Submarine tactics

RED TEAMS

PHILOSOPHY

SUBMARINES

PHILOSOPHY

Most effective when allowed to attack soft targets or supply chain

Even though they are part of the fleet, roaming and hunting to find, engage, and attack supply chain targets can WIN WARS

1945 Imperial Japan was no longer able to conduct war as a direct result of Allied Submarine tactics

RED TEAMS

PHILOSOPHY

Most effective when allowed to attack soft targets or supply chains targets

When empowered to roam and find targets with a high center of gravity, meaningful and consistent findings result

The sole mission of an offensive security team is the complete nullification of defensive capabilities (controversial statement!)

SUBMARINES

RESOURCES

Must be staffed and utilized appropriately, in accordance with the rest of the Fleet

A single submarine is too valuable to risk. Too valuable to lose. And as a result: unable to fulfill its nature

A flotilla of Submarines without a supporting Fleet puts the flotilla at risk and reduces its combat capabilities

RED TEAMS

RESOURCES

SUBMARINES

RESOURCES

Must be staffed and utilized appropriately, in accordance with the rest of the Fleet

A single submarine is too valuable to risk. Too valuable to lose. And as a result: unable to fulfill its nature

A flotilla of Submarines without a supporting Fleet puts the flotilla at risk and reduces its combat capabilities

RED TEAMS

RESOURCES

Must be staffed in accordance and proportion with the rest of the cybersecurity team

A single operator is overloaded and cannot explore to conduct proper center of gravity analysis on what targets need attacked

A Red Team should only be brought in once core components of the cyber team are in place to support them

SUBMARINES

RED TEAMS

WARFARE

Tasking a Submarine to do anything other than roaming attack missions is a misuse of its unique talents

Historical Example: Submarine Warfare comparison in the Pacific vs Atlantic in WW2

Countries that utilized their Submarines to run supply missions instead of roaming attack let their adversary run supply chains all over the theater

TACTICS

SUBMARINES

WARFARE

Tasking a Submarine to do anything other than roaming attack missions is a misuse of its unique talents

Historical Example: Submarine Warfare comparison in the Pacific vs Atlantic in WW2

Countries that utilized their Submarines to run supply missions instead of roaming attack let their adversary run supply chains all over the theater

RED TEAMS

TACTICS

Tasking a Red Team to do things that deviate from their unique talents is a misuse of the Red Team

Every minute that a Red Team spends not utilizing their unique talents on mission is a minute that the company has duplicated capabilities

Only the Red Team can do what it does

SUBMARINES

PUTTING IT INTO PRACTICE

When I see the team straying off course, deviating into projects that do not utilize their unique talents, I ask:

IS THIS SUBMARINE SH*T?

SUBMARINES

PUTTING IT INTO PRACTICE

If the answer is no:

GO DO SUBMARINE SH*T!

Pictured: The desired end state of a security team

BATTLESHIP

PHILOSOPHY

Big ship, big guns. Must be big important!

Because important, attracts commanders that want to move up the ranks

Fleets meet on the high seas to use their big guns. Fleet tactics revolve around big important ships carrying big important people.

Use big guns to hit land targets (within reach of the coast). Big battles lead to big promotion

SOC+IT

PHILOSOPHY

BATTLESHIP

PHILOSOPHY

Big ship, big guns. Must be big important! Because important, attracts commanders that want to move up the ranks

Fleets meet on the high seas to use their big guns. Fleet tactics revolve around big important ships carrying big important people.

Use big guns to hit land targets (within reach of the coast). Big battles lead to big promotion

SOC+IT

PHILOSOPHY

Big budget, big important. Not always big effect

Effectiveness metrics tied to business. SOC's of yore, which also included IT (or IT including cyber), measured by anything but security effectiveness

Big departments lead to big promotion

BATTLESHIP

SOC+IT

WARFARE

TACTICS

The Fleet centers around its most important ship: the Battleship

Naval warfare centers around big guns.

See: The Battle of Tsushima Strait

Once the Battleship's big guns were no longer effective: time to move these big guns somewhere else where they can blow something up

See: Everything the USS North Carolina did in WW2 Pacific Theaters

BATTLESHIP

WARFARE

The Fleet centers around its most important ship: the Battleship

Naval warfare centers around big guns.
See: The Battle of Tsushima Strait

Once the Battleship's big guns were no longer effective: time to move these big guns somewhere else where they can blow something up

SOC+IT

TACTICS

Where the money goes, so there are the most important people

Security warfare centers around the money: the big budget spends of security tools, the SOC, the hardware

Once an incident occurs: it's time to take this big budget somewhere else that deserves it!

BATTLESHIPS

PUTTING IT INTO PRACTICE

This is class of warship is obsolete

It served its purpose with dignity, but that time is in the past

It will be defeated when engaging a modern adversary

OBSOLETE

DESTROYER

PHILOSOPHY

Fast, mobile, ready to move to the where it needs to be

Can engage adversaries if properly supported

Attracts commanders not seeking glory, but people that want to see a job done right

SOC (SMB)

PHILOSOPHY

DESTROYER

PHILOSOPHY

Fast, mobile, ready to move to the where it needs to be

Can engage adversaries if properly supported

Attracts commanders not seeking glory, but people that want to see a job done right

SOC (SMB)

PHILOSOPHY

Scrappy, focused on what matters most: the adversary out in front (critical findings)

Can burst to IR if properly supported with 3rd party

Attracts problem solvers with engineering mindsets that attack the problem of scaling more with limited resources

DESTROYER

SOC (SMB)

WARFARE

TACTICS

Force projection is limited, does not extend much past the coastline

Engages smaller or lightly armored adversaries

Does well supporting members of the Fleet who can engage advanced or large adversaries

DESTROYER

WARFARE

Force projection is limited, does not extend much past the coastline

Engages smaller or lightly armored adversaries

Does well supporting members of the fleet who can engage advanced or large adversaries

SOC (SMB)

TACTICS

Defensive throughput derived from limited capacity and capability. Difficult to get beyond critical alerts only

Self sufficient when engaging lower tier adversaries

Able to integrate with 3rd parties to combat higher tier adversaries

DESTROYERS

PUTTING IT INTO PRACTICE

Natural entry point for the modern cyber fleet

It is natural for the Destroyer to be the center of the fleet as it grows

Once a class of ship with higher force projection is added, the Destroyer moves into a supporting role

BLOCKADE

CRUISER

SOC (Mature)

PHILOSOPHY & WARFARE

Force projection is moderate, and extends past coastline moderately

Engages adversaries as part of a Fleet that might include one set of advanced capabilities: Minesweeper, Submarine, Amphibious

A moderately sized Fleet supports the Cruiser as it keeps adversaries at range

PHILOSOPHY & TACTICS

CRUISER

PHILOSOPHY & WARFARE

Force projection is moderate, and extends past coastline moderately

Engages adversaries as part of a Fleet that might include one set of advanced capabilities: Minesweeper, Submarine, Amphibious

A moderately sized Fleet supports the Cruiser as it keeps adversaries at range

SOC (Mature)

PHILOSOPHY & TACTICS

Large enough to engage incidents less than Critical

Can engage with more advanced adversaries through the support of advanced capabilities: Risk, Red Team, or IR

As a larger cyber Fleet, has some autonomy to float and engage with targets as it sees fit

CRUISERS

PUTTING IT INTO PRACTICE

Adding specialized and advanced capabilities should support the Cruiser, which is at the center of the Fleet

The Fleet supports the Cruiser, and the Cruiser guides the Fleet

PATROL

AMPHIBIOUS

PHILOSOPHY & WARFARE

Specialized asset to extend force projection of the Fleet to land

Limited to no combat capabilities on the high seas against other ships and Fleets

Capabilities against other ships involves the capturing the vessel, whereas the Fleet is engaged in the destruction of the threat

IR

PHILOSOPHY & TACTICS

AMPHIBIOUS

PHILOSOPHY & WARFARE

Specialized asset to extend force projection of the Fleet to land

Limited to no combat capabilities on the high seas against other ships and Fleets

Capabilities against other ships involves the capturing the vessel, whereas the Fleet is engaged in the destruction of the threat

IR

PHILOSOPHY & TACTICS

Battles adversaries outside of main cyber engagements

Supports the cyber Fleet through capturing and securing adversary resources

Small team, most effective when agile and supported

AMPHIBIOUS

PUTTING IT INTO PRACTICE

An agile team that engages the adversary through their specialized talents

Requires a Fleet, and their mission supports the Fleet currently engaged in battle with an adversary

Mission: Capture and secure adversary resources, denying support to extend engagements

CAPTURE AND SECURE

MINE HUNTER

PHILOSOPHY & WARFARE

Specialized asset to support the Fleet from unseen threats

No combat capabilities on the high seas. No force projection

Guides the Fleet away from lurking danger or tags danger for neutralization from the Fleet when current combat stops

RISK

PHILOSOPHY & TACTICS

MINE HUNTER

PHILOSOPHY & WARFARE

Specialized asset to protect the Fleet from unseen threats

No combat capabilities on the high seas. No force projection

Guides the Fleet away from lurking danger or tags danger for neutralization from the Fleet when current combat stops

RISK

PHILOSOPHY & TACTICS

Supports the cyber Fleet to ensure combat readiness is available for incidents by guiding away from danger

Shields the cyber Fleet from outside interference during incidents

It takes a certain type of person to want to poke bombs. Treat Risk staff with kindness - they are part of the cyber Fleet!

MINE HUNTER

PUTTING IT INTO PRACTICE

Fleets center around the ships that have the largest force projection: Mine Hunters do not have any force projection

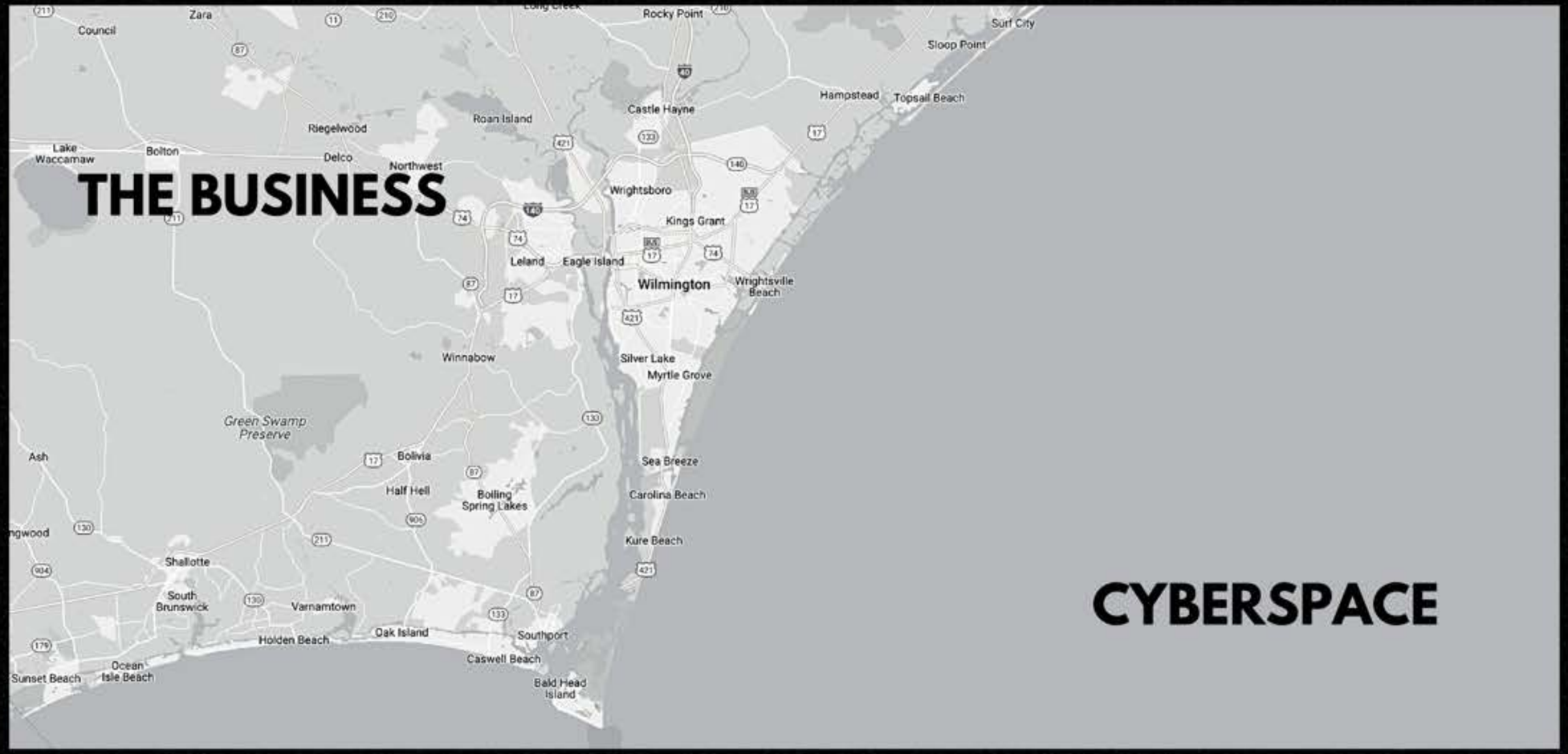
Mine Hunters clear the way from lurking danger, as long as it does not detract from combat readiness (the purpose of the Fleet!)

During incidents, Mine Hunters support the cyber Fleet by screening outside interference

ADVISE AND SHIELD

FORCE PROJECTION

SO FAR



FORCE PROJECTION

SO FAR

FORCE PROJECTION

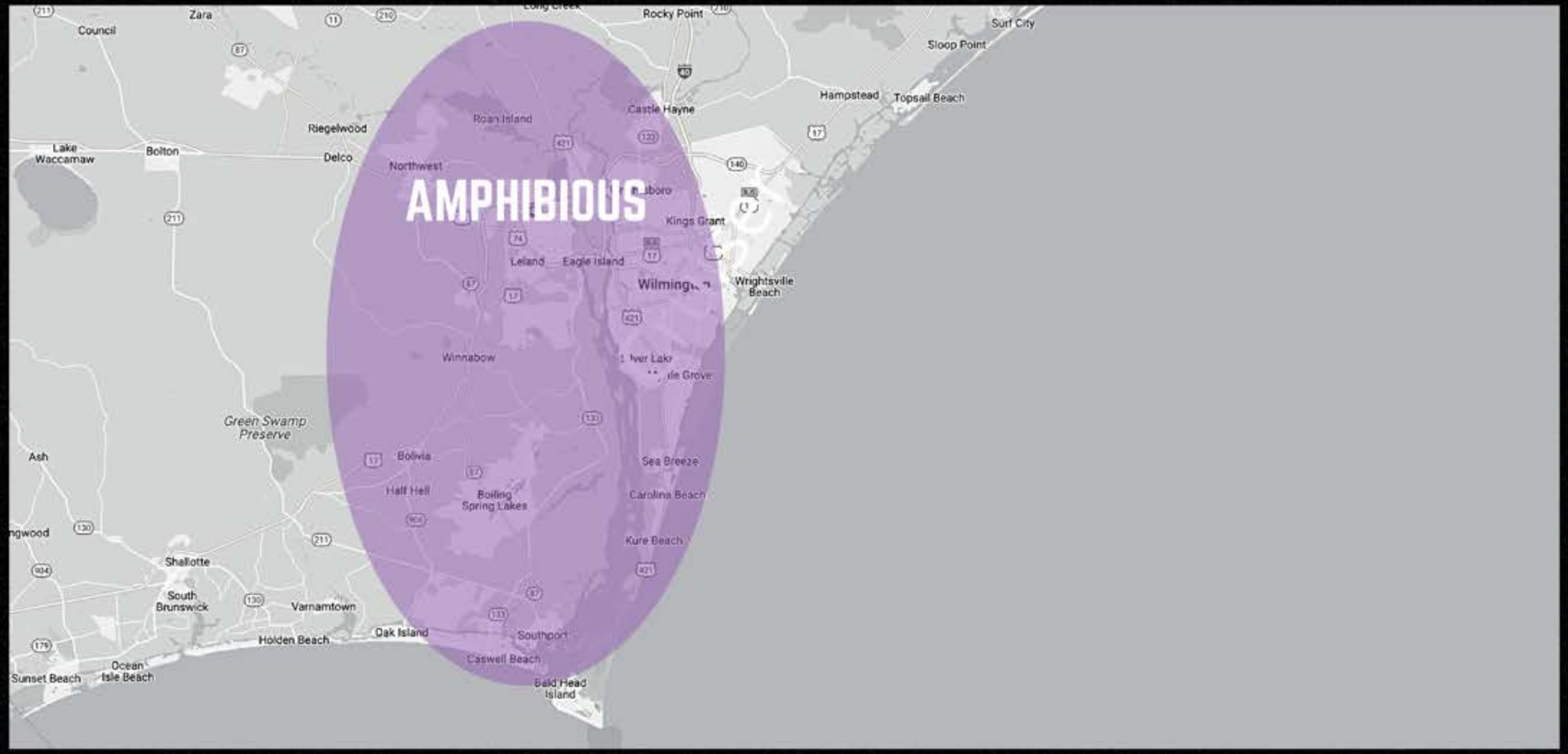
SO FAR

FORCE PROJECTION

SO FAR

FORCE PROJECTION

SO FAR



FORCE PROJECTION

SO FAR

CARRIER

THREAT HUNT

PHILOSOPHY

Pinnacle of force projection

Combat capabilities for land and sea targets the world over

The Fleet centers around the Carrier to support and protect as it readies itself to launch aircraft

Story: Battleships and Carriers in WW2

PHILOSOPHY

CARRIER

PHILOSOPHY

Pinnacle of force projection

Combat capabilities for land and sea targets the world over

The Fleet centers around the Carrier to support and protect as it readies itself to launch aircraft

Story: Battleships and Carriers in WW2

THREAT HUNT

PHILOSOPHY

Pinnacle of cyber projection

Can follow, investigate, and maintain active engagement with adversaries across multiple theaters

Can stay in the fight until the fight is done. Not having to move on when their big guns are done doing big gun things

CARRIER

THREAT HUNT

WARFARE

Turn into or away from the wind to launch or land aircraft

Find and engage adversaries to deny or degrade their combat capabilities until supporting forces can root them out

Control an area through force projection of their presence

TACTICS

CARRIER

THREAT HUNT

WARFARE

Turn into or away from the wind to launch or land aircraft

Find and engage adversaries to deny or degrade their combat capabilities until supporting forces can root them out

Control an area through force projection of their presence

TACTICS

Follow up to deep IR actions or find adversaries based on hunches and intelligence

Autonomy to traverse multiple business units and infrastructure to continually engage a threat until the threat is no more

Control the operational tempo of engaging advanced and embedded adversaries

CARRIER

PUTTING IT INTO PRACTICE

Carriers bring to bear an impressive and unmatched arsenal.

A Carrier without a supporting Fleet is vulnerable and cannot realize its full potential

A Fleet that doesn't center around the Carrier is putting it's most lethal asset at unnecessary risk

ANYTIME.
ANYWHERE.

EVOLUTION

OF THE CYBER FLEET

NOT RECOMMENDED

STARTER
REQUIRED ONLY

ADVANCED
REQUIRED + SUPPORT
OPTIONAL SPECIALIZED

MODERN
REQUIRED + SUPPORT
SPECIALIZED

REQUIRED
CENTER OF FLEET

SUPPORT
SUPPORT THE CENTER

SPECIALIZED
UNIQUE TALENTS

BLOCKADE

IN-HOUSE SOC

TRIAGE SOC

PICK ONE

PATROL

PATROL

HUNTERS

TRIAGE SOC

IN-HOUSE SOC

AT LEAST ONE OF EACH

SOVEREIGN

CAPTAIN'S LOG

SUPPLEMENTAL

New types of warships redefined the "center" of the fleet...

...which redefined the tactics for both strategy of the fleet....

....and the strategy to the path of command

ADMIRALS

NEED COMBAT EXPERIENCE

The Battleship had the best opportunities for large, meaningful combat

But if the Battleship was no longer the center of the Fleet, did it still offer the best opportunity for impactful, meaningful Fleet action experience?

NO

IT DID NOT

Pictured: Future leaders looking for action

CREW SIZE

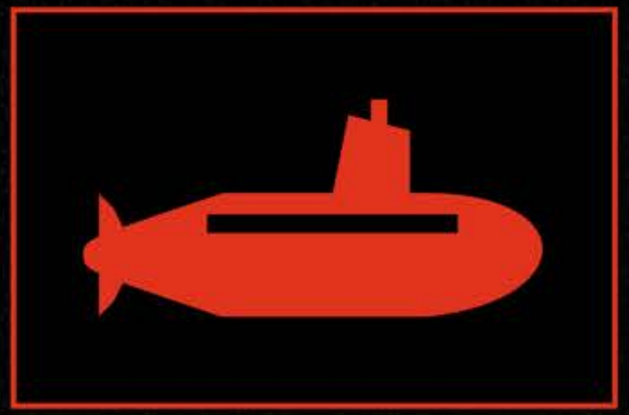
OF A BATTLESHIP VS SUBMARINE

2000+

~100

SUBMARINE SKIPPERS

ARE VALUABLE LEADERS

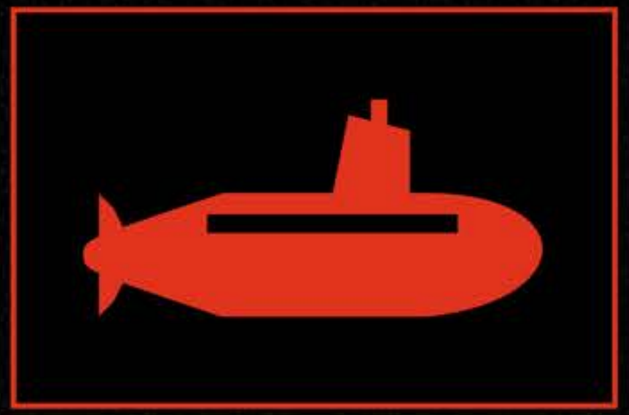


Smaller crew size means that junior leaders can get command of a boat that provides meaningful impact to the Fleet

Providing combat experience leadership at much earlier stages in careers

RED TEAMERS

ARE VALUABLE LEADERS



Smaller team sizes combined with **global business impact** that carries great personal risk to the red team

Red teamers get **strategic, impactful, experience** much earlier in their careers when compared to peers

SO WHERE

ARE ALL THE SUBMARINER ADMIRALS?

Typically, and on average: leading the Navy

IT IS THOSE OFFICERS WHO ARE TODAY GAINING SENIOR RANK IN THE NAVY. "THERE'S JUST TOO MUCH BRAIN POWER IN THAT GROUP TO KEEP THEM DOWN," A NAVAL OFFICER SAID.

NYT ARTICLE 1985, *PENTAGON: THE STEADY RISE OF THE SUBMARINERS*

SO WHERE

ARE ALL THE RED TEAM

CISOs, VPs, and Senior Leaders?

Typically, and on average: still on keyboard

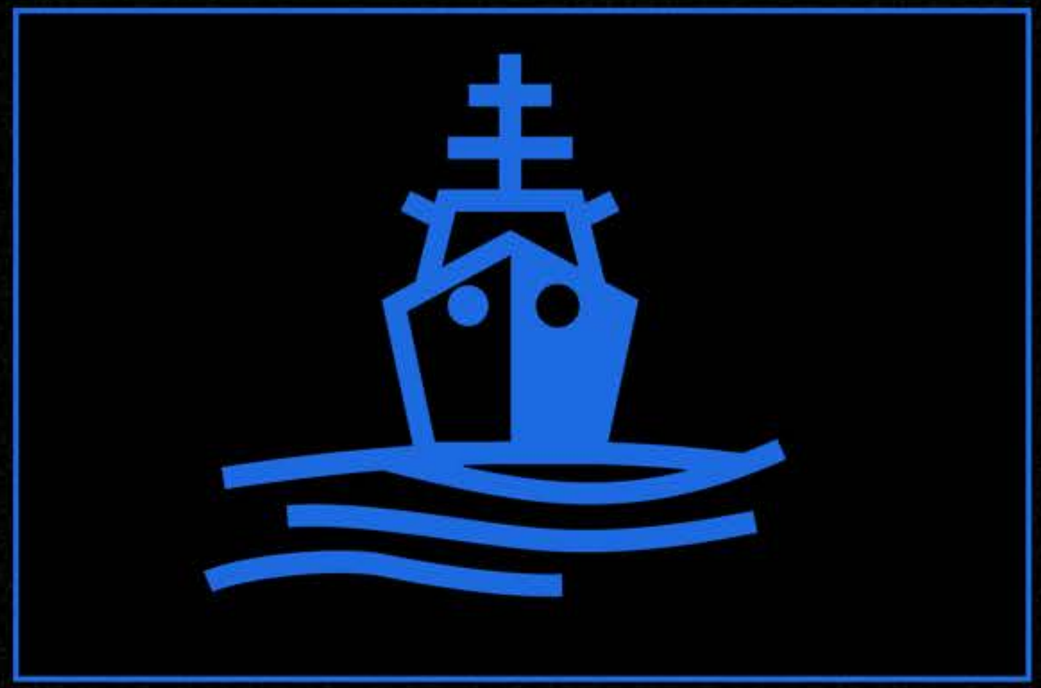
WHY?

I SPECULATE

Nobody has told them how valuable their command and combat experience is at a strategic level

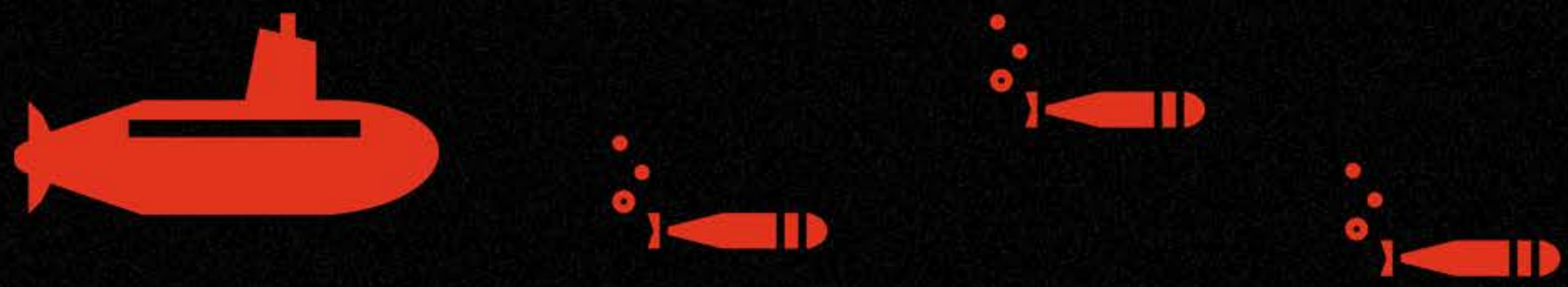
BECAUSE

CYBER FLEETS STILL CENTER ON THE BATTLESHIP



IT'S TIME FOR RULE BREAKERS

TO START BREAKING SOME RULES



IT'S TIME FOR SUBMARINES

TO DO SUBMARINE SH*T

AS PART OF A FLEET

BATTLESHIPS:
THANK YOU FOR YOUR SERVICE

You paved the way for

Fleets to evolve

You held the line and

protected us

You did what you did best

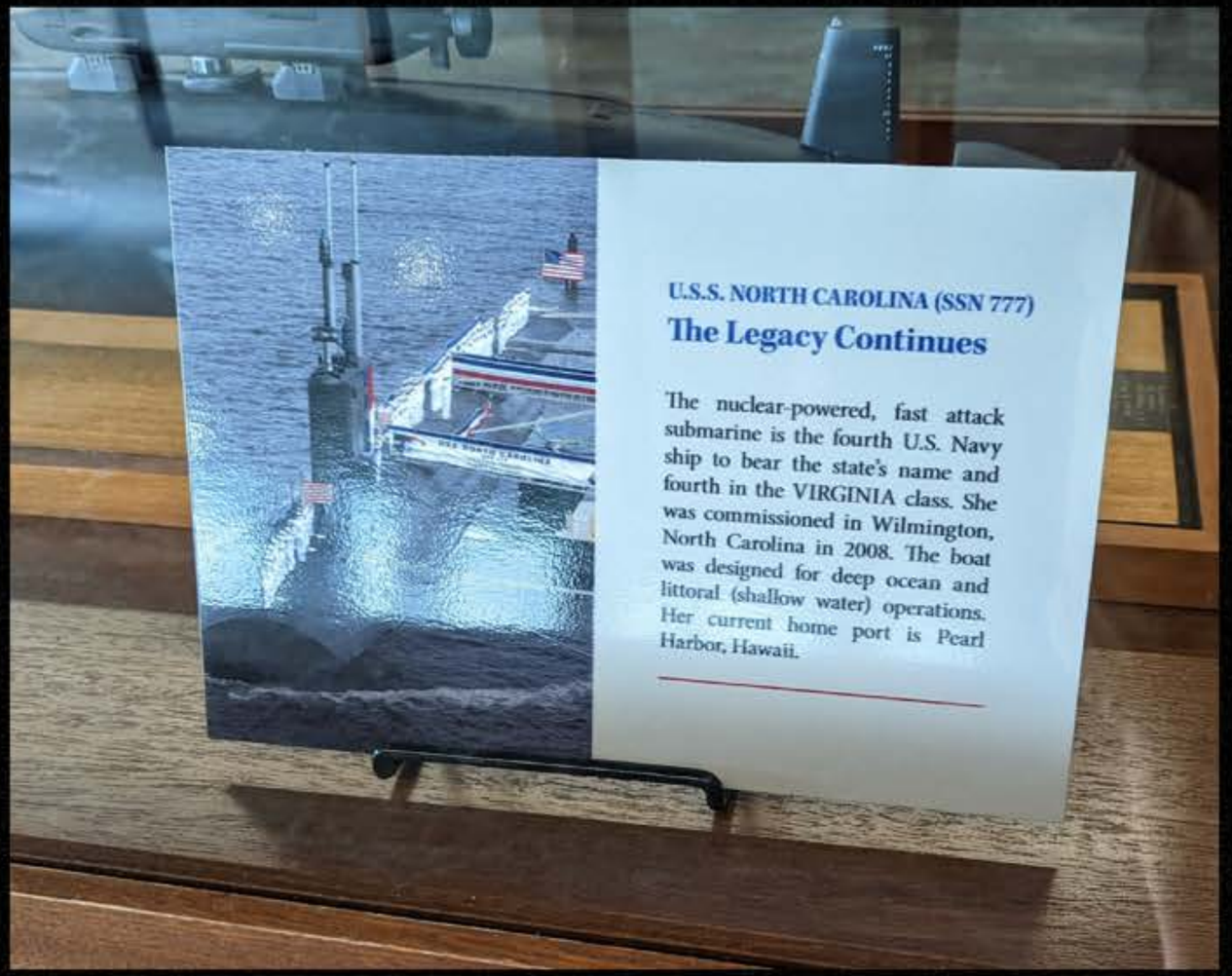
when it was your time to do

it

Pictured: Me, a noob, touring the USS North Carolina, WW2 Battleship nicknamed "The Showboat"

BUT YOUR TIME

IS OVER



Pictured: The next vessel to bear the name

USS North Carolina was a Submarine

FAREWELL HACKERS

FAIR WINDS AND
FOLLOWING SEAS