To: National Security Council
From: FSociety [Matthew Brophy, Jackie Faselt, Katy Mayerson, Andrew Seligson]
Re: Decision Document

EXECUTIVE SUMMARY

We are monitoring cyber attacks which affect U.S. maritime critical infrastructure and global trade. The NSC should initiate the **Cyber Unified Coordination Group** to remediate the following threats:

1. Ransomware
2. Data Manipulation
3. Ongoing Conspiracy (Manticore and 1881 Colectiv)

We have developed an escalatory framework centered around three primary lines of effort: **RESPOND**, **REINFORCE,** and **RETALIATE**. This plan uses a whole-of-government approach to remediate immediate threats and impose new costs to our adversaries. We recommend Option 2.

POLICY OPTIONS

OPTION	*Lines of Effort*		
	RESPOND	**REINFORCE**	**RETALIATE**
1	**Port Cyber Remediation Task Force** *CISA; US-CERT; USCG; DOS*	**Maritime Public-Private Partnership** *MTS-ISAC; CISA*	**International Legal Action** *DOJ; DOS; FBI*
2		**Offensive Security** *FBI*	**The Financial Wedge** *SEC; DT-OFAC; USCYBERCOM*
3			**Strike** *USCYBERCOM*

RECOMMENDATIONS AND JUSTIFICATION

Option 1 imposes insufficient costs to our adversaries to deter a third attack.
Option 3 risks escalating tensions with Iran and could be utilized in event of imminent attack.

We recommend Option 2. This option effectively responds and reinforces, while using a measured retaliation effort to isolate Manticore and cut off proxy support.

U.S. Agency Stakeholders

CISA (Cybersecurity and Infrastructure Security Agency) | **US-CERT** (Computer Emergency Readiness Team) | **USCG** (Coast Guard) | **DOJ** (Department of Justice) | **DOS** (Department of State) | **DT-OFAC** (Department of Treasury Office of Foreign Assets Control) | **FBI** (Federal Bureau of Investigation) | **MTS-ISAC** (Maritime Transportation System Information Sharing and Analysis Center) | **SEC** (Securities and Exchange Commission) | **USCYBERCOM** (Cyber Command)