To: National Security Council
From: FSociety [Matthew Brophy, Jackie Faselt, Katy Mayerson, Andrew Seligson]
Re: Cyber Threat Assessment and Policy Option

EXECUTIVE SUMMARY

Through our detailed analysis we have identified three cyber threats originating from two threat actors, the Iranian politically motivated Manticore APT group (Manticore) and the financially motivated Romanian 1881 Colectiv (1881):

1. **Ransomware**
2. **Data Manipulation**
3. **Ongoing Conspiracy**

These threats have hindered the operational continuity of international trade and compromised trade supply chain integrity, thereby negatively impacting U.S. national security. Below, we outline these threats and their associated risks and propose an escalatory framework to respond to the crisis, reinforce U.S. critical infrastructure, and retaliate by imposing costs upon these cyber adversaries.

U.S. Coordinating Agencies: CISA (Cybersecurity and Infrastructure Security Agency) | **DOJ** (Department of Justice) | **DOS** (Department of State) | **DT-OFAC** (Department of the 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) | **US-CERT** (Computer Emergency Readiness Team) | **USCYBERCOM** (Cyber Command)

THREAT AND RISK ASSESSMENT

Threat 1: Ransomware — *Near Term* | High Impact

1881 has launched ransomware attacks on at least seven ports worldwide, including the key U.S. ports of Houston and Corpus Christi. Once deployed, the Baskerville ransomware compromises cargo manifest systems and digital backups, crippling operational continuity. 1881 further targeted email services and access management software, posing threats to digital and physical security at affected ports. Additionally, 1881 has monetized this operation by shorting stocks on affected companies.

- ***Maritime Trade Disruption:*** Port systems affected by Baskerville cannot unload cargo, causing disruptions to global maritime trade networks. For example, delays at the Nigerian Port of Harcourt have impacted oil refineries and USAID food imports, which could precipitate a regional energy crisis and acute food insecurity for millions.
- ***Market Manipulation:*** 1881's monetization efforts disincentivize cessation of attacks or provision of decryption keys. These suspicious trading patterns may undermine shipping and petroleum markets. 1881 may use this windfall to fund additional cybercrime operations.

Threat 2: Data Manipulation — *Medium Term* | Medium Impact

Manticore has taken advantage of a vulnerability in TidalWaves, a popular cargo manifest software. This vulnerability allows these actors to manipulate cargo manifest data, which may compromise supply chain integrity. Reports show that a wide range of cargo has not reached its intended destination.

- ***Sanctions Evasion****:* Iran could use the TidalWaves exploit to evade U.S. economic sanctions and arms embargoes. In the worst case, Manticore may manipulate cargo manifest data to obfuscate transportation of weapons. Suspicion of cargo theft may escalate tensions with Iran.

Threat 3: Ongoing Conspiracy — *Medium – Long Term* | High Impact

We assess that Manticore and 1881 collaborated to conduct ransomware and data manipulation attacks and are conspiring to execute a third attack. If successful, this attack will escalate pressure on critical infrastructure. This threat supports Manticore's political motivations and 1881's financial motivations.

- ***Unquantifiable Damage:*** Considerable economic and operational damage may result from escalating existing attacks on affected ports.
- ***Future Collaboration:*** The success of Manticore's use of 1881 as a proxy for this series of attacks may cement future Iranian collaboration with 1881 and additional cybercrime groups.

POLICY RECOMMENDATIONS

We recommend the **Respond, Reinforce, Retaliate** framework to address the nation's current cyber threats. This plan uses a whole-of-government approach to remediate immediate threats while imposing new costs upon our adversaries. The Reinforce and Retaliate plans include additional escalatory measures should the NSC pursue a higher risk strategy. The NSC should initiate the Cyber Unified Coordination Group (**CUCG)** to lead and coordinate the escalatory framework.

RESPOND

The Respond effort utilizes a Port Cyber Remediation Task Force coordinated by **CISA** to address immediate impacts. This task force will deploy **US-CERT** to Texas to lead technical remediation. **USCG** will secure access management in ports and **CUCG** will release a joint statement discouraging the use of TidalWaves until patching. Additionally, **DOS** will assess and mitigate effects to global trade, sharing best practices with affected allies. Finally, **CISA** will investigate the ransomware, analyze manifest logs, and facilitate communication to the public providing reassurance regarding ongoing remediation efforts.

Advantage	***Disadvantage***
Remediates the immediate impact of ransomware on the affected ports	Potential coordination challenges amongst various stakeholders

REINFORCE

The Reinforce effort aims to protect additional U.S. port infrastructure. **CISA** will issue warning to all U.S. critical infrastructure operators about a potential second strike. **MTS-ISAC** will coordinate information-sharing among identified critical maritime infrastructure.

Advantage	***Disadvantage***
Hardens against second attack, bolsters Indications and Warnings (I&W) capability	Increases threat posture sensitivities across U.S. intel surrounding potential attack

In a more escalatory response, we recommend that the **FBI** make use of offensive security measures by planting honeypots in areas of interest for threat actors. These measures enable collection of adversary TTPs and enable distribution of IoCs.

Advantage	***Disadvantage***
Distribution of IoCs helps port operators quickly respond to incidents	Honeypots may not deliver all information; creates vulnerability of relying on limited intelligence

RETALIATE

The Retaliate effort aims to impose financial and legal costs on our cyber adversaries. The **DOJ** will indict the arrested 1881 suspect, while the **DOS/FBI** will engage in bilateral interrogations of the Romanian suspect in Interpol custody. Simultaneously, the **SEC** will hold options trading on affected U.S. ports to interrupt 1881's monetization efforts.

Advantage	***Disadvantage***
Intelligence gathering informs future decisions	Slow moving international legal process may prove ineffective

A further escalatory response will seek to interrupt all financial ties between Manticore and 1881, thereby cutting off all funds to 1881. **DT-OFAC** will investigate and sanction any Iranian individuals supporting 1881, while **USCYBERCOM** will explore technical measures to disrupt Manticore's cryptocurrency wallets.

Advantage	***Disadvantage***
Drives financial wedge between threat actors	Assumes Romanian cybercriminals are solely financially motivated

In the final escalatory response, **USCYBERCOM** would take immediate action to strike the command and control infrastructure of the Iranian and Romanian threat actors.

Advantage	***Disadvantage***
Temporarily halts all operations from these actors	Risks escalation, particularly given Iran's revenge-based motivation