MEMORANDUM FOR: The National Security Advisor
FROM: #CtrlAltElite
SUBJECT: Response to Global Port Ransomware Attack

Situation Summary:

As of March 19, 2021, seven port facilities have been affected by a BASKERVILLE ransomware attack, bringing cargo unloading at these ports to a standstill. Attackers appear to have gained access through the TidalWaves Port Management System whose software is used globally by port facilities. Actors have been in these systems since at least May 17, 2020. Initial intelligence indicates that Manticore *(Iranian-sponsored APT*) hired 1881 Colectiv (*Romanian cyber-criminal group*) to manipulate port data and cover it up with ransomware.

Situation Severity:

The cyberattack on these port facilities threatens global economic stability as well as U.S. national security priorities. Ports facilitate over 90% of global trade yet current cybersecurity protections are insufficient for their role in critical infrastructure. The victim ports are key to international maritime trade: the ports of Corpus Christi, Houston, and Marseille are among the top 60 world ports by cargo volume. The Port of Houston alone supported $801.9 billion of total U.S. economic value through its public and private marine terminals in 2018.

- *Unknown Scale*: At this time the number of ports affected is unknown. Irregularities in tracking data at the Port of Houston noted on March 8, 2021 indicate that the ransomware may be intended to cover-up manipulation of data shipping and cargo ports around the world.
- *Global Economic Disruption*: The world already grapples with economic uncertainty and a global recession caused by the COVID-19 pandemic. The pandemic is fragmenting global trade and supply linkages. Further disruption to the commercial supply chain could be disastrous.
- *Acute Impacts*: It is reported that millions in food aid from the USAID Food for Peace program are affected by the attack on the Port of Harcourt, which is likely to intensify food insecurity for millions of Nigerians in an already unstable region of the world. The cyberattack further complicates external activity related to Nigerian terrorist group, Boko Haram.

Because this incident poses demonstrable harm to critical infrastructure, national security, and economic security, a Cyber UCG will be formed by NSC Principals under PPD-41 to coordinate federal operations and inform national policies.

Key Policy Objectives:

- ➢ Ensure continuity of global port commerce
- ➢ Identify and disrupt threat actors behind malware
- ➢ Strengthen critical infrastructure resiliency and supply chain security
- ➢ Establish international norms in cyberspace

Policy Recommendations

- **Direct local and international FBI branches to send Cyber Task Force teams to nearby ports.** When available, release the *Malware Initial Finding Report* to relevant stakeholders.
- **FBI OPS reach out to TidalWaves to identify and notify breached customers** while urging ports to initiate Disaster Recovery plans
  Risk: Dependent on ports having and initiating resilient Disaster Recovery plans.
- **Centralize all communication** regarding the incident to come from NSC press office
  Risk: May overwhelm NSC press office.
- **Commence dialogue with international partners:** call an emergency session of the UN Security Council and International Maritime Organization.
  Risk: There may be bureaucratic challenges amongst nations
- **Increase security presence at ports near conflict areas,** especially Port of Harcourt.
  Risk: Security personnel may be attacked, leading to injuries or casualties.
- **Enact USAID Emergency Food Security Program** to alleviate acute food insecurity concerns in West Africa.

- **Task intelligence community with investigating the relationship between 1881 Colectiv and Manticore** while also finding missing cargo.
- **DOJ opens case against 1881 Colectiv members and Manticore.** Arrest known 1881 Colectiv members in international law enforcement operations.
  Risk: Limited ability to successfully prosecute Iranians; Premature arrests may constrain legal case against 1881 Colectiv
- **CISA Representative interviews with major news networks** to combat misinformation and answer questions.
  *Risk***:** Critics of the Biden Administration may dismiss the interview.
- **Engage private-sector security firms** to assist in technical investigation and forensic analysis of port breaches

- **Update international trade cybersecurity frameworks**. Amend UN International Maritime Organization's (IMO) *Safety of Life at Sea* and the *Standards of Training, Certification and Watchkeeping* Framework to include cybersecurity training; introduce the *Baskerville Resolution* where members offer trade incentives for compliance with ISM MSC.428(98).
- **Develop international law enforcement cyber capacity** by providing technical training and equipment through DOJ OPDAT.
- **Enhance supply chain security** with an Executive Order mandating stricter regulations for government agencies and critical infrastructure; fund the development of machine learning technologies that can proactively detect supply chain cyber breaches.
- **Prioritize establishing National Cyber Director** per the 2021 NDAA
  *Risk***:** Gridlock in Congress may challenge appointments.

Potential Future Actions: *Dependent on attribution of a responsible actor.*

- Multilateral sanctions
- Reciprocal offensive cyber operation