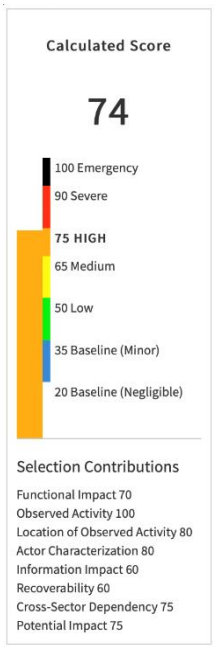
CYBER KNIGHT RIDERS

SIPA **HANDOUT – DAY 2**

TO: National Security Council | **FROM**: Cyber Knight Riders, SIPA / Columbia University

SUBJECT: National Security & Economic Threats from ransomware attacks against Ports



EXECUTIVE SUMMARY: The spread of ransomware to US and international ports amounts to a HIGH National Cyber Incident, affecting international trade and posing national security threats to the US. We propose the NSC (1) corroborates intelligence and establishes crisis coordination via a temporary interagency working group, (2) ensures national (cyber) security via technical and physical security measures, (3) mitigates economic and financial threats, (4) maintains US geopolitical influence, (5) establishes effective crisis communication.

1. Corroborate Intelligence and Establish Crisis Coordination

Baseline	1-1	**Temporary interagency working group "PORTSIDE"** (NCCIC, FBI CyWatch, Coast Guard National Response Center, ODNI, COTP, port operators, MTS-ISAC): (1) International maritime crisis response unit; (2) Information sharing private sector, port/shipment operators, cybersecurity companies
	1-2	ODNI as lead coordinator of intelligence activities: consult with US IC, Five Eyes and partners
	1-3	DOJ/FBI to: (1) investigate ransomware; (2) FBI information collection from Romanian arrests
Moderate	1-4	Convene NSC Deputies Committee to ensure all interagency processes can be facilitated
Strong	1-5	Convene NSC Principals Committee to ensure presidential level authorization of necessary actions

2. Ensure National (Cyber) Security

B	2-1	CISA/US-CERT coordination with affected port & shipping operators and TW
	2-2	PORTSIDE to ensure physical and cyber security of ports and their systems
	2-3	DOD/DHS to: (1) search for missing military goods (2) assess military supply shipments & embarkation plans
M	2-4	Naval Cooperation and Guidance for Shipping assistance in monitoring and communicating with merchant ships
	2-5	DHS and MTS-ISACs to request shipping companies restrict access to critical port software
	2-6	FEMA Port Security Grant Program for emergency funds to prevent port physical attacks
S	2-7	USC Title 10 Federal mobilization of National Guard for increased physical security at ports

3. Mitigate Economic and Financial Threats

B	3-1	US coast guard, port authorities, shipping companies to prioritize shipments of high national interest
	3-2	US coast guard and CISA/US-CERT to (1) track ships from affected ports; (2) isolate ships potentially infected by malware; (3) remove malware from affected ships in order of national priority
	3-3	DOT/DOE/TSA measures to secure US oil and energy supply; coordination with allies for port access
M	3-4	FRB/U.S. Department of the Treasury monetary and fiscal policy options for potential supply shocks; Office of the Comptroller of the Currency (OCC) to ensure price and financial stability
S	3-5	USCYBERCOM PE/DF operation to disrupt cybercrime groups' capabilities and prevent escalation

4. Maintain US Geopolitical Influence

B	4-1	Advise DOS to ensure USG support of Nigerian government
	4-2	Identify potential supply re-routes (sea, land or air) for delivery of USAID food and supplies
	4-3	Advise DOS to (1) address Romania, EU and NATO for cooperation on investigation and disruption of cybercrime groups and (2) to assess/reinforcement backchannels to Iran for potential future use
M	4-4	Encourage US private cybersecurity companies to additionally support Nigerian cyber defense
	4-5	Advise DOS to request UN DPPA & SG good offices/mediation to reduce tensions in Nigeria & Ghana
	4-6	US social media companies: assess takedown of information operations of Ghana's involvement in Nigerian attacks
S	4-7	Pressure US-based social media companies to suppress information operation against link to Ghana
	4-8	Advise DHS/CISA to support and consult Nigerian cyber defense units with personnel and resources

5. Establish Crisis Communication

B	5-1	Issue a public statement outlining the ongoing situation and government measures being taken
M	5-2	Issue public updates on a periodic basis to update the public on continued US response and mitigation
S	5-3	President Biden to address the nation and international community, emphasizing strong response

>>> Proposed Recommendations in BLUE <<<