Summary and Synopsis:

Significant Cyber Incident halting global port operations creates profound economic implications; Expanding attacks including malware-infected ships are being investigated; Threat actors are Romanian cybercriminals (*moderate confidence*) hired by Iranian APT (*low confidence*).

	Policy Recommendations			
	Contain Malware	Attribute Actors	Act Multilaterally	Communicate Effectively
Highly Recommended *Benefits Outweigh Costs*	**Immediate:** Scan all port and ship systems for malware **Immediate:** CYBERCOM hunt for Baskerville malware in defense networks **Immediate**: FBI led task force investigate port and ship system breach severity (local FBI CTFs, CISA, CBP, ICE, US-CERT, M-CERT, USCG) **Near-Term:** Engage private-sector security firms to assist in technical investigation and forensic analysis of port breaches	**Immediate:** Task intelligence community with continued investigation of the relationship between 1881 Colectiv and Manticore **Immediate:** Request FBI presence at Europol interviews of 1881 Colectiv operatives **Immediate:** Task DIA to investigate missing military equipment with defense contractors ***Cost: Use of intelligence resources***	**Immediate:** Encourage diplomatic dialogues at UN IMO regarding economic impacts **Long term:** Propose "Baskerville" Resolution at UN IMO SSE **Near-Term:** Direct embassies to offer U.S. assistance to impacted nations' port malware response through our ALAT expertise and Secret Service CFTFs. **Cost:** ***Investigative resources*** **Near-Term:** CIA / NGA coordinate with FVEY in shipping surveillance operations	**Near-Term:** Leverage DoS in investigating the disinformation post regarding the state of Ghana while advising the Ghanaian mission in Nigeria of potential security concerns **Near-Term:** Disseminate technical findings (M-ISAC, MTS-ISAC, MPS-ISAO, VirusTotal) **Near-Term:** Create a Panel of U.S. government officials from impacted sectors to hold a press conference on the attack's implications **Long Term:** Engage the Nigerian government in operational dialogues to support their recovery ***Cost: Diplomatic relations***
Recommended With Caution *Benefits = costs*	**Immediate:** FBI led task force urges ports to initiate Disaster Recovery plans ***Cost: Investigative resources*** **Near-Term:** Activate Army National Guard cyber units to assist in active defense of port networks ***Cost: Monetary and media attention***	**Long-Term:** CYBERCOM / NSA propaganda campaign against actor(s)' leadership ***Cost: May escalate geopolitical issues***	**Immediate:** USAID OFDA dispatch DART to Nigeria ***Cost: Monetary*** **Immediate:** Advise international allies to increase their own port security if near conflict areas ***Cost: State may have limited resources***	**Near-Term:** Department of State issue security advisory for Nigeria **Cost:** ***May escalate geopolitical issues*** **Near-Term:** U.S. Ambassador to Nigeria privately encourage government of Nigeria to address domestic misattribution to Ghana ***Cost: Controversy***
Recommend With Significant Concerns *Costs potentially outweigh benefits*	**Immediate:** Enact FEMA Emergency Grants ***Cost: Monetary*** **Long Term:** Securing the ecosystem ***Cost: Monetary***	**Near-Term:** CYBERCOM / NSA threat hunt forward into Iranian networks ***Cost: Intelligence Gain/Loss*** **Long-Term:** CYBERCOM / NSA operation against actor(s)' critical infrastructure. ***Cost: May escalate geopolitical issues***	**Near Term:** Defend forward with NATO's RRT ***Cost: May escalate geopolitical issues*** **Long Term:** Sanctions towards actors(s) involved for their involvement with the ransomware attacks ***Cost: May escalate geopolitical issues***	**Near-Term:** Conduct a joint press conference between the leaders of Nigeria and Ghana at the African Union Headquarters ***Cost: Tense relations***

Future Policy Recommendations:

Continue to evaluate the economic turmoil created by Baskerville and the state actors involved. In addition, establishing the National Cyber Director, fund research of technological solutions, and exploring sanctions against the responsible actor.

#CtrlAltElite: Evan Gertler. Arsene Frederic Jr., Elizabeth Marge, Christopher Rodriguez-Molina