APPENDIX C: FOUR SCENARIOS

Future A - Band of Brothers

THE SETTING

The year is 2025. The "connectedness" among nations, individuals and information is an ecosystem that integrates across networked societies and communities. The ubiquity of available information and knowledge transcends sovereign boundaries, and the knowledge diffusion provides potential to lift up Third World Nations into the Information Age. Major power competition, however, drives a new version of the Cold War with information and cyber security as the coin of the realm to be competed within non-aligned nations.

2025 KEY DRIVERS:

- High cooperation among Governments
- High cooperation between Governments and the Private Sector / Industry
- High level of Nation-State competition
- High level of Non-State threats

Nations are lifted by broad access to current information and stimulation of global exchange (trade, culture, policies, technology, communications, etc.). Mid-tier nations see progress at normalizing and formalizing global cyber activity and institutionalizing standards of conduct within the cyber expanse. However, there is tremendous friction between Russia and her neighbors with cyber probes into the Ukraine and even NATO nations. China's rise in Asia continues to result in unease with her neighbors. In response to these events and a nuclear Middle East (Iran and Israel), many nations have turned to developing cyber weapons that can hold nations at risk as a hedge against nuclear weaponry.

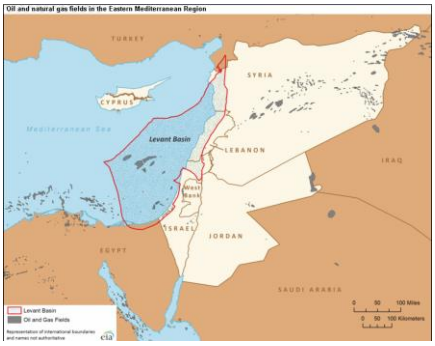
In 2019 provocations by a resurgent Iran against Saudi Arabia and Israel resulted in an anonymous, devastating cyber retaliation. Portions of the Iranian energy grid collapsed; additional damage was reported to key Iranian critical infrastructure and to economic targets linked to the Iranian Republican Guard. The subsequent "Cyber Revolt of 2020" caused governments to work diligently to improve cyber cooperation. With U.N. Security Council Resolution 3326 and the broad acceptance of the Tallinn Treaty, many governments and private industry entered into a new period of partnership and cooperation. However, governments and private industry are also in a highly competitive environment for the scare resources required to fuel the high-tech industries that have become the lifeblood of competitive advantage. Some Third World Nations negotiate compensation from and partnership with advanced nations to develop their resources in exchange for advancing their technology.

With robust global communications, many of the highest technology innovators are moving to remote areas of the Africa, South America and Asia that have relatively low government oversight and regulations. This has enabled ultrahigh-tech Transnational Organizations to wield power and influence much more freely and decisively than recognized Nation-States, including powerful transnational criminal cartels. Major powers seek to find the creases in U. S. authorities by fielding commercial fleets that also

serve government interests and missions. The Coast Guard is challenged to know the global "order of battle" and the intentions of vessels wherever they are encountered. Due to the environment of high cooperation among Western allies, more individual nations and regional cooperatives are requesting USCG expertise in building out their maritime safety, resource, and revenue organizations. Although political competitors with deep mistrust of the US, countries such as Russia, China, and even North Korea, welcome the USCG as a special interlocutor particularly on topics such as maritime safety, law and regulatory enforcement, port and harbor security, and environmental protection. While the presence of U.S. Navy ships may be viewed as hostile, the U.S. government encourages such USCG outreach activities while also tasking the USCG with more port and harbor security and engagement missions in areas of friction such as the Far East. The USCG has a delicate balancing act and significantly more tasking to parse foreign and domestic actors' attempts to avoid direct conflict and evade law enforcement and oversight.

BACKGROUND

The period leading up to 2025 could be characterized as tumultuous. Unable to address the pervasive and regular breaches of national and private systems, global constituents and consumers staged flash riots, "cyber blockades" and globally participated political actions that forced government leaders and private industries to band together. In Iran, several cyber attacks impacted the national electrical grid, which caused the deaths of 264 people. The watershed event was the 2020 "Cyber Revolt", which 2.1 billion users across 185 nations leveraged a point-and-click website to effectively shut down the global economy for 8 days – no communications, no Internet, no financial transactions, no government activity, private industry internal and cloud networks were terminated, and automated industries were widely disrupted (oil & gas, manufacturing, transportation, etc.). After two years, governments and private industry agreed on common security technologies, policies and processes that formed the foundation of the Tallinn Treaty. In 2022, suspected Russian paramilitary commandos using cyber mercenaries quickly subdued the Hatay Province in Turkey and established a base in Antakya, formerly Antioch. This quickly led to Russian Geological companies establishing rights to the Leviathan Gas Field, which is located in the Eastern Mediterranean. Previously inaccessible due to the depth of water, new robotic and deep-sea systems have enabled companies to make this source of energy attainable. Most assessments of the Leviathan Gas Field put the total volume at roughly 27 times the size of all the oil fields in the Middle East and will fundamentally alter the political, security and financial landscape of the Eastern Mediterranean while demoting the position of Middle Eastern energy producers and financiers. Turkey, Syria, Cyprus, Jordan, Israel, Egypt, and now Russia are in a contentious battle for resource rights and "first to drill". In 2023, UN Security Council passed resolution 3326, that made a "quasi-military-backed cyber



offensive action" to be an international crime and authorizes UN signatories the full weight and measure of their resources to combat this designated hostile action.

Additionally, the Arctic has large passages and is open for navigation for an average of 157 days a year. The U.S., Canada, Russia, Norway, China, and Japan are all rushing to establish ports to take advantage of this key trade route. By 2050, most experts agree that Arctic passages may be available for maritime use all year round.

The divide between the technically skilled and non-skilled workforce is highly contentious. Automation, robotics and distance learning have transformed the labor market. In 2020 and again in 2023, low-skilled workers across Europe and the China stage widespread riots due to wholesale shifting of textile, agricultural and manufacturing jobs to automated/robotic machinery. Industrial productivity continues to increase year over year and novel uses of 3D and 4D printing have enabled individualized products with little warehousing, segregating high-skilled and low-skilled workers in fracturing societies. Global criminal cartels are capitalizing on disaffected and unemployed low-skilled/Industrial Age skill individuals. The transnational criminal activity is being optimized in ways never before experienced and with alarming profitability with business and project management best practices available online. The rise of accepted crypto-currencies and exchanges permits rapid, secure transactions across national borders that complicates taxation and tariff enforcement.

USCG has seen demand for its services increase as maritime distress signals, at-sea sensors, port/harbor sensing, and transnational maritime crime are completely networked and on the rise. The USCG has seen port and maritime security missions increase with the increase in US Navy activities in the Far East, Europe and the Arctic. USCG resourcing increased only slightly from 2016 – 2025, and the Coast Guard has had to partner extensively across DoD, DHS, FBI, states, Industry, maritime partners, and International Consortiums to adopt and implement improved cybersecurity and cyber environment awareness across the U.S. domestic maritime domain. As the Departments and Agencies within the U.S. government gain confidence and are committed to partnering and common systems, the USCG has found it is adopting advanced technologies with increasing speed and operational impact – more robust and secure data systems, unmanned aerial systems, robotic/automated harbor systems, and optimized fusion centers.

Uncertainty		Alternative Future A	Alternative Future B	Alternative Future C	Alternative Future D
U1	Cooperation between government and private sector	**High Cooperation**	**Low Cooperation**	**High Cooperation**	**Low Cooperation**
U2	State Competition and Threat	**High Threat**	**High Threat**	**Low Threat**	**Low Threat**
U3	Degree of non-state competition and threat	High Threat	Low Threat	High Threat	Medium Threat
U4	Pace of IT/cyber technological development	High Pace	Low Pace	High Pace	Medium Pace
U5	Availability of Cyber educated personnel	Medium Availability	Low Availability	Low Availability	Medium Availability
U6	USCG reliance on publicly accessible networks	High Reliance	Low Reliance	Medium Reliance	Medium Reliance
U7	Competition between offense and defense cyber tools	Offense Dominant	Defense Dominant	Seesaw, but advantage w/offense	Defense advantage
U8	Cyber vulnerability of Maritime Transportation system	Med Vulnerability	Highly Vulnerability	Low Vulnerability	Med Vulnerability
U9	Identity Management/ Organizational trust	Medium Trust	Trust High	Medium Trust	Low Trust
U10	Willingness of government/ non-government to retaliate from an attack	Improved Sharing / defense measures	High Willingness	Medium Willingness	Low Willingness
U11	USCG Budget and Composition	Slight Improvement	Improved	Flat	Declining Budget
U12	Pace of USG responsiveness to cyber	High Adoption	Low Adoption	Medium Adoption	Low Adoption