Future B - Cybergeddon

THE SETTING

The year is 2025. In 10 short years, the private sector has widely, but unevenly adopted such powerful cybersecurity technologies such as block chain, Physically Unclonable Function (PUF), Field Programmable Gate Array (FPGA), Space/Time Algorithms, and Quantum computing technologies (to name a few), which have improved singular organization cyber resiliency and data security but reduced the incentive to cooperate with Government organizations. Much of the rationale for lack of cooperation stems from the inefficient and unduly tedious governmental processes to share information, the lack of indemnity, and the risk of litigation by privacy rights groups. There is a relatively modest threat level from non-state entities against the private sector due to game-changing advances in cyber security technologies and widespread adoption. Governments are unable to reach an accord on cyber laws and acceptable norms, and intergovernmental cooperation is modest, inhibiting uniform implementation of effective common cyber security. Most notably, NATO failed to accept the Tallinn Manual (aka the Tallinn Manual on International Law Applicable to Cyber Warfare) and closed the NATO Cooperative Cyber Defence Centre of Excellence over staffing standards. This lack of international cooperation is accompanied by increased internal USG competition for cyber funding, authorities, and personnel that result in frequent duplication of capabilities and constant legal challenges by corporations, NGOs, and other agencies. A 2018 economic downturn and friction between China and her neighbors over oil and mineral rights has led to substantial international tension. Nation states retain significant cyber capabilities despite the development of advanced cyber defenses. Autonomous cyber attacks against oil rigs in the Far East are seen as emanating from China and Chinese units continue to probe and steal key US and allied technology and weapons information. To stem the outflow of critical defense and leading edge intellectual property, private companies begin to develop organic active cybersecurity countermeasures (offensive capabilities) or hire cyber mercenaries to protect their infrastructure and Intellectual Property. Some have gone so far as to lobby the USG to issue “Cyber Letters of Marque and Reprisal” against the most flagrant sources of cyber malicious activity by noting that the authority is enumerated in Article 1 of the U.S. Constitution. The focus by industry increasingly tilts towards effective “individual security” as cybersecurity begins to drive the pace and adoption of new technologies. This focus drives an increased demand for high-skilled labor that the US education system is unable to produce, leaving the US reliant on foreign born or trained workers for many technical positions. There is increasing animosity between the government and private sector to balance productivity and domestic employment. In the 2024 election, a new US President, concerned about

2025 KEY DRIVERS:

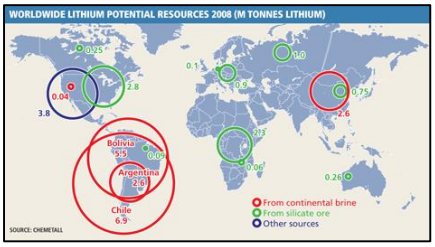
- Low cooperation among Governments
- Low cooperation among Governments and the Private Sector / Industry
- High level of Nation-State competition
- Low level of Non-State threats

potential for conflict in Asia and the Artic, increased defense and homeland security spending with resources provided by the post 2022 US recovery. The Coast Guard has significant additional resources that are focused on maritime critical infrastructure protection and maritime security. Continual friction among the international community and between US Allies and China has resulted in very real concerns to key US infrastructure and international mineral and territorial rights. Increased bellicose rhetoric in the Senkaku Islands area focused on claimed Economic Exclusion Zones by China and issues regarding international transit west of Attu Island in the Aleutians from the Russians has caused the US to rely more heavily on USCG presence vice US Navy presence. The USCG is becoming aware of "disruptions" to their networked maritime systems similar to the Navy's experiences in the late 2010's. Additionally, the USCG is finding Chinese and Russian ships in tactically advantageous positions prior to the USCG arriving on station. The competition for scarce resources and advanced technology is driving nations to an almost continual state of friction and mistrust, which has manifested itself in several regional flash-points. DHS has brought up the potential of cyber or physical attacks on USCG ships and aircraft, but the White House maintains a white hull would likely appear friendlier than a grey hull. Foreign fleets short of grey hulls use any hull to advance their objectives, complicating Coast Guard mission profiles.

Advances in transportation and green energy technologies are threatening the stability of energy-based economies in Russia, Venezuela and the Middle East. The networked Maritime Transportation System is perceived as increasingly vulnerable, particularly after a significant malicious cyber attack in 2023 initially attributed to North Korean cyber mercenaries. Commerce is severely disrupted in Europe and some in the international community suspect China to be using proxies for cyber operations.

BACKGROUND

The cyber-enabled environment has diminished the disparity between the "haves" and "have not's", at least among governments. As rare-earth rich countries and environmentally gifted countries make the jump from agrarian to informational countries (bypassing industrial age), they are capitalizing on U.S. education and ubiquitous distance learning programs to self-generate a new generation of engineers, computer programmers, scientists, and mathematicians to fuel their information societies. Since 2020, top lithium producers, such as Chile, Argentina and Brazil are the "new Middle East" and with international clout to match. Many advanced industries are completely reliant on Lithium, which is driving the material to incredible values. While these countries are on the ascent, they continue to deal with high government corruption, criminal cartels, unsecured boarders, and high criminal trafficking. In 2022, countries like Russia, Canada, Sweden, Norway, and Finland began capitalizing on their competitive advantage as "cold" countries to house the next generation of data storage, transmission and server farm housing. The investment enables them to capitalize on the minute advantages of information transport delay – high-speed trading, monetary disparity, and minute exchanges of data. The perceived exploitation of the Arctic and issues with receding Arctic ice initiated



international rancor over global warming and the accords contained within the 2015 Paris Agreement, which enabled a number of nations (notably Russia and China) to ultimately reject the Paris Agreement.

An economic downturn in 2018 resulted in a turn towards nationalism by the Chinese government. China and her neighbors are competing for drilling rights in East China and South China seas and tensions are high. The discovery of oil around 2020 near the Senkaku's by Chinese drillers exacerbated the friction. The US has responded by increasing patrols of Navy and Air Force assets. The USCG has several large cutters now deployed permanently out of the Philippines to provide white hulled assets for use in disputed waters and additional units deployed to provide port security throughout the Far East. In 2023, Vietnamese and Japanese oil rigs were sabotaged by anonymous cyber attacks. Most experts considered China the instigator.

The group "Anonymous" also resurged in 2018 with a massive release of ambassadors' private conversations conducted at the United Nations. Covering all 193 members, the 18-terabyte dump of private correspondence, conversations and photos ranged from mildly inane to outright offensive. This single event alone likely impacted a decade of trade negotiations and derailed a common framework for cyber defense. Various high level officials openly discuss the possibility that Anonymous is state sponsored. Anonymous struck again in 2019 and 2020 with the release of key and unfavorable details on U.S. and western companies negotiating in Asia and on the Russian periphery. Multinationals took note but given the effective difficulty of working with government many of these firms developed their own "cyber protection divisions" or hired non-US cyber protection "experts" to protect their intellectual property and their international market rights.

In 2023, the Global Maritime Transportation System was corrupted in such a way that all logistics data was unreliable for two days. This caused the entire global MTS to grind to all stop during the period, wreaking havoc on global logistics. Most experts suspected (without specific attribution) that North Korea was likely behind the action due to a stoppage of grain after the breakdown of nuclear discussions. In a twist of irony, the US, UK and Spain requested Lloyd's of London employ a Congolese cybersecurity group to "take action" against North Korea's Bureau 121 and No. 91 Office, both considered cyber warfare units.

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