Future C – Rise of the Geeks

THE SETTING

The year is 2025. In 2017 NATO ratified the Tallinn Manual on the International Law Applicable to Cyber Warfare (aka the Tallinn Manual) establishing rules and norms for warfare in the cyber domain; the United Nations followed suite with the Azores Accord, which established a framework for nations and private industry to collaborate on increasing cyber security and personal security in a "connected world." The 2019 Azores Accord enabled governments and the private sector to collaborate in cybersecurity by sharing information and adopting novel cyber technologies to combat terrorism, cyber crime and transnational criminal activities. The development of increasingly effective and powerful cyber capabilities and declarative policies have resulted in a state of cyber detente between nation states, but increased the threat from non-state actors and proxies who do not have physical infrastructure that can be held at risk.

2025 KEY DRIVERS:

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

Government practices and adoption of newer technologies and information sharing have diminished lesser criminal activity and low-level malware throughout the Internet. Although governments share information more freely and have successes against low sophisticated threats, there is a continual competition between disruptive and security capabilities and dominance shifts back and force among cybersecurity experts and expert hackers. The dramatic increase in technological innovation has resulted in rapid changes in the transportation and maritime industries, which increased incentives for criminal activity. Although the nation-state threat is diminished, new, powerful threats have emerged – the transnational criminal and hyper-empowered individual. Transnational criminals are bringing a wealth of resources to manipulate the cyber environment for criminal activities. Although DHS has infused the USCG with a 15% budge increase, the USCG struggles with governance, adoption and implementation of advanced technologies such as multi-intelligence data fusion, unmanned systems, remote sensors, and robotics with their accompanying personnel and supply chains

BACKGROUND

After Anonymous released private conversations of ambassadors to the United Nations in 2018, member nations used the event to galvanize support to cooperate and collaborate to protect the physical

security of officials and their personal security. The response established the unprecedented 2019 Azores Accord, which resolved indemnity and reduced liability with private industry companies that collaborated with U.N. member nation governments. Transnational companies rushed to support the articles within the Azores Accord, specifically those that protected intellectual property, opened member-nations to new technology, and created a common security framework with advanced cyber tools that stabilized and sped up temperamental government processes. The common security framework had the unintentional result of extending robust (i.e. not government accessible) data security and powerful cyber tools to almost any citizen or group within the member-nation.

Criminal organizations and savvy individuals alike immediately grasped the magnitude of the available cyber tools. With little bureaucratic obstacles, criminal cartels began to employ high tech specialists to adopt and implement big data analysis, predictive analytics, unmanned systems, and multi-source data fusion. Now cartels had new methods and new markets for illegal drug transportation, money laundering, counterfeit hardware, and human trafficking. Although international government collaboration with private industry was increasing the risk of software vulnerabilities, the promise of foreknowledge enabled by a more rapid implementation of technology maintains a wide profit margin for transnational, well-resourced criminal cartels. In response to the 2020 government confiscation of the Callie Cartel's data facility in Juarez Valley, Mexico, the Cartel accomplished the 2021 the shutdown of the Port of Houston for 4 days, causing an estimated $17 billion in losses and highlighting the power of transnational criminal organizations.

Super-empowered individuals are also using hyper-protected, anonymous and temporal flash-sites to coordinate flash-mob activities against governments, organizations, or individuals in violent objection to a policy or when a perceived slight is noted. Environmentalists in particular are using new, powerful cyber technologies to target a range of issues from endangered animal hunting, damaging fishing, climate change, and microenvironment protections. In 2020, a group calling itself Friends of the Andes used sequential and globally dispersed DDoS attacks to shutdown Lithium mining operations throughout Chile, Argentina and Brazil in response to toxic runoff from the Lithium mining operations. Additionally, groups such as Anonymous are using the public information on individuals combined with social media and network mapping to aggregate awkward and/or illicit information on public officials to cause outcry, embarrassment and/or expose illegal activity, often on a global scale. Multiple disclosures have caused ambassadors to be removed and, in some cases, physical risk to the officials.

Due to exact nanomaterial placement, 2019 was the Year of the Internet of Things (IoT). At the 2019 Consumer Electronics Show (CES), nearly 90% of the new technologies connected to the Internet. These developments in the transportation, logistics and communications sectors resulted in overcrowded bandwidth restraints and increased difficulty in conducting maritime and disaster response operations. The demand signal from new technologies and the compensation available outside of government have resulted in low availability of high-tech personnel to government organizations.

The US Coast Guard struggles with recruiting and retaining high-tech personnel to mid-grade ranks. In 2018, the military forces instituted a radically new framework for military members to serve as officers and specialists with full agility to switch between active and reserve and for term or career options. There is much anticipation that a flexible service capability will at least make high-tech specialists available to the government for military application. Although funding has increased, the pace of technology adoption has resulted in a de facto challenge to adopting, maintaining and expanding the use of advanced and cyber technologies.

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