



Alternative Futures in Cyber Security

Coast Guard Office of Emerging Policy – Evergreen IV

THE VICE COMMANDANT
OF THE UNITED STATES COAST GUARD



I am pleased to present the final report from the Evergreen Workshop: *Alternative Futures in Cyber Security*, which reflects the many long-term challenges and trends our service must confront in the cyber domain as we plan for an uncertain future. This report is the culmination of extensive research, expert opinions, and key insights gathered from over thirty cyber experts who attended a recent workshop. The Key Success Factors identified within this report should be consulted as the Coast Guard implements the Cyber Strategy and should inform processes and work within established policy.

Cyber technology is integrated in all aspects of Coast Guard mission performance. The exponential development and proliferation of technology presents unique opportunities for greater efficiency and effectiveness while expanding threats and challenges. The Coast Guard must become an agile and innovative organization, capable of adapting to rapid change in order to address the new reality and remain relevant in an increasingly fast-paced, digital world.

Cyber threats and challenges will continue to test our ability to ensure a secure, prosperous, and resilient maritime environment. Focus on the three strategic priorities in the cyber domain will remain a vexing problem for a variety of reasons: the ubiquity of the cyber domain allows for simultaneous attacks, the 'Internet of Things' facilitates an increasingly wired world, and cyber networks are becoming more complex with technology that can be exploited by an ever-growing user base, including insiders. The Coast Guard, as the steward of critical maritime infrastructure, must lead the effort to defend it from a broadening array of cyber threats and remain *Always Ready*.

The Key Success Factors are intended to inform the Coast Guard's ongoing Cyber Strategy implementation efforts; they will require careful stewardship of available resources and risk-informed decision-making. To this end, this report will further the vision for operating in the cyber domain as the Coast Guard "*Defends Cyberspace, Enables Operations, and Protects Infrastructure*."

Semper Paratus,

Admiral Charles D. Michel
Vice Commandant

Office of Emerging Policy / Evergreen
United States Coast Guard

About VES:

VES provides government and commercial clients with a range of professional and innovation services including: technology innovation acceleration, business consulting services, professional engineering and program oversight, and program and budget support. VES supports analysis and studies in a variety of areas including defense, energy and health care where we aid organizations in solving complex problems in new and innovative ways. VES is a veteran owned certified Service Disabled Veteran Owned Small Business (SDVOSB) and Veteran Owned Small Business (VOSB).

Workshop and analysis performed by Ventus Executive Solutions LLC under contract number GS10F178BA, issued by

USCG HEADQUARTERS (CG-912)
2703 MARTIN LUTHER KING JR AVE SE
STOP 7828
Washington DC 20593-7878

1 TABLE OF CONTENTS

2	EXECUTIVE SUMMARY	1
3	BACKGROUND AND OBJECTIVE	2
4	EVERGREEN PROCESS	3
4.1	SCHOEMAKER METHOD	3
4.2	OVERALL PROJECT PROCESS	4
4.3	UNCERTAINTIES ARE KEY	6
4.4	STRATEGIC SEGMENTATION	6
4.5	KEY SUCCESS FACTORS	7
5	ANALYSIS AND RESULTS	7
5.1	BACKGROUND RESEARCH	8
5.2	TREND AND UNCERTAINTY ANALYSIS	8
5.3	ALTERNATIVE FUTURES	12
5.4	HEADLINES	15
5.5	STRATEGIC SEGMENTATION	20
5.6	WORKSHOP AND DEVELOPMENT OF KSFS	22
5.7	WORKSHOP OUTPUT AND CONCLUSIONS	22
6	COMPARISON OF RESULTS WITH COAST GUARD STRATEGIC DOCUMENTS	27
7	CONCLUSIONS	28
	APPENDIX A: LIST OF PEOPLE INTERVIEWED FOR BACKGROUND RESEARCH	29
	APPENDIX B: RED CELL AND BLUE CELL ATTENDEES	30
	APPENDIX C: FOUR SCEANARIOS	31
	APPENDIX D: KEY SUCCESS FACTORS AND DEFINITIONS	47

EXECUTIVE SUMMARY

A combined team from the Evergreen Office and Ventus Solutions (VES) conducted a project that examined future cyber challenges for the U.S. Coast Guard (USCG) and identified strategic cyber needs of the U.S. Coast Guard (USCG) in the 2025 time frame.

Following rigorous research and analysis using scenario-based planning methods, the team identified twelve key forces driving future uncertainty for the USCG. The Evergreen/VES team then leveraged details from the twelve variables to build four worlds: *Band of Brothers*, *Cybergeddon*, *Rise of the Geeks*, and *Hedgehog*.

In a subsequent workshop, four teams examined each alternative future to identify key areas of leadership focus or emphasis for Coast Guard consideration. These areas of emphasis—called Key Success Factors (KSFs)—are designed to enable the Coast Guard to continue to perform above peer organizations. VES provided a number of methodologies and algorithms to both weight output from each team and to aid in selecting a temporal strategy for possible implementation.

Thirty-seven KSFs were selected by the teams, with a wide range of recommendations across Coast Guard culture, organization, training, manning, and resourcing. Of these, thirteen ranked significantly higher across multiple alternative futures. VES then examined interactions between KSFs, and along with workshop scores, provided a recommendation for seven KSFs to be examined in the near term by Coast Guard leadership. These are:

- **Professional Cyber Career Field**
- **Adaptable, Flexible Human Resources System**
- **Tolerance for Innovation**
- **Cyber Center of Excellence**
- **Enhanced Operational Training for Cyber Units**
- **Cyber Mission Teams**
- **Resilient Infrastructure with Enclaves**

We recommend Coast Guard leadership begin by pursuing the first three KSFs. They represent corporate cultural changes that are necessary for continued mission success in the future. Of note, workshop participants placed a high emphasis on protection of the Maritime Transportation System; accordingly, the “Resilient Infrastructure” KSF ranked highly. Furthermore, we recommend that the Coast Guard consider Innovation Pools (collaborative research and development activities with private sector organizations) for inclusion in the top group of thirteen, as it could be a high payoff collaboration with the private sector on cyber.

Finally, the team conducted a review of the results and compared outputs with the 2015 *USCG Cyber Strategy*. We found the results consistent with the current strategy, but also noted that the vast majority of the KSFs align with the seven long term success vectors of the strategy. This team believes cyber poses a significant challenge to the USCG, but believes there are a number of actionable, near-term steps that can be considered to help the Coast Guard achieve its objectives in the coming years. Pursuit of the top KSFs is a prime place to start.

2 BACKGROUND AND OBJECTIVE

The purpose of this project was to examine future cyber challenges for the U.S. Coast Guard and to identify and synthesize solutions to complex problems that could arise from those cyber challenges. A key element of the project workshop was to develop alternative future world scenarios focused on the cyber domain that would enable insight into the future Coast Guard operating environment. An additional project goal included identifying strategic needs in anticipation of these future-operating environments.

The White House 2015 National Security Strategy highlights cybersecurity as an escalating challenge.¹ Ensuring cybersecurity remains a particularly difficult problem to solve for a number of reasons: attacks may come from anywhere in the world at any time, the physical world is increasingly connected to cyberspace, and cyber networks are becoming progressively more complex, with technological change bringing both new vulnerabilities as well as opportunities. Threats may come from National governments, terrorists, organized crime groups, hackers, or disgruntled insiders. Understanding the magnitude of the challenge, U.S. Coast Guard (USCG) Senior Leadership published a new USCG Cyber Strategy in June 2015. This strategy articulated the Coast Guard vision for cyber operations and noted: *“We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation’s critical maritime infrastructure.”* As part of this document the Coast Guard identified the rapidly evolving cyber domain and cybersecurity as one of the most serious economic and national security challenges of today.²

The overall mission of the Coast Guard is to ensure the Safety, Security, and Stewardship of our Nation’s maritime interests in the heartland, in the ports, at sea, and around the globe. As part of this broad overall mission, the Coast Guard must execute eleven statutory missions. In our view, virtually any operational mission conducted by the Coast Guard in support of its statutory mission incorporates use of technology and networks with potential cyber vulnerabilities. As noted in the Coast Guard’s 2015 strategy, the service must strategically adapt to meet the challenges of the digital era. First and foremost, the Coast Guard must embrace cyberspace as an operational domain. The USCG’s Cyber Strategy identifies three distinct cyber priorities critical to overall mission success: Defending Cyberspace, Enabling Operations, and Protecting Infrastructure. The Evergreen project objective is to enable this future mission success.

¹ White House. National Security Strategy, Washington, D.C., February 2015, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

² United States Coast Guard Cyber Strategy, Washington, D.C., June 2015, <http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf>.

3 EVERGREEN PROCESS

The Evergreen Office (Office of Emerging Policy) supports Coast Guard strategy development and is a key element of the USCG strategic foresight initiative. That initiative is to provide defined and vetted strategic needs and instill strategic intent throughout the service by engaging various levels of internal and external stakeholders through scenario-based planning methods. Evergreen uses scenario-based planning methods to identify and synthesize solutions to complex, strategic problems and to develop strategic needs in preparation for a highly dynamic and constantly evolving operating environment. In short Evergreen helps the Coast Guard prepare for an uncertain future.

In 2015, with Evergreen IV the Coast Guard started a trend towards executing shorter-term, more subject-based efforts with a time horizon of approximately ten years. Evergreen intends to delve deeply into specific topics such as cyber, the Arctic, energy, climate change, and others as directed by Coast Guard Senior Leadership. Drilling down into a specific area enables Evergreen and associated stakeholders to consider in more detail how future uncertainties could impact the Coast Guard operating environment in these specific areas. Scenario Planning

Organizations use Scenario-Based Planning to get around a fundamental problem of long term planning: no one can predict the future. In this process, a team attempts to bound the future by creating a number of plausible futures. Typically, these scenarios stretch ones' thinking to allow planners to consider new or unforeseen possibilities. By examining a number of different future worlds, planners gain a better appreciation of what capabilities an organization might need to emphasize to improve the odds of future success and they gain some understanding of the complex interactions among variables. Scenario planning avoids a common weakness of linear planning, i.e., the future will be like the recent past.

Organizations tend to underperform when developments proceed along a different path than expected. In the renowned book The Innovator's Dilemma, Harvard professor and businessman Clayton Christensen notes how even disruptive innovators can get blindsided by other disruptive technologies and technologists. Christensen demonstrated that leaders of these technology companies did not anticipate or comprehend how new technologies might impact their businesses.³

Scenario-based planning reduces the probability of these surprises and helps organizations prepare and "future proof" their decisions.

3.1 SCHOEMAKER METHOD

There are a number of methods used to conduct scenario-based planning. Peter Schwartz and Paul Schoemaker have each advanced their own methods. This project used a modified Schoemaker method, for this method enables one to bound the future and then provides a well-organized approach to determining follow-on activities. Schoemaker, a pioneer in the field of decision sciences and Research Director of the Mack Institute for Innovation Management at the Wharton School (University of Pennsylvania), considers scenario planning to be an attempt to "capture the richness and range of possibilities, stimulating decision-makers to consider changes they

³ Clayton Christensen. The Innovator's Dilemma, New York: Harper Business, 2011.

would otherwise ignore.”⁴ It is important to highlight that scenarios are used to bound the future instead of forecasting the future. The basic method is presented below in Figure 1:

	Step	Explanation
1	Define Scope	Define issues to be understood by the organization in terms of time frame, scope and decision variables.
2	Identify Major Stakeholders	Identify major stakeholders, who are affected or may influence the issues, they may be both internal and external to the organization.
3	Identify Main Forces	Identify and study the main forces that shape the future within the scope looking at social, economic, technological, environmental and political domains.
4	Identify Trends	Identify which forces are trends and understand how they will affect the issues of interest.
5	Identify Key Uncertainties	Identify the main uncertainties from the list of forces, how they interrelate, and rank them on both importance and degree of uncertainty.
6	Construct Initial Scenario Themes	Select the two uncertainties of greatest importance and greatest uncertainty, and develop a 2x2 matrix of plausible scenarios. Suitable outcomes from other key uncertainties and trends are added as elements to all scenarios.
7	Check for Consistency and Plausibility	Assess the consistency and plausibility of the initial scenarios; are trends compatible within the time frame, are outcomes of uncertainties combined in logical manner, and are the presumed actions of stakeholders compatible with their interests?
8	Redefine Scenario Themes	Reassess the ranges of uncertainty variables and retrace the steps to develop final scenarios.

Figure 1: Basic Schoemaker Method

4 OVERALL PROJECT PROCESS

VES employed the Schoemaker process and merged it with the Evergreen process to provide a robust strategic planning process that supports the Coast Guard mission. We depict the overall process in Figure 2. The following sections detail critical elements of this strategic planning process.

⁴ Paul J.H. Schoemaker and V. Michael Mavaddat. “Chapter 10: Scenario Planning for Disruptive Technologies” in Ed. George S. Day and Paul S. Schoemaker, Wharton On Managing Emerging Technologies, Hoboken: John Wiley & Sons, 2000.



Figure 2: VES derived Evergreen strategic planning process

4.1 UNCERTAINTIES ARE KEY

Forces can include trends and uncertainties. Trends have a high probability of occurring in the future, and frequently are accounted for in organizational planning. An example of a trend would be the aging population of Baby Boomers. The well-anticipated aging of the “Boomers” and the resulting population bulge means that baby boomers drive a significant and growing portion of government and private sector spending in a number of key areas including: health care, retired housing, investments, retail purchasing, and transportation. Businesses and organizations can anticipate and plan around these demographic-driven changes.

Scenarios Bound The Future

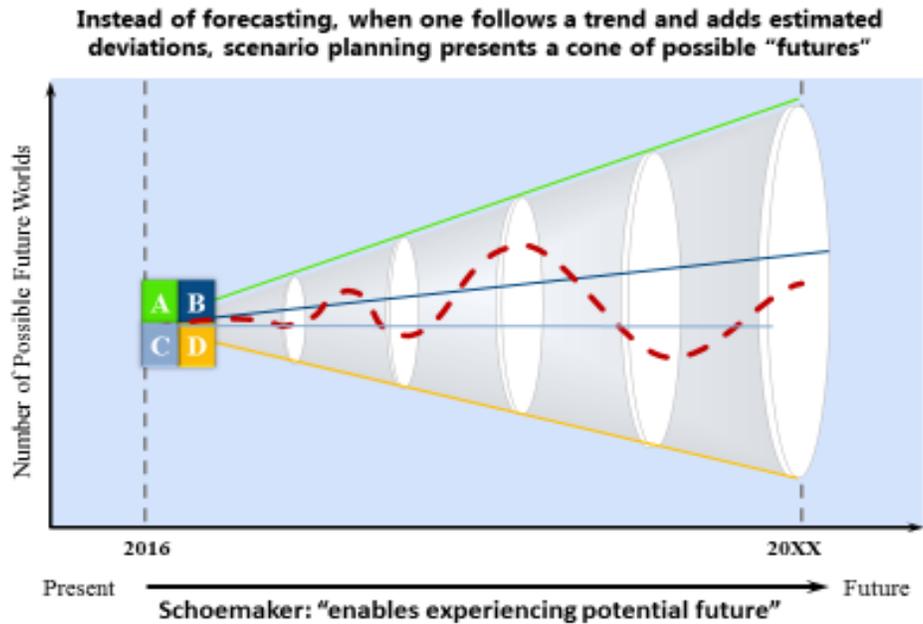


Figure 3: Bounding Possible Futures

Uncertainties are those forces that have an unknown level of predictability and impact. New technologies and innovations can certainly drive uncertainties but an organization or business will likely have a difficult time determining the full impact of new technologies. An example of an uncertainty is “what role will the development of Artificial Intelligence play in ten years?” There is a wide swath of possibilities regarding the development of Artificial Intelligence, which could dramatically influence society, organizations, and individuals. Both the scale of change and the likelihood of change occurring impacts an organization’s planning. As a result of the importance of uncertainties, we concentrated on examining cyber- and Coast Guard-related uncertainties during development of the alternative futures process.

4.2 STRATEGIC SEGMENTATION

This project conducted a strategic segmentation exercise to understand the operations of a defined organization and to understand how to optimize performance given a current or future operating environment. Such a segmentation exercise ensured the project team examined all key areas of operational responsibility. The benefits of strategic segmentation are several fold:

- Focuses resources on “strategic” initiatives
- Improves service to stakeholders
- Aligns activities for impact

- Aligns strategy with the outside world
- Recognizes competitors, opportunities, and threats
- Visualizes evolution of operating environment

The Evergreen/VES team conducted a concise analysis of the eleven statutory Coast Guard mission areas. The intent of this analysis was to ensure that during the workshop, attendees considered both the breath of the Coast Guard mission areas as well as the interests of various Coast Guard constituent elements and stakeholders. We grouped similar activities to aid workshop attendees to efficiently consider the impact of alternative futures.

4.3 KEY SUCCESS FACTORS

Key Success Factors (KSFs) are areas of leadership emphasis that will enable an organization to perform successfully in a given environment. Development of KSF's corresponds with the Evergreen process of developing defined and vetted strategic needs as well as instilling strategic intent. We also highlight that KSFs are designed to enable and support the USCG internal requirements generation process. KSFs provide an area of emphasis or focus for development of these requirements. Areas of emphasis that provide value across multiple alternative futures are "no regret" moves in that they add value in a large number of plausible futures. Carefully crafted requirements generated to support these KSFs should significantly aid the Coast Guard maintain its status as a world class organization.

It is important to note that KSFs do not encompass all the activities an organization may undertake. In the case of the Coast Guard, building high quality cutters and aircraft is an essential part of maintaining a robust Coast Guard. We would not consider this a KSF but rather a form of "table stakes"—necessary and important activities but ones that do not necessarily discriminate a successful organization from a great organization. Instead, KSFs consist of those activities that enable an organization to provide exceptional and resilient capabilities. KSFs can involve non-material changes, such as changes to organizational structure, culture, or training as well as investment in key material capabilities.

5 ANALYSIS AND RESULTS

The Evergreen/VES team designed four alternative future world scenarios focused on the cyber domain. We developed these using the methodology discussed in Section 3 of this report and with additional, pertinent detail discussed in this section. As part of this process, VES and Evergreen held three pre-workshop team meetings including Blue Cell and Red Cell focus groups with over a dozen attendees. The intent of the large number of touchpoints was to ensure that Coast Guard stakeholders could work closely with the VES team to shape the final product. In short, this final product is a result of significant collaboration with both Coast Guard uniformed and civilian thinkers as well as outside stakeholders.

5.1 BACKGROUND RESEARCH

In preparation for the project, the Evergreen/VES team set analytical boundaries. The team chose a ten-year time horizon based upon the rapid pace of technological development. In addition, the selected ten-year time horizon provided a reasonable period for leadership focus on Key Success Factors that can pay dividends. The team also selected a global scope for USCG missions. Finally, the Evergreen/VES team determined that the scope of the analysis should include not only the future of cyber, but also changes in other technological drivers for the Coast Guard. Other technological changes would imply second order and tertiary effects on cyber and the Coast Guard mission set and analytical rigor required their consideration as part of a cohesive whole.

The team conducted substantial background research at the onset of the process to understand future. As part of this research, we conducted a significant number of interviews with individuals inside the Coast Guard, cyber and technology experts in the private sector, and a renowned futurist (see Appendix A). The interviewees were told to think about the future of cyber, using a 2025-2030 timeframe, and how it could affect them operationally. They were queried about significant cyber events that had affected the USCG, and how well these events were anticipated. Questions also teased out the degree to which Coast Guard reliance on Information Technology (IT) systems, distributed sensors, and software might change in the future and how particular mission sets might be affected. In addition to the interviews, VES surveyed a significant number of outside reports and analyses to determine how cyber and associated technologies might change in the future. As part of this process, VES incorporated two cyber experts with substantial National Security Agency (NSA) experience to aid the research effort.

5.2 TREND AND UNCERTAINTY ANALYSIS

As a result of the research and interviews, VES identified more than 180 future forces that might have impact on the Coast Guard. VES then determined whether these forces were trends or uncertainties. After analysis, VES identified 20 Key Trends (see Figure 4).

USCG – Key Trends

- Data as an increasing part of firm/organization value
- Replacing labor through lower cost automation
- Push towards robotics/automation AI
- Increased use of digital technologies and interconnectivity
- Within maritime transportation system, each ship continuously networked sensor and node within the global information grid
- Increasingly relying on digital communication
- Increased personal empowerment through social media (everyone an on-scene reporter--'hyper-empowered individual' able to voice opinion, start movements, and conduct actions on a global scale with personal perspective.... Or agenda.)
- High-speed transactions will cause linked, cascading direct effects and second/third order effects will be more damaging and widespread.
- Governments and organizations will continue to have to address issues such as privacy, ownership and security.
- State Fusion Centers will be increasingly connected and required to respond to intra-state activities.
- Evolved and sophisticated threats to critical infrastructure and human implants will increasingly blur the distinction between cyber and physical attacks.
- DoD / other Federal Departments will increasingly be tasked with overlapping missions that do not require a Title 10 response.
- New information networks will enable rapid analysis of large data sets (i.e. Big Data) that will enable a statistical prediction of events from historical patterns.
- Three vital areas of cyber resilience: focus on information sharing, critical infrastructure and policy development.
- In a constant networked environment, not every single system can be protected to the same level, requiring prioritization.
- Networked information logistic systems will optimize the Maritime Transportation System in a way that cannot be man-reproduced, which asymmetrically increases the repercussions if a system is compromised, damaged, or destroyed.
- Global media coverage and real-time reporting of local issues magnifies and intensifies governments and industries to respond quickly to news stories, especially those involving emergencies and humanitarian issues.
- Public and government demand for immediate understanding, response and mitigation to "Black Swan" events fueled by global media coverage.
- National systems for intelligence collection will increasingly be demanded to support disaster relief and humanitarian assistance operations both regionally and globally.
- Due to climate change, the volatility and seriousness of catastrophic disasters, especially along coastal areas, will increase the demand for emergency response resources.

Figure 4 - Key Trends

Trends, while important, generate less impact on organizations and remain easier to plan for. Consequently, the Evergreen/VES team then shifted its focus to uncertainties.

Uncertainties – Unpredictable Forces. The remaining 180 forces were ranked by their degree of uncertainty as well as the degree to which they their importance and potential impact to the Coast Guard. As a result, the team narrowed the overall list to 26 key uncertainties (see Figure 5).

Key Uncertainties (*top 26*)

- Degree of globalization of networks
- Degree of cooperation between government and commercial industry on cyber matters
- Degree of cyber educated labor
- Effectiveness of offensive vs defensive tools
- Degree of tech integration w/maritime systems
- Ease of access/use of effective attack/def tools
- Degree of USG reliance on publicly accessible networks
- USCG budget and composition of budget
- Willingness of gov/non-gov organizations to retaliate to cyber attack
- Degree of state competition/and threat
- Degree of non-state competition and threat
- Number of sophisticated criminal networks
- Reliance of econ/USG on existing info network
- Degree of US econ reliance on international trade in general and energy in particular
- Degree of vulnerability on Maritime Transportation System
- Degree of concentration of USCG efforts domestically or in 50 states
- Pace of USG responsiveness to change in cyber
- Pace of technological development
- Degree of automation of networks
- Impact of AI cascading failures
- Degree of advance in non linear computing power
- Adequate funding for cyber lifecycle maintenance
- Cultural proclivity to prefer security over performance of system
- Degree of asymmetry in attack
- Climate change impact on littoral vulnerably and arctic
- Ability to identify personal and users and trust- identity management and interaction be individual and organization trust

Figure 5 – Key Uncertainties

Figure 6 contains a graph of these key drivers plotted by their impact on the Coast Guard missions and their degree of uncertainty. The list of 26 was further whittled down to 12 forces that stood out from the rest in terms of impact; these are in order of rank:

Office of Emerging Policy / Evergreen
United States Coast Guard

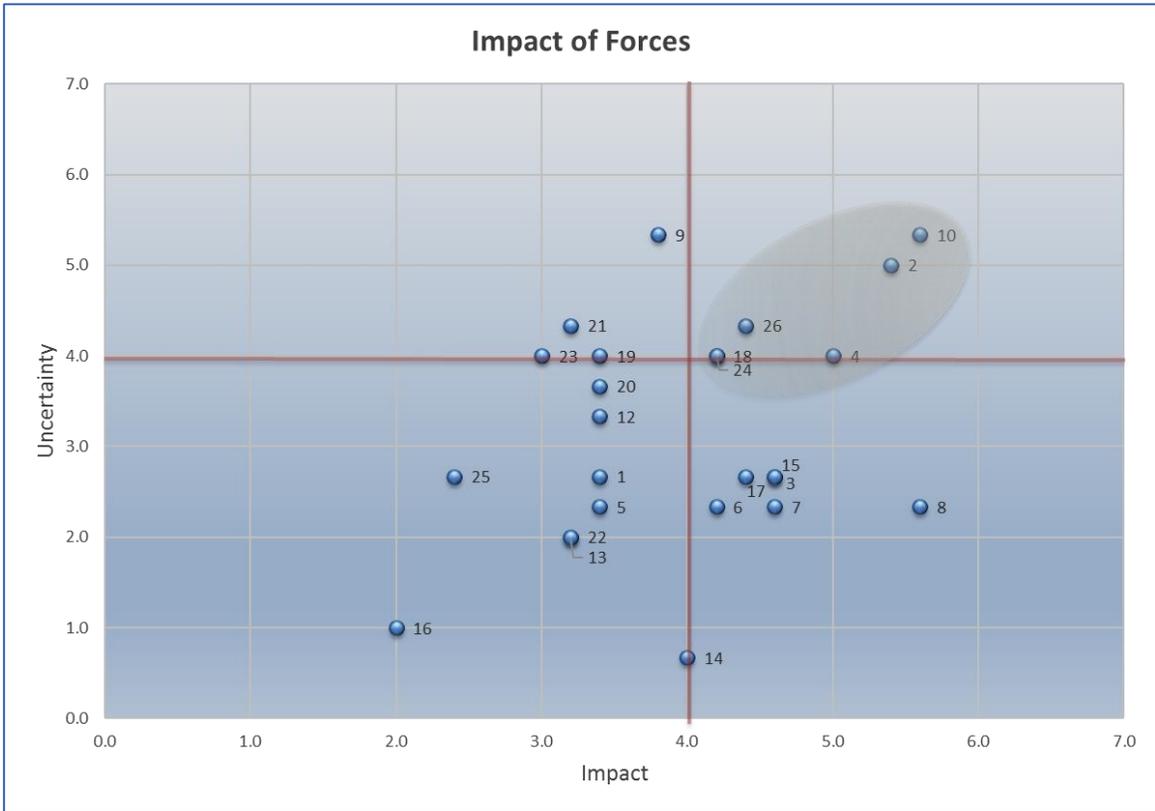


Figure 6: Degree of Uncertainty and Impact of Key Forces

Uncertainty			
U1	Cooperation between governments and between the government and private sector	U7	Cyber vulnerability of Maritime Transportation system
U2	State Competition and Threat	U8	Identity Management/ Organizational trust
U3	USCG Budget and Composition	U9	Willingness of government/ non-government to retaliate from an attack
U4	Availability of Cyber educated personnel	U10	Pace of IT/ Cyber technological development
U5	USCG reliance on publically accessible networks	U11	Degree of non-state competition and threat
U6	Competition between offense and defense cyber tools	U12	Pace of US government responsiveness to cyber

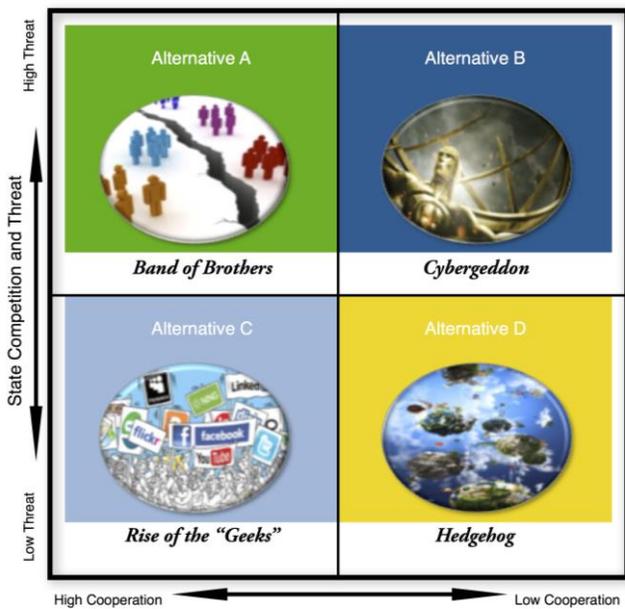
Figure 7: Top Twelve Key Uncertainties

The Evergreen/VES team ran a Blue Cell mini workshop with over a dozen service and civilian as well as outside experts in attendance. We verified our weighting of the various forces and using Human Centered Design tools (HCD) we determined the key drivers of the alternative futures. We then developed the initial alternative futures designs. After additional analysis, the Evergreen/VES team then executed a Red Cell mini workshop. The Red Cell also had 12 Service and civilian Coast Guard experts in attendance as well as outside experts. As part of that effort, the team finalized the draft of the alternative futures and selected the appropriate segmentation of Coast Guard mission areas to prepare for the final workshop. Blue Cell and Red Cell attendees can be found in Appendix B.

5.3 ALTERNATIVE FUTURES

As discussed, using scenario-based planning does not enable forecasting or predicting the future; instead, such planning bounds the future. VES built a scenario matrix starting with identifying the two drivers that are the most uncertain and the most critical in terms of impact on the organization. A 2x2 matrix is constructed from the extremes of the two drivers. VES presented three scenario options at the Blue Cell meeting:

- Degree of Cooperation between governments and between government and the private sector vs. pace of IT/Cyber related technological
- Degree of State Competition/threat in cyber domain vs. degree of cooperation between governments and between the government and private sector



- Degree of cooperation between governments and between the government and private sector vs. Competition between attack and defense tools

The Blue Cell team members selected the second option and then requested a minor change. They requested that the major force “degree of cooperation between government and the private sector” be divided into two separate uncertainties when space permitted (i.e., “degree of cooperation between government and the private sector” and the “degree of cooperation between government”). Such descriptions more fully underline the necessity of collaboration in two directions. The result of these drivers is a 2x2 matrix incorporating 4 major alternative futures (Figure 8).

Figure 8: 2 x 2 Matrix with 4 Alternative Futures

Office of Emerging Policy / Evergreen
United States Coast Guard

A blueprint of the four scenarios was made using the final 12 uncertainties derived from the Blue Cell. The resulting blueprint is pictured in Figure 9. Four scenarios were devised from the blueprint: Band of Brothers; Cybergeddon, Rise of the ‘Geeks’, and Hedgehog. Of note, each alternative future incorporates a mix of twelve major uncertainties leading to a rich and varied view of the future. We include the full write up of the scenarios in Appendix C.

Blueprint

Uncertainty		 Alternative Future A	 Alternative Future B	 Alternative Future C	 Alternative Future D
		U1	Cooperation between government and private sector	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 often 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 / defensive 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

Figure 9: Blueprint of twelve major uncertainties

In the scenarios Band of Brothers and Rise of the ‘Geeks’ there is significant cooperation between the government and the private sector, and government and civilian entities work together sharing and collaborating to combat issues in the cyber domain. In these two futures, there exists a high threat from non-state actors, as cyber crime yields significant benefits for criminals. The major difference between these two scenarios is the cyber threat from other nation-states: in the Band of Brothers the threat is also high from nation states, while it is low in Rise of the ‘Geeks’. The remaining two scenarios are characterized by low cooperation between the government and the private sector, with little sharing between the two; the major difference between these two is again the cyber threat from other nation states. Of note, internationally, one future has international friction/competition comparable to today; two are more benign international environments and in one future there is significantly more international friction than today. The complete scenarios are located in Appendix C. A short synopsis of each follows below:

The first Scenario can be characterized by bands of allies working together against common threats. **Band of Brothers:** International friction remains relatively elevated, and the cyber threat is high from both state and non-state actors. The pace of technological advances has been unrelenting since 2015. Advances in automation, robotics, and education have transformed the labor market. The divide between the skilled and non-skilled workforce is highly contentious, and criminal cartels are capitalizing on this divide. Individuals and institutions are networked like never before; these networks are vulnerable to cyber attacks. In 2019 an anonymous cyber attack against Iran crystallized the danger of state sanctioned cyber attack. Not to be outdone, transnational criminals employ increasingly sophisticated tools to challenge industry. IP theft threatens innovation and economic survival. With global private industry, governments agree to international norms and standards in cyberspace, resulting in a high degree of cooperation. Cooperation and sharing become important within agencies and between Allies in a world where cyber offensive tools are dominant. USCG missions grow, and it remains a valued interlocutor internationally. However, USCG funding increases only modestly.

Cybergeddon: Cyber judgment day, is defined by low cooperation and high distrust between government and private industry. The private sector has widely but unevenly adopted powerful cybersecurity technologies such as blockchain, which has greatly improved cyber resiliency and data security. These new cyber defense technologies reduce the threat from non-state actors but also reduce cooperation between government and the private sector. A 2018 economic downturn has led to friction among nations in the Pacific, and the principal cyber security threat emanates from nation states. Significant competition for scarce resources is leading to friction and sometimes border skirmishes. The private sector decides to protect itself or hire cyber mercenaries and develops active cybersecurity countermeasures (offensive cyber capabilities) to protect intellectual property. The increased industry focus on cybersecurity drives the pace and adoption of new technologies and a resulting increased demand for high-skilled labor. The U.S. education system is unable to keep pace with demand, leaving the U.S. reliant on foreign born and trained workers. The USCG has significant additional resources but has new concerns with the rising external threats. In particular, the Maritime Transportation System is at risk.

It is good to be a 'Geek' in the scenario **Rise of the Geeks:** Significant international cooperation exists and a series of international agreements establishing rules and norms for warfare in the cyber domain, has led to a reduced risk of cyber-attacks from state actors and an improved international climate. Although the nation-state threat is diminished, new, powerful threats have emerged—transnational criminal networks and hyper-empowered individuals—as evidenced by the 2021 seven billion dollar J.P. Morgan theft. There is a periodic swing in dominance between cybersecurity experts and expert hackers and their associated offensive and defense tools. Rapid changes in the finance, transportation and maritime industries have increased incentives for well organized criminal groups to exploit. As a result, government and private sectors collaborate widely to combat international crime. Bandwidth is in shortfall. Consequently, it is a good life for Geeks: a life of crime pays and cyber personnel are everywhere in short supply. The significant pace of technological innovation challenges the USCG with obsolescent software and required mid-life upgrades.

In the final scenario, the government behaves much like a Hedgehog—curled up and inwardly focused. In **Hedgehog** a second era of détente and the 2019 economic downturn focus government on economics, and there is little cyber cooperation. Domestic issues are dominating the political landscape, drawing attention away from international security topics. Most of the cyber threat emanates from criminals/transnationals, but even in the private sector the threat is somewhat benign due to proliferation of robust defense technologies. Governments struggle to enact cyber policies or accords, which fosters distrust with the private sector. Societal friction increases

the insider threat. Commercial technology outpaces the ability of government agencies to upgrade. The Internet remains a playground for small time criminals and transnational gangs along with hyper-empowered individuals that transcend national sovereignty boundaries. But generally, large transnational criminal organizations find greater opportunity elsewhere—particularly the development of new and increasingly powerful illicit drugs. USCG funding is declining given the challenges of entitlement spending, with subsequent delays and reductions in USCG programs.

5.4 HEADLINES

Participants were asked to imagine news headlines for the years leading up to 2025 for each of the scenarios. This process helped to immerse the participants in their futures in order to provide a better feel for what capabilities would be needed to win in those futures.

Band of Brothers

2016

- Cartel's Traffic Cocaine into U.S. with Container Ship – Hijacked Manifest at Fault
- Drones Threaten America's Drug Interdiction Efforts
- Cyber Attack Against Lithuania, NATO Invokes Article 4 "An Attack On One Is an Attack On All"

2018

- Russia's New Cold War
- BRIC Establishes Cyber Alliance in Response to Western Alliance Cyber Cartel
- Israel Suspected of Cyber Attack Against Iran: Iranian Power Grid Collapses

2020

- Cyber Threats to Electric Grid Threaten National Security

2022

- Saudi Arabia Leads OPEC in Lowering Oil Prices to Discourage Russian Exploration

2024

- Worldwide Havoc Within Reach of Every Human
- Cartel Installs Undersea Cable to Improve its Crypto Exchange

2025

- Arctic 'Lightship' Hijacked: 3 Oil Tankers Run Aground, Millions of Gallons of Oil Spilled

Cybergeddon

2016

- Russia Reject Cyber Norms; Putin: "These Are American Neo-imperialist Ideas"
- Apple Supply Chain Severely Disrupted
- Consumer Innovations Thunder Past Government Investment in Cyber
- ISC Hacks Multiple U.S./Foreign Banks

2018

- You Said What? Framework for Cyber Defense Deal Derailed
- Kuwait's Large-scale Desalination Plant Fails—Questions of Cyber Attack Raised
- Google Announces Offensive Cyber Capabilities as Hacks Increase
- Japan and Republic of Korea Agree to Joint Naval Patrols, Seen as Response to PRC
- Could International Impasse Lead to the Rise of Cyber Nations?
- Rise of The Hacker: UN Data Breach Halts Trade Talks

2020

- Chile, Argentina, Brazil Demand Security Council Seat Amidst Growing Clout
- Drive for Lithium Propels 3rd World Countries onto Global Stage
- Industry Threatens to Act on Cyber Theft

Office of Emerging Policy / Evergreen
United States Coast Guard

- The Rise of the Offshore Knowledge Economy
- Anonymous Torpedoes Cyber Defense Framework
- Drive for Oil Places China & Japan at Odds in the Senkaku Islands

2022

- Paris Accord Collapses Amidst Tension over Arctic
- Lithium Shortage Expected as Cartel Gains Control of Major Mine in Argentina
- U.S. Education Gap Leads to Loss of World Markets
- U.S./S. Asian Countries Establish Exclusive Trading Relationship
- Ships Halted! Cyber Attack Freezes Worldwide Shipping

2024

- Spike in Food Prices Due to North Korean Cyber Attack
- Data Farm Opened in Arctic
- “Who needs government?” Private sector speeds ahead, leaves Feds squabbling
- U.S. Increases National Security Spending to Combat Asia-Pacific Threats
- Cyber Attack Halts Global Maritime Trade

2025

- U.S. Places Sanctions on China
- President Seizes Cyber Firms in Act of National Security
- No Really: Quantum computing is almost here!

Rise of the “Geeks”

2016

- Credit Card Companies’ Profits Soar with New Chip/Pin Technology

Office of Emerging Policy / Evergreen
United States Coast Guard

- Facebook Hacked!
- Apple Watch Now Compatible with All Other Devices
- U.S. Enters Agreement with China On Sharing Cyber Threats
- Drone Assassination Attempt on Wisconsin Governor Thwarted

2018

- Savvy Cyber Actors Increasing Threat
- Coast Guard UTS Hacked Ports Closed as A Result
- Alaska Fishing Fleet Misguided to Fish Illegal Area Via Spoof of AIS Signals
- Privacy Groups Wary of International Cooperation
- New Jersey Public Schools to Go Paperless by 2021
- Trans-Pacific Partnership: Global Cyber Agreement Reached!

2020

- Cartels' Cyber Sophistication Skyrockets
- Experts Say "Beware Hackers, White and Black Hats"
- Drones Capture Never Before Seen Images of Remote Places on Earth
- Logical, Private Infrastructure ... For A Price
- 2020 – The Internet of Everything
- NATO: Cyber Attacks Are Physical – Warns Anonymous, Others of Consequences

2022

- Pfizer Announces Chip/Pump Drug Delivery System Controlled by App
- J.P. Morgan, Still Reeling, Merges with Bank of London
- Discarded Internet of Things (IoT) 'Things' Now Source for Terrorists to Mine Data, Plan Attacks
- California Announces Consumer Consent for Any Chip-Containing Good
- CG Deploys First Unmanned SAR Boat & Station Gloucester—More to Come

2024

- Home-Based Generator/Battery Power Market Soars Following Blackout

Office of Emerging Policy / Evergreen
United States Coast Guard

- “CG with Caribbean Partners Stop \$150B of Drugs at 24 Ports Simultaneously”
- I’m a Person Not a Data Point!
- Public Concerned About IoT and Privacy with Everything Tracked

2025

- U.S.–UK Open Joint Naval Cyber Range
- Princeton Review Revamps SAT to Include Computer Literacy Test
- Attack of the Killer Coffee Pots! Why The IoT Was Not Such a Good Idea

Hedgehog

2016

- Apple Looks Elsewhere; Half of Its Suppliers Factories in China Shuttered
- Microsoft Warns Government It Will No Longer Support Legacy Software

2018

- Federal Agencies Can’t Find CIO’s
- LA/LB Grinds to Halt Due to Malware - Poor Oversight, \$4B Lost Revenue
- DHS Taps Coast Guard to Lead Cyber Strategy
- Private Cyber Security Firms’ Stock Soar
- Longest Security Compromise in DoD History Due to Unsupported OS
- Putin Dies, Russian Region Stabilizes

2020

- FAA Ground Aircraft—\$2B Per Day Losses Due to SW Issues
- Record Retirements Cripple Education System Without Young Teachers
- Congress Calls for Review of Pentagon Systems After 5th Cyber Treason
- SGX 3G Stumps NSA

Office of Emerging Policy / Evergreen
United States Coast Guard

- Maritime Cyber Security Software Firm Contracted to Secure Ports
- USCG Mission & Vessel Inspection Programs Unfunded—Shift to Private Industry

2022

- U.S. Closes Borders to New Immigrants
- USCG Skills in Demand Globally!
- Quantum Encryption V3 Release
- North Slope Fracking Stable Despite Middle East Oil Crisis
- Oil Industry Demands New Cyber Governance

2024

- Cartel Uses Malware to Shut Down NSC
- DHS Called “Laggard” By Congress Over Lack of Technology Updates
- International Shipping 100% Automated
- Keystone Pipeline Unavoidable with Saudi Crisis
- USCG Yields Cyber Authority to Cyber Safe Inc.
- Government Shut Down for Month Following Anonymous Hack

2025

- No End in Sight for Refugees in Italy
- Offshore Energy 100% Automated
- DHS Sheds TSA & Combines Efforts with Customs

5.5 STRATEGIC SEGMENTATION

The Evergreen/VES team conducted a strategic segmentation to examine Coast Guard operations and to determine how best to optimize Key Success Factors that might improve these operations. Whereas one might consider alternative futures as the future “weather” the USCG will face, the strategic segmentation is the “terrain”

on which the Coast Guard will be operating.⁵ The team considered multiple ways to segment Coast Guard operations including:

- Type of operation/mission areas
- USCG commands and entities
- Potential Threats/Adversaries
- Regional Breakdown
- Breakdown of outside entities who will work with USCG
- Core capabilities
- Stakeholders
- Mission Outcomes (e.g., drug bust, safe sorties from port)

After analysis, the team selected “mission areas” and USCG “stakeholders” (see Figure 10) as the two best dimensions to consider current and future Coast Guard operations.

		Types of Operations			
		Maritime Security Operations & Defense Ops	Maritime Law Enforcement	Response (SAR, MER)	Prevention & MTS
KEY USCG/ Partner Players	People Recruit/Train/Retain				
	Infrastructure Bases/Investment				
	Operating Units Sea/Air				
	External Partners DHS, DoD Services, Allies, NGO's, OGA's				

Figure 10 – Strategic Segmentation

The Coast Guard “stakeholders” were grouped into four categories: people, infrastructure, operating units, and external partners. The people category included uniformed service, civilian, and contractors. That category focuses on how these cohorts are recruited, trained, and retained and how the service shapes the workforce over time. The team defined Infrastructure as bases, general infrastructure, headquarters, logistics, and other supporting units and general investments (computers, networks etc.). Operating units included sea and air units, and commensurate command and control systems for those units. We defined external partners in a broad sense, including

other departments and services of the U.S. government, foreign governments, public sector, and private sector partners of the Coast Guard.

To simplify the number of areas to be examined, the eleven statutory mission areas of the USCG were grouped into four programs aligned to Homeland Security act missions:

- Maritime Security Operations and Defense Readiness
- Maritime Law Enforcement
- Prevention and Maritime Transportation System
- Response

⁵ Paul Shoemaker. Profiting from Uncertainty, New York: Simon and Schuster, 2002, 77-78.

Maritime security operations and defense readiness consists of: defense readiness, maritime intercept, port operations and security of ports, waterways, and coastal seas; rotary wing intercept; combating terrorism; and maritime operational threat support. Maritime law enforcement encompasses migrant and drug interdiction, living marine resources, and other law enforcement areas. Prevention and maritime transportation system includes: port security, marine safety, marine environmental protection, navigation aids, and ice operations. The response mission area combines both search and rescue and marine environmental protection.

The resulting segmentation matrix contains 16 units and was further simplified after review by Red Team members into 8 groups of “like” areas. We simplified the numbers of areas to enable a richer discussion during the workshop (each team only would need to discuss the future implications for eight areas rather than sixteen areas). As an example of this simplification, the team considered the personnel requirements for recruitment and retention as similar across the four major Homeland Security act mission areas. In a similar fashion, operating units conducting maritime security and defense operations and maritime law enforcement require and employ similar capabilities and were considered as one grouping.

After the segmentation exercise, the team was left with eight major areas to examine during the workshop. The importance of the exercise is not in how the groupings occurred, but rather to ensure that workshop participants considered all types of Coast Operations and stakeholders as they were examining how the cyber alternative futures could impact the future of Coast Guard operations.

5.6 WORKSHOP AND DEVELOPMENT OF KSFs

With the Blue Cell and Red Cell testing complete and reviewed, the workshop design was finalized. Results and observations from the two cells were reviewed with Evergreen and incorporated into the final workshop design.

The primary purpose of the workshop was two-fold: finalize the alternative futures and develop Key Success Factors (KSFs) that enable superior Coast Guard performance in each of those futures as well as across the futures. The teams developed KSFs using a human centered design methodology to draw out diverse views and opinions and enable a broader understand of what the Coast Guard could emphasize to enable superior performance and resilience in the face of an uncertain future.

5.7 WORKSHOP OUTPUT AND CONCLUSIONS

The teams developed 37 Key Success Factors (see Appendix D for a list of all KSF’s and respective definitions). The teams discussed and verified that the KSFs were not ordinary activities that every Coast Guard or like organization must undertake, but rather high return activities likely to enable future Coast Guard success. VES collected team data on the weighting of each KSF and the standard deviation of scores. Additionally, each team

developed definitions of KSFs and combined like KSFs across alternative futures to enable understanding of which KSFs provided substantial value across multiple futures. VES algorithms calculated the weight of each KSF in each future and further refined weighting by including the impact by the weighting of a particular future. Importantly, many of the KSFs played a significant role in multiple alternative futures. A KSF that weighs highly in all four futures is a “no regret” activity and is worthy of leadership attention.

Figure 11 shows the highest scoring KSF’s.

Several observations are pertinent in the output of these thirteen highest-ranking KSFs. First, one must highlight that these KSFs tend to be highly ranked across multiple futures. Secondly, the KSFs cover multiple areas of emphasis including culture, organization, training, and investment.⁶



Figure 11 – Top Key Success Factors

as

cyber operational training program. VES participants believe a cyber operational training program would likely have even greater positive impact than denoted by its overall workshop derived score. Simply put, operational weaknesses and strengths would be uncovered by aggressive exercises and training resulting in significant feedback to mission teams and other cyber support personnel.

Some of the highest ranked KSF’s involve the creation of a Professional Cyber career field. In support of this, the workshop teams recommended adopting a flexible Human Resources (HR) system. Such a system would enable recruitment of more senior personnel with targeted skill sets and would enable such personnel to depart and reenter the service as required. Of note, workshop participants rated the flexible HR system higher than development of a professional cyber career field because of the additional salutary effects to a range of other USCG mission areas. Other linked KSFs include development of cyber mission teams for operational deployment or placement required and a robust operational

⁶ Of note, high tolerance for innovation and integrating new technologies requires a focus on culture within the U.S. Coast Guard. Changing culture often requires sustained leadership focus and is generally hard. The development of clear national and international cyber standards and norms is also a challenging long term activity.

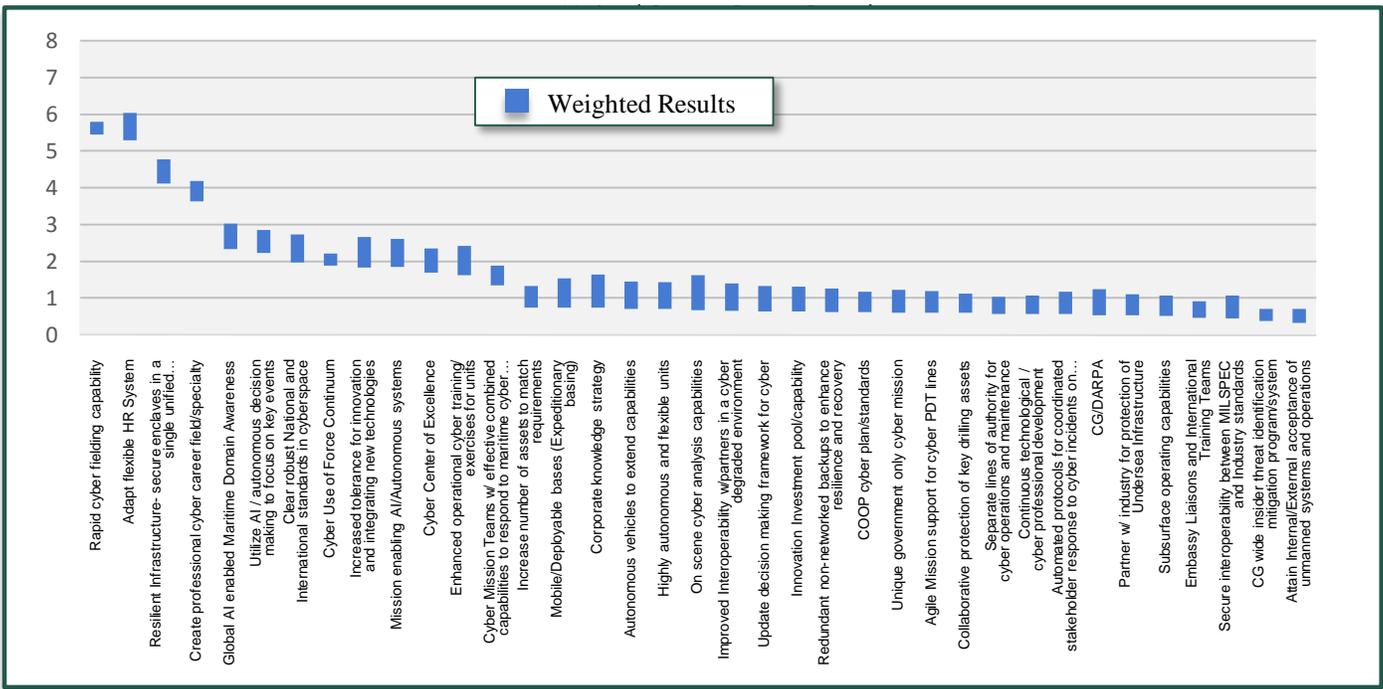


Figure 12 – Top KSFs Weighted by Futures

Figure 12 displays the results of VES algorithms weighting the different KSFs. No organization has unlimited management and the results of Figure 11 enabled the team to determine a natural breakpoint after KSF 13.

A key concern of the workshop teams was the security of the Maritime Transportation System. As a result of concern for this system and for other key infrastructure, the workshop participants rated development of resilient infrastructure with secure enclaves and non-networked redundancies highly. This concern also played a role in the recommendation to emphasize Artificial Intelligence (AI) and autonomous decision making to speed response to threatening cyber activities. Workshop participants also emphasized the importance of rapid cyber fielding to enable timely responsive of cyber capabilities. Teams recommended this rapid fielding not just to protect critical infrastructure, but also to enable appropriate protection of USCG operational units and to extend USCG response operations.

Several workshop teams recommended a Cyber Center of excellence to select and oversee requisite capabilities and training. Also of note, the idea of having a cyber element in the use of force continuum needs further review. The concept would enable the USCG to use cyber in support for activities that could result in use of force. For example, cyber could be used where appropriate to stop a drug running fast boat before more lethal methods are employed.

In many of the futures examined, the teams assessed a growing importance of Maritime Domain Awareness (MDA). Use of cyber, and big data analytics could potentially enable improved execution of this task with reduced use of expensive operational assets. Team members also emphasized the importance of AI linked with autonomous systems both to reduce use of USCG operational assets but also to provide support for other key mission areas such as Marine Environmental protection where UUVs and autonomous capabilities are likely to grow in importance.

VES then examined the links between KSFs in order to determine interdependencies. Highly- ranked KSFs that support lots of other KSFs but require little support themselves tend to be good early investments. We display the result in Figure 14 below. KSFs in the upper right support many and require little support; the upper right is heavily supported but also has many dependencies; bottom right quadrant requires a great deal of support but supports fewer KSFs. In short, an organization would consider a temporal investment strategy progressing clockwise from the upper left.

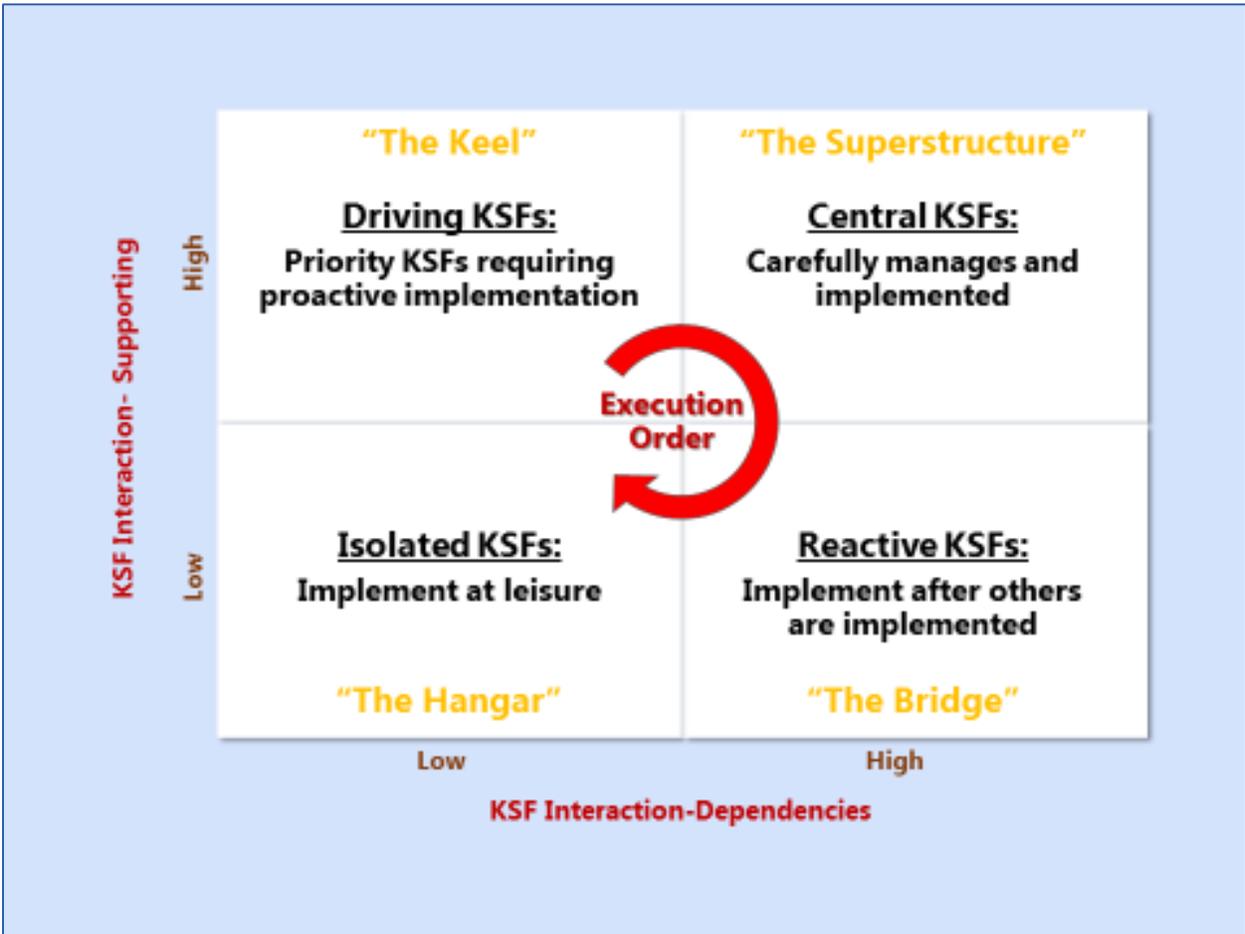


Figure 13 – KSF Dependencies and Their Implications for Implementation

Office of Emerging Policy / Evergreen
United States Coast Guard

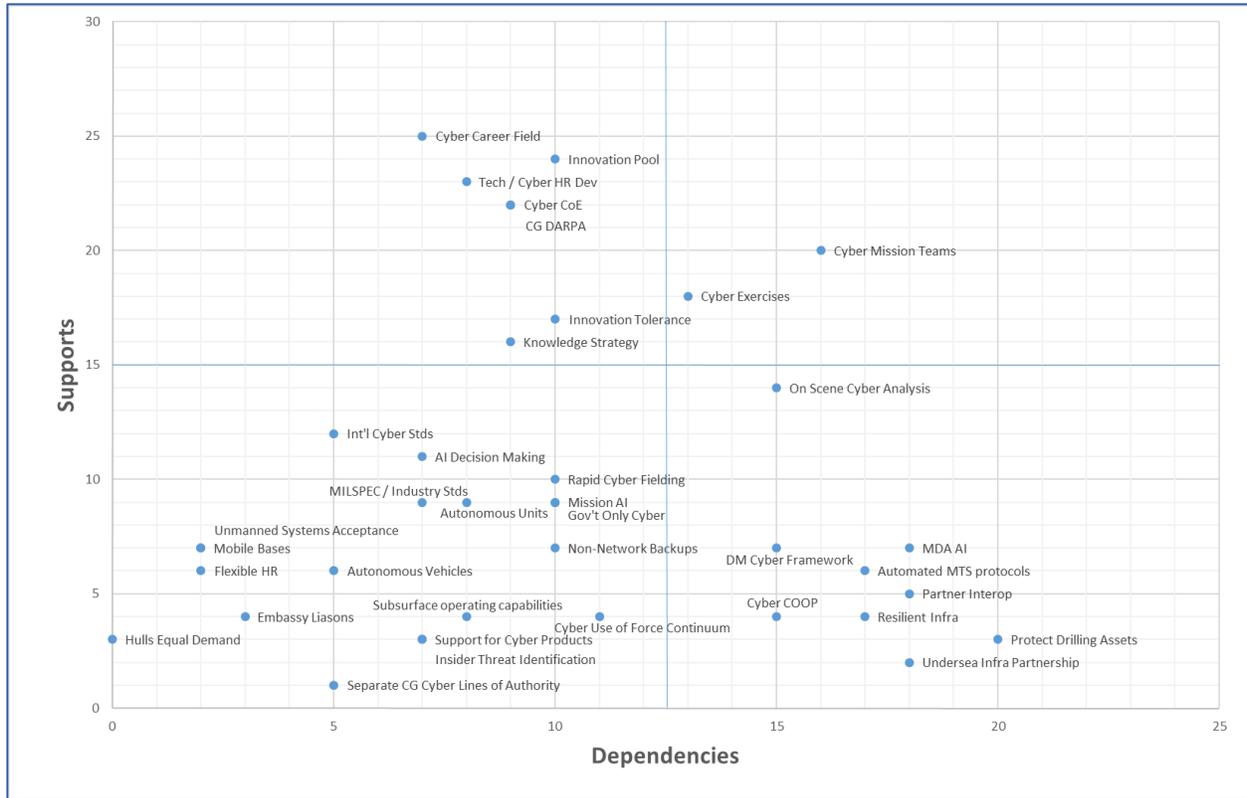


Figure 14 – KSF Dependencies

VES then compared desirable early areas of emphasis (i.e., KSFs) with the workshop’s recommendations of thirteen key KSFs. The result was seven KSFs recommended for early consideration or adoption (see Figure 15 below). Of these we recommend three of the ‘Driving’ KSFs for initial consideration. Also of note, workshop

participants placed a high emphasis on protection of the Maritime Transportation System (MTS). The “Resilient Infrastructure” KSF ranked highly as a result, but could require significant coordination with cyber professionals. However, we moved this KSF up temporally because of the importance placed on MTS by workshop participants.

KSF Interaction Takeaway

- ▶ **Highly ranked Driving KSF’s**
 - Create professional career field
 - Adaptable Flexible HR system
 - Tolerance for Innovation
 - Cyber Center of Excellence
- ▶ **Highly ranked Central KSF’s**
 - Enhanced operational training for cyber units
 - Cyber mission teams
- ▶ **Next group of KSF’s (Reactive)**
 - Resilient Infrastructure w/Enclaves
 - Recommend earlier adoption than Interaction survey would suggest

Recommended first steps

Figure 15: Recommended early actions

VES then reviewed the overall results to determine if the USCG should consider one or more lower ranked KSFs as a “bet”, even if only beneficial in one future. We felt that

the “innovation pool” concept is worthy of consideration for inclusion with the thirteen other highest ranked KSFs. In this concept, the USCG would consider pooling small amounts of R&D dollars with either private sector organizations or government organizations in support of software and other innovations that could have outsize impact on USCG missions. Organizations like In-Q-Tel and the newly created Defense Innovation Unit Experimental (DIUx) enable the intelligence community and the defense community to gain access to cutting edge private sector ideas while leveraging pooled resources.

6 COMPARISON OF RESULTS WITH COAST GUARD STRATEGIC DOCUMENTS

VES conducted a review of workshop output and conclusions and compared it with the recently released (June 2015) USCG Cyber strategy. We found the KSFs were entirely consistent and nested within the three specific strategic priorities noted by the Coast Guard (Defending Cyberspace, Enabling Operations, and Protecting Infrastructure). We also compared the KSFs to the seven long term support factors developed by the Coast Guard. 32 of the 37 KSFs linked to one of the seven support factors (see table below). Five additional KSFs touched on additional capabilities that cyber could enable but also touched on broader USCG capabilities. In short, the overall workshop results fit extremely well with developed and articulated U.S. Coast Guard Cyber strategy.

USCG Cyber Strategy Support Factor	Workshop Key Success Factors
Recognition of cyber space as an operational domain	<ul style="list-style-type: none"> • Cyber use of force continuum • Update decision making framework for cyber
Developing cyber guidance and defining mission space	<ul style="list-style-type: none"> • Clear robust National and International standards in cyber space • CG wide insider threat identification mitigation program • Unique government only cyber mission • Separate lines of authority for cyber operations and maintenance
Leveraging partnerships to build knowledge, resource capacity, and an understanding of MTS cyber vulnerabilities	<ul style="list-style-type: none"> • Partner with industry for protection of Undersea infrastructure • Collaborative protection of key drilling assets • Improved interoperability with partners in cyber degraded environment • Secure interoperability between MILSPEC and Industry standards • Embassy liaisons and International training teams • Automated protocols for coordinated stakeholder response to cyber incidents on MTS
Sharing of real-time information	<ul style="list-style-type: none"> • Mission enabling AI/autonomous systems • Global AI enabled Maritime Domain Awareness • Utilize AI/autonomous decision making to focus on key events • On scene cyber analysis capabilities
Organizing for success	<ul style="list-style-type: none"> • Cyber mission teams with effective combined capabilities to respond to maritime cyber threats • Corporate knowledge strategy • COOP cyber plan/standards • Increased tolerance for innovation and integrating new technologies

Office of Emerging Policy / Evergreen
United States Coast Guard

Building a well-trained cyber workforce	<ul style="list-style-type: none"> • Adapt flexible HR System • Create professional cyber career field/specialty • Continuous technological/cyber professional development • Enhanced operational cyber training/exercises for units
Making thoughtful future cyber investments	<ul style="list-style-type: none"> • Innovation investment pool/capability • CG/DARPA • Cyber center of excellence • Redundant non-networked backups to enhance resilience and recovery • Agile mission support for cyber product lines • Rapid cyber fielding • Highly autonomous and flexible units • Resilient infrastructure – secure enclaves in a single unified infrastructure with non-networked redundancies

VES also compared workshop results with the Evergreen IV Strategic Needs and other recently released strategy documents (USCG’s Arctic Strategy, USCG Living Marine Resources Ocean Guardian, 2014 USCG’s Western Hemisphere Strategy). The workshop results synchronized well across the board with a variety of key strategic needs articulated by Evergreen. For example, Evergreen discusses the need for a fully integrated Maritime Domain Awareness (MDA) capability; workshop participants echoed this with a KSF recommending examination of AI-enabled MDA. Evergreen specifically recognized the importance of Talent Management and Individual Technology Specialization; two of the highest-ranked workshop KSFs involve a more flexible and adaptable HR system and a Professional Cyber Career field. Evergreen highlighted the importance of a Secure C4IT system and specifically noted the importance of “preventing unauthorized actors from infiltrating automated systems with the Maritime Transportation System.” The generated KSFs provide several key concepts that are strongly aligned and supportive of this Evergreen recommendation, and independently determined. Other technical and culture change KSFs aligned with needs outlined in the other USCG strategic documents as enablers.

7 CONCLUSIONS

Evergreen/VES analyzed a variety of plausible cyber futures and the potential impact of those futures on the Coast Guard. The team assessed the potential impact of these cyber futures as significant. We caution that no one cannot predict the future. Indeed, the methodology presented here is designed to “bound” the future and enable an organization to “future proof” strategy. However, participants noted with concern that in several of the futures the pace of technology would provide many challenges (and opportunities) to organizations such as the Coast Guard. As a result, workshop participants proposed several significant cultural, organizational, training, and investment areas of emphasis which should enable the Coast Guard to continue to perform its critical missions despite these uncertainties. The team recommended seven of these areas for early emphasis and consideration within existing USCG assessment processes.

APPENDIX A: LIST OF PEOPLE INTERVIEWED FOR BACKGROUND RESEARCH

Name	Title	Organization
RADM Marshall Lytle III	Assistant Commandant	Command, Control, Communications, Computers and Information Technology (C4&IT)
CAPT Gregory Czerwonka	Chief	USCG Detachment, US Cyber Command
CAPT Michael Dickey	Deputy Commander	CG Cyber Command
CAPT John Felker (Ret)	Director	National Cybersecurity and Communications Integration Center
CDR Paul Brooks	Engineering Officer	USCG Air Station Cape Cod
LtCol David Halla	Director of Operations	Electricity Information Sharing & Analysis Center (E-ISAC)
CDR Eugene McGuinness	Engineering Officer	Air Station Barbers Point
CDR Thomas Olenchock	Chief	USCG Future Force Division
CDR Peter Van Ness	EA to CG-6	Cyber Ninja TRANSCOM
CDR Nicholas Wong	Chief	Domestic Ports Division (CG-FAC-1)
LCDR Frank Nolan	Legal	Office of Claims and Litigation (CG-0945)
LCDR Sean Plankey	EA to CG-7	Deputy for Operations Policy and Capabilities (DCO-Acting)
Mr. Dave Anthony	Writer, Director, Producer	Call of Duty: Black Ops (2010) Call of Duty: Black Ops II (2012) Call of the Dead (2011)
Mr. Jeff Garzik	CEO & Founder	Bloq.com
Mr. Earle Kirkley	Vice President of Threat Intelligence	Uphold

APPENDIX B: RED CELL AND BLUE CELL ATTENDEES

Blue Cell Attendees:

Charnon, Steven J LCDR
Codd, John B LCDR
Ford, Zachary R LCDR
Jojola, Jennifer M LCDR

King, Richard L ITCM
Nolan, Frank G LCDR
Russell, Anthony L CDR
Smith, Jeanine CIV

Smith, Michael E CIV
Theel, Jonathan D CDR
VanNess, Peter R CDR

VES facilitators: Mike Poirier, Bill Nieuwsma, Brian Stites, Judy Nieuwsma

Red Cell Attendees:

Charnon, Steven J LCDR
Doucette, Eric CAPT
Ford, Zachary R LCDR
Howell, Andy CDR

Kennedy, Maggie LCDR
Lewis, Ed MKCM
Moran, Jim CDR
Plankey, Sean LCDR

Smith, Jeannine CIV
Smith, Michael CIV
Toves, Scott
Zinn, Matthew

VES facilitators: Mike Poirier, Bill Nieuwsma, Brian Stites, Michael Good, Judy Nieuwsma

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 scarce 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

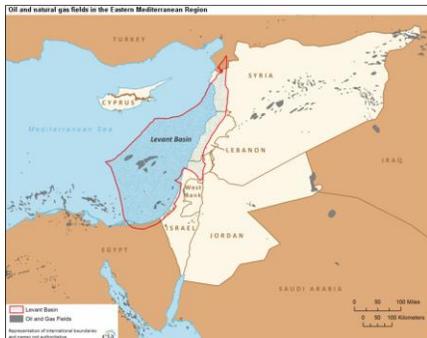
serve government interests and missions. The Coast Guard is challenged to know the global “order of battle” and the intentions of vessels wherever they are encountered. Due to the environment of high cooperation among Western allies, more individual nations and regional cooperatives are requesting USCG 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.

Office of Emerging Policy / Evergreen
United States Coast Guard

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

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

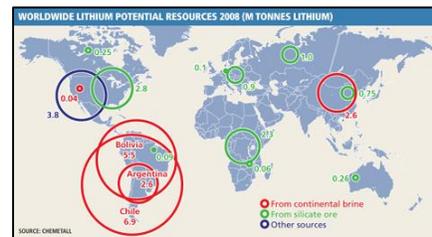


potential for conflict in Asia and the Arctic, increased defense and homeland security spending with resources provided by the post 2022 US recovery. The Coast Guard has significant additional resources that are focused on maritime critical infrastructure protection and maritime security. Continual friction 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 borders, 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.

Office of Emerging Policy / Evergreen
United States Coast Guard

	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

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 forth 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% budget 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.

Office of Emerging Policy / Evergreen
United States Coast Guard

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.

Office of Emerging Policy / Evergreen
United States Coast Guard

	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

Future D – Hedgehog

THE SETTING

2025: What a difference a few short years makes. The death of Vladimir Putin in a freak skiing accident in 2017 resulted in a change of tone to Western and Russian relations. The negotiated resolution of the Syrian crisis that year reduced the friction between NATO and Russia. But the 2019 economic downturn – light in the West but significant throughout emerging market economies - played a key factor in the Second Era of Detente. Concerned over losing access to US and European markets, China dramatically scaled back its public economic espionage and theft of intellectual property. Not all is peaceful: While Iran has increased its economic cooperation with the West, the chaos of the 2021 “Green” revolution in Saudi Arabia resulted in substantial damage to oil producing facilities and a substantial increase in the price of oil – mitigating the economic downturn in some developing energy-producing countries.

2025 KEY DRIVERS:

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

On the cyber front, without an external threat to motivate them and with austerity policies attempting to shuffle entitlement spending, governments do little to cooperate with the private sector. The private sector continues to create consumer electronics that far exceeds military grade systems, leading to robust anonymity and disruptive cyber capability. Cybersecurity starts to trend dominant thanks to block chain technologies and other advancements in 2020 through development of Intel’s new chip technology. This is a world where the private sector has to work hard to protect itself – but it has the means. The general availability of highly technical skilled personnel and the healthy but not frothy development of the Internet of Things (IoT) results in the private sector maintaining reasonable cybersecurity capabilities. The Internet remains a playground for small time criminals and transnational gangs along with hyper-empowered individuals that transcend national sovereignty boundaries. But generally, large transnational criminal organizations find greater opportunity elsewhere. The lack of political fallout from disruptions and criminal activity results in government reluctance to employ retaliation. Under this relatively benign environment and impacted by significant social spending on aging Baby Boomers, the Coast Guard and other federal agencies are strapped for funds. Maintenance and upgrades to existing platforms are delayed and software often remains on government systems after sunseting in the commercial world. There remains a level of discord in US society and government is focused on the “insider” threat.



BACKGROUND

With the warming of relations between NATO and Russia and the Chinese conformance to international ethical activities in cyberspace, governments have tended to breathe a general sigh of relief that the prospects of a hot “cyber” war have substantially diminished. Largely driven by high-tech job and income inequities, the 2019 global economic downturn was acute in developing countries due to the expansion of robotics into the textile industry combined with increasing environmental resource stresses. In China, Southeast Asia, India, and South America, low-skilled factory workers are widely being replaced that causes mass migrations by an increasingly disenfranchised labor class.

Affluent countries and regions within countries are hailing increased industrial and informational productivity and a corresponding increase in high-tech jobs; countries like Germany, Canada and the US are under global pressure to accept multitudes of unskilled immigrants. The 2021 coordinated attacks on oil infrastructure across Saudi Arabia, Turkey and Ukraine (reportedly by terrorists originating from immigrant sources) have prompted those governments to delay accepting refugees, citing increased border security requirements. Over 43 boats ferrying refugees from Albania to the boot of Italy and the extensive media coverage showing hundreds of floating bodies have motivated the Italian government to request significant assistance by the USCG to train an additional 35 maritime coastal security units throughout the Mediterranean. Greece, Cyprus and Turkey have also requested USCG assistance to train several hundred personnel each for maritime border security and search and rescue (SAR). While some of these refugees have advanced degrees, the anxiety over the “insider threat” delays job placement and citizenship for almost all immigrants to several years. Many immigrants are exploited by criminal organizations, especially those with advanced computer programming, engineering and science backgrounds. Frustrated and disenfranchised, high-tech skilled refugees provide a potent workforce for criminal organizations interested in capitalizing on Internet scams, electronic financial theft, and illicit transportation of weapons, drugs and human trafficking.



Embittered by the obstructions and endless bureaucracy, private industry continues to develop and unevenly adopt technologies that focus on cyber resiliency, system hardening and robust encryption. The promise of quantum computing failed to materialize, but materials nanotechnology has enabled Intel to continue Moore’s Law. Each year, new technologies are exhibited at the Consumer Electronics Show (CES) that surpass MilSpec systems. Government and Law Enforcement overtures to limit advanced encryption have largely been dismissed by industry in favor of “consumer privacy” and the explosion in the IoT market. New technologies within the consumer market indicate that security is trending upward compared to the number of extensive hacks into major companies.

However, government systems continue to lag consumer electronics and network technology by vast margins. Some in Congress have suggested immediate action is required, which was one of the major election issues in 2019. An oft-used example by Congress, Microsoft started selling Windows 14.2 in 2018 while the USG started its annual computer refresh the same year with Windows 8.1, which Microsoft discontinued support in 2018 (Windows 8.1 debuted in 2012). The widespread USG delay in computer

and network updates has severely curtailed the adoption of advanced technologies such as unmanned vehicles, mobile sensors, and multi-source data fusion by USG agencies. The FBI has been the most vocal USG agency to publically decry the inability of the USG Departments to develop an agile, common security framework and devise methods to more easily work with private industry.

Since 2021, domestic issues have dominated the U.S. political landscape and drawn attention away from international and maritime security topics. In conjunction with Baby Boomers increasingly stressing the healthcare industry and social welfare programs, the Social Security Fund is being exhausted faster than previous negative forecasts. To provide immediate funding, the DoD and DHS are the two departments most immediately impacted with austerity measures. As a result, the USCG budgets beginning in 2022, were reduced by 10% per year through 2025, even in the face of increasing domestic and international requests for assistance.

Office of Emerging Policy / Evergreen
United States Coast Guard

	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

APPENDIX D: KEY SUCCESS FACTORS AND DEFINITIONS

KSF	Definition
Rapid Cyber Fielding	<p>Augment existing acquisitions process; for greater agility to meet timely software and hardware needs.</p> <p>Insure procurements are interoperable with current systems and upgradeable.</p>
Adapt Flexible HR System	<p>A workforce that integrated active duty, civilian and other cyber professionals, allowing flexible entry/exit, and meets defined competencies. Streamline hiring practices using non-traditional means of acquiring and retaining cyber professionals, through DCO, reserved, contractor and temporary options.</p>
Resilient Infrastructure-secure enclaves in a single unified infrastructure with non-networked redundancies	<p>Provide defensive capability for assured data integrity within core USCG systems such as the MTS (Assured Data Integrity)</p> <p>Creation of hardened protected nodes that can also work offline.</p>
Create Professional Cyber Career Field/ Specialty	<p>Establish a cyber career identity; define a portable civilian, enlisted and officer career path with dedicated training programs, qualifications and structures aligned with industry standards and credentials.</p>
Global AI Enabled Maritime Domain Awareness	<p>Aggregated information to create a comprehensive COP (Common Operating Picture) for the maritime domain. Utilize segmented, real-time data to influence mission operations with enhanced decision making.</p>
Utilize AI/Autonomous Decision-Making to Focus on Key Events	<p>Create AI enhanced decision-making systems that augment and support all levels of strategic & tactical decisions. AI enabled mission execution and planning; utilize big data mining, crowd sourcing and algorithm based data-driven decision making tools to filter out “white noise” and summarize information for human consumption for informed decision making.</p>
Clear Robust National and International Standards in Cyberspace	<p>Clarify existing cyber legal authorities and seek new authorities where necessary to ensure a robust international and domestic legal architecture that establishes the USCG as the preeminent authority in the maritime related cyber domain. This includes establishing international cyber related norms for sovereign nations to prevent and respond to maritime incidences; and</p>

Office of Emerging Policy / Evergreen
United States Coast Guard

	establishing norms for use of cyber force against non-state actors implemented through domestic US law and regulations.
Cyber Use of Force Continuum	Clearly define authorities and jurisdictions to conduct offensive and defensive cyber operations against non-state actors. Recognition of cyber as a tool on the force continuum. Example: use of cyber tools to stop UAS drug running.
Increased Tolerance for Innovation and Integrating New Technologies	Increased risk tolerance for innovation and integrating new technologies (automation and outsourcing of systems), with expectation of efficiency gains. Change management culture in regards to decision-making unencumbered by the status quo.
Mission Enabling AI / Autonomous Systems	Adoption of emergent AI technologies and resilient systems (including UAV's, UUV's) to help perform missions and improve decision-making. Utilize all source capabilities including big data/social media to allocate SAR- ensure understanding of actual SAR mission vs diversion; improve real time asset allocation. Incorporate unmanned systems where practical to reduce resource requirements and ensure operational efficiency.
Cyber Center of Excellence	Hub for cooperation, collaboration and communication between CG/DHS/interagency/academia/NGO's/allies. National and international industry recognized cyber expertise focused on technologies, authorities and enforcement; building partnerships; directing innovation investments.
Enhanced Operational Cyber Training/Exercises for Units	Incorporate cyber into exercise plans, policies, and procedures. Create cyber-com deployed training teams to educate, assist, evaluate, and inspect cyber readiness.
Cyber Mission Teams	Codified Coast Guard cyber mission teams that leverage OGA/industry cyber capabilities to respond to maritime cyber threats, and inspect, assure and protect networks and network functions both at sea and ashore.
Increased Number of Assets (Hulls) to Match Requirements	Adequately resource CG fleet for effective global presence.
Mobile/ Deployable Bases (expeditionary basing)	USCG provides mobile/deployable base capability to support expeditionary basing starting with the Arctic area and the Gulf of Mexico.

Office of Emerging Policy / Evergreen
United States Coast Guard

Corporate Knowledge Strategy	Define what knowledge the CG wants to own versus procure.
Autonomous Vehicles to Extend Capabilities	Flexible multi-use assets, small autonomous sensors for air/underwater to augment manned vehicles and improve mission execution and range. Leverage technology to mitigate risk.
Highly Autonomous & Flexible Units	Self-sustaining, multi-mission units capable of meeting emergent operations and operating in information-degraded environments.
On-Scene Cyber Analysis Capability	Analysis capability not dependent on long pipes/bandwidth limits to reach back and includes DOMEX (real-time).
Improved Interoperability with Partners in a Cyber Degraded Environment	Ability to conduct Coast guard operations with partners in a cyber-degraded environment. Includes communications and navigation, development of procedures, and appropriate training and exercises.
Updating Decision Making Framework for Cyber	Create automated threat identification and response options when encountering cyber activity.
Innovation Investment Pool/Capability	Consider use of In-Q-Tel and/or seed funding to look for cutting edge cyber tools, R&D and collaboration with industry.
Redundant Non-Networked Backups to Enhance Resilience and Recovery	No overdependence on cyber systems; maintain non-cyber capabilities. Enhanced enterprise resiliency through human/analog/disaggregated elements to ensure rapid recovery following significant cyber events.
COOP Cyber Plan/Standards	Add cyber resiliency into COOP plans and standards for USCG and into private external partners' business continuity plans.
Unique Government Only Cyber Missions	Build on unique CG authorities to carve niche from other government/NGO organizations to define specialized missions focused on maritime cyber threats.
Agile Mission Support for Cyber Product Lives	Fully fund product upgrades and maintain product utility and security rather than defer important upgrades due to cost.

Office of Emerging Policy / Evergreen
United States Coast Guard

Collaborative Protection of Key Drilling Assets	Collaborative determination of what key nodes need to be protected including drilling/oil infrastructure industry, insurance industry and USCG.
Separate Lines of Authority for Cyber Ops & Maintenance	Eliminate/reduce conflict of interest created by combined authorities; separate authority for C4IT maintenance and acquisition from cyber operations to insure operations are mission-focused.
Continuous Technological/Cyber Professional Development	Professional development, starting at accession and throughout career, focused on increasing general and specialized cyber knowledge throughout the workforce.
Automated Protocols for Coordinated Stakeholder Response to Cyber Incidents on MTS	The speed of cyber drives the need for AI response to cyber events; pre-determined responses, evolution of MOTR process and accepting risks to gain efficiencies.
CG/DARPA	Create a venture capital Quasi-government (DARPA–esqe) department for technological exploration of emerging technologies.
Partner with Industry for Protection of Undersea Infrastructure	Review and consider expanding Coast Guard responsibilities relating to undersea infrastructure and partner with industry to ensure that protection.
Subsurface Operation Capability	Create subsurface operation capable of protecting critical infrastructure (undersea cables) and detecting, determining and defeating submerged threats.
Embassy Liaisons and International Training Teams	Leverage CG’s non-threatening posture to enhance our current foreign footprint to improve international cyber environment through liaisons and training.
Secure Interoperability Between MILSPEC and Industry Standards	Prevent MILSPEC standards from preventing the application of new technologies and industry standards.
Insider Threat Identification and Mitigation Program and System	Develop ability to identify and address insider threats within the government (Snowden effect).
Attain Internal and External Acceptance of Unmanned Systems and Operations	Drive cultural resistance to adapting unmanned vehicle planning, procurement, and use in addition to traditional manned systems.

Key Success Factor (KSF) Commonality

Brief: Following the 'Evergreen Cyber Futures' workshop in January 2016, Evergreen program personnel conducted three additional workshops. These mini workshops were attended by Coast Guard Academy Cadets, members of the 2016 Mid-Grade Officer Career Transition Course cohort, and members of the May 2016 Senior Enlisted Leadership Course. The mini workshops were approximately 1.5 – 2 hours in duration and used Human Centered Design methodology to elicit ideas and identify KSFs. The raw data was analyzed by DCO-X personnel; the results and conclusions are included below.

Common KSFs (MOCTC):

The Coast Guard must...

- (1) Compete for changing global workforce
- (2) Strengthen international cooperation with other countries
- (3) Leverage partnerships to move international cyber legislation forward
- (4) Create strong partnerships
- (5) Develop, recruit, and retain tech savvy workforce
- (6) Build and strengthen interagency agreements

Common KSFs (SELC):

The Coast Guard must...

- (1) Lobby for additional funding
- (2) Develop, recruit, and train a technologically advanced workforce
- (3) Stay ahead of current technologies

Common KSFs (USCGA Cadets):

The Coast Guard must...

- (1) Increase funding in cyber operations
- (2) Recruit, retain, and train a cyber workforce
- (3) Use latest technologies
- (4) Partner with private sector
- (5) Increase domestic and international partnerships

Conclusions: The two-day 'Evergreen Cyber Futures' workshop identified 13 KSFs that should be pursued in order to prepare the Coast Guard for an uncertain cyber future. These 13 KSFs were the product of significantly more discussion and analysis unavailable to the mini workshops. In spite of this, there were some striking similarities that validated some of the conclusions of the longer 'Evergreen Cyber Futures' workshop.

Rapid Cyber Fielding was the top scoring KSF. The groups defined this as the need for the Coast Guard to rapidly integrate emerging cyber technologies in all aspects of the Coast Guard. While they realized the barriers to rapid integration, they felt that the excessive bureaucracy could be modified and streamlined to make the Coast Guard more competitive in the cyber domain and place the Service on equal footing with potential adversaries. All three mini workshops developed similar KSFs with a focus on new and emerging technologies. Specifically, the SELC and USCG workshops identified the need for the Coast Guard to **stay ahead of current technologies** and **use latest technologies** respectively. While not scientific, it is compelling that a group of senior enlisted and mid-grade officers identified similar themes.

Two more 'top 5' KSFs were: **adaptable flexible HR system** and **create professional cyber career field**. Both of these KSFs deal specifically with ensuring the Coast Guard is not only prepared to deal with the emerging cyber domain, but agile and adaptable enough to adjust to future changes. All three mini workshop groups identified very similar themes. MOCTC identified the need to **develop, recruit, and retain a tech savvy workforce**. The SELC cohort identified the need to **develop, recruit, and train a technologically advanced workforce**. Finally, the Cadets identified the need to **recruit, retain, and train a cyber workforce**. This was a recurring theme throughout all discussions. The Coast Guard has specialized aspects of its workforce (e.g. aviators, marine inspectors, MSSTs) to better prosecute missions and ensure success. Much of this specialization requires years of training at a considerable cost. The overarching theme for all workshops was that the cyber career field should be treated in a similar fashion. Cyber warriors must continually be at the top of their game and understand the ever-changing environment. This will no doubt require training on par with traditional career specialization and possibly require the Coast Guard to rethink legacy career paths and compensation.

Finally, **international partnerships** and **clear/robust national/international cyberspace standards** were identified as two critical KSFs by the 'Evergreen Cyber Futures' workshop. The MOCTC group identified the need to **strengthen international cooperation with other countries** and **leverage partnerships to move international cyber legislation forward**. The Cadets identified the need to **partner with the private sector** and **increase domestic and international partnerships**. Once again, a small sample size of current and future Coast Guard officers identified similar needs to the group of previously assembled cyber experts.

The purpose of the follow-on mini workshops was to sample various groups within the Coast Guard and validate the findings of the larger workshop. Similar methodologies were used throughout the workshop process. While unscientific, the correlation between the 4 different workshops makes a compelling case for the Coast Guard to pursue and implement many of the KSFs identified in the 'Evergreen Cyber Futures' workshop.