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 sunsetting 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.

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