November 19, 2025

# White Paper

GEOIntelligence

Great Power Competition refers to strategic rivalry between dominant nations – typically military and economic superpowers – all vying for global influence, security, and technological superiority. Most recognize that China, Russia, and the United States as today’s Great Powers. The players in this competition seek leverage in free market opportunities, governance, and regulatory gaps, to exercise their willingness and ability to exert power and gain advantage across all elements of power (that is, Diplomacy, Information, Military, and Economics, or DIME). Great Power Competition occurs within most geographic regions, yet at the same time, globally.

Further, this competition spans all domains – land, sea, air, space, and cyberspace – where each is continuously advancing in capabilities to attempt to dominate or control in order to achieve desired objectives. These domains are the competitive maneuver spaces where nations conduct physical and virtual operations, commerce, and communications. Ideally, such activities peacefully occur relative to commonly shared rules of law, governance, and regulations to which all participants ascribe. However, there is wide variance on the spectrum of shared norms and values relative to domains, and therein lies geostrategic competition and friction between state and non-state actors.

All five domains are in constant play in the renewed Great Power Competition, offering opportunities yet also risks. This report focuses on cyberspace – the most recent of the domains and one that serves as an exemplar of both prospects and challenges. By definition, cyberspace comprises interconnected networks, infrastructure, software, and human capabilities that enable the creation, storage, transmission, and use of digital information. It functions both as a military battlespace and as the backbone of civilian commerce, communications, and governance. It is essential for people and economies to thrive globally, particularly through cyber and information security.

What is very interesting when circling back to the five previously mentioned domains, cyber functions as a critical enabling domain that supports and integrates operations across the other four domains, though at the same time, cyber remains dependent on their physical and logistical capabilities. The decisive subsets of this domain are data, Artificial Intelligence (AI), and quantum computing. Data fuels intelligence, decision-making, and innovation across all domains, while AI and quantum computing transform that data into actionable insight, accelerating decision cycles and enabling autonomous capabilities.

Yet there are risks – to be sure, all are aware of the importance of “cybersecurity” either through proactiveness or from the school of hard-knocks – more likely both. Cybersecurity, of course, is the practice of protecting computer systems, networks, data, and connected devices used for access from digital attacks. Information security is the practice of protecting digitized information by safeguarding the confidentiality, integrity, and availability of data through multi-layer security controls.

## Cyber Domain Ecosystem:

Cyber Domain Ecosystem Infrastructure: The primary infrastructure necessary for the cyber domain to function includes power through global electricity grids, global communication networks, data centers, and cloud architecture. Global electricity grids fuel the cyber infrastructure to compute, store, and transmit data and information across the cyber ecosystem (for more on energy, please see Bancroft GEOIntelligence White Paper on Energy and its Economic Implications). National and international grid networks provide electricity generation, storage, transmission, and delivery of energy. The supply chain for power sources and their infrastructure components requires international market participation and efficient use of natural resources, including renewables.

Further, global communication networks are necessary to transmit data, information, and financial transactions worldwide. These communication systems use physical assets across all domains (again, sea, land, air, space, and cyberspace). For example, land assets include networking facilities, fiber and cable lines, wireless communication towers, and network points of presence. This complex network links land assets to undersea international communication cables, as well as the domains of air and space through Low Earth Orbiting (LEO) satellites and the wireless spectrum ranging from unlicensed Wi-Fi networks to licensed public wireless networks to classified military spectrum bands. The performance of communication networks is based on coverage, capacity, interoperability, and security of the communications, which are massive in scope and have physical and logical disruption threats. These communications networks ultimately deliver information to end users via voice and text messages, data files, wire transfers, live streaming, and classified national security intelligence. Communication networks are essential for the cyber ecosystem and can be a point of failure.

Hardware, Data Management, and Advanced Electronics: Data centers house information technology servers and have existed since the beginning of the digital age. The cyber domain relies on data centers to compute and store massive amounts of data in both physical and cloud architectures, which in turn enables users to access structured and unstructured data. As advanced technologies evolve, the Electric Power Research Institute projects that by 2030, almost 10% of U.S. electricity could be used by data centers alone. Structured data ranges from entertainment networks to information in enterprise-grade computer systems requiring security credentials for access. Unstructured data can be accessed either with security credentials if confidential or on the internet if publicly available. As technology advances, dependency on data centers and cloud architecture, allowing remote access, will increase. Data centers require real estate with available electrical power and communication network access. They also require infrastructure redundancy and physical security assets. The data center market has grown substantially, driven by demand for advanced technologies with elements such as servers to compute at increasing speeds, and these will depend on continued microchip innovation.

Microchips are comprised of transistors made up of semiconductors, and they provide technological components for a wide spectrum of assets ranging from the most advanced computers, such as data center servers, to personal computers, cell phones, and the Internet of Things (IoT), which includes numerous monitoring and transacting devices.

Semiconductors are a base component for microchips included in electronic devices. The supply chain for them is a key element upon which the infrastructure and capabilities of the cyber domain are dependent. According to the Center for Strategic and International Studies, the starting point for the semiconductor value chain is the design phase that creates semiconductor blueprints for power, performance, and cost. The Intellectual Property (IP) associated with these designs is led by the U.S., Europe, and Japan, facilitating the architecture for the future of technological advancements.

Semiconductor manufacturing and fabrication is a complex process that transforms raw materials into microchips at the nanoscale and requires specialized tools, chemicals, and gases used with software and IP processes for control. These activities are primarily concentrated in Taiwan and South Korea and have been highlighted as a national security risk (for threats from China in this regard, please see Bancroft GEOIntelligence Executive Summary on the South China Sea Implications and Economic Considerations and Bancroft GEOIntelligence Executive Summary on Taiwan Security Implications and Economic Considerations). The U.S. Chips Act is a starting point for derisking investments across the United States and the globe to diversify semiconductor manufacturing.

Final assembly of the chips into electronic devices, including testing and packaging, is global with a significant concentration in China. Rare earth minerals such as various forms of silicon, copper, and others today are primarily sourced in China, the U.S., and the Global South. The complexity, interconnectivity, and geographic dependencies within the semiconductor supply chain present a significant potential for disruption and fuel strategic positioning among global powers.

Software is the link between physical infrastructure and logical elements of the cyber domain, bringing hardware components and data together to provide information and other outputs to support mankind. Software ranges from operating system management and cyber access security to end-user analysis, transaction, and consumption of information and entertainment. The levels of software utilization in any one transaction are numerous, including infrastructure, access, computing, applications, and output, with different levels of scope and authentication. Cyber governance and security have become a critical mission element of the cyber domain. Communication, enterprise, and personal networks, as well as energy grids, are attacked every day, and every hour (365/24/7) by nefarious actors attempting to compromise data, disrupt operations, and commit cybercrimes. How data is used and secured is a primary concern for every country, company board of directors, senior leadership team, and individual.

## Security/Risk:

The magnitude and impact of cyber threats cannot be overstated. On one bookend, threats include the potential of widespread catastrophic cyberattacks to damage or disrupt national or regional infrastructure (for more on strategic attacks, see Bancroft GEOIntelligence White Paper on Escalation Dynamics in Great Power Competition Risks, Redlines and Ramifications). On the other hand, threats can involve cybercrime. The WEF asserts, “if cybercrime were a country, it would rank as the third-biggest economy globally, trailing only the US and China.” Global cybercrime costs are projected to reach $10.5 trillion annually by the end of 2025, and in 2024 The Chief Risk Officers Outlook “ranked cyber risk among the top three threats severely affecting organizations.”

Facing these threats requires understanding both their nature and character to operate at the speed, if not ahead, of the cyber domain challenges, requiring strategic thought, vision, engagement, and action with increasingly public and private collaboration. Whether an enterprise is military or commercial, the threat of cyber continues to increase. Although the character of warfighting domains continues to accelerate, the nature of exercising power comes down to following basic risk mitigation practices and protocols to:

- Understand domain composition, such as policies, strategic objectives, and operations
- Know and anticipate threat actor capabilities, intentions, and capacities
- Possess deterrence capacity and resilience capabilities to mitigate threat activities
- Understand the many attack vectors in the cyber domain (supply chain, malware, phishing, hardware/software, networks, denial of service, insider threat, and so on)
- Educate the entire team that touches your systems and networks – every member must be a cyber-defender, as it can take only one weak link to allow adversary entry into your corporation
- Maneuver cross-over activities, blurring lines between cybercrime and attacks by state-sponsored actors and proxy criminal networks or quasi-legitimate business entities
- As appropriate, notify government agencies of suspected cyberattacks and crimes, such as the FBI's Internet Crime Complaint Center (IC3), the Cybersecurity and Infrastructure Security Agency (CISA), etc.

## Cybercrime and Warfare Strategic Frameworks – Public and Private Sector Partners:

In the U.S. Government, the strategy for cybersecurity prioritizes defensive activities. The Department of Defense (DoD) focuses on defending its information network, building resilience, and supporting current operations while defending against and mitigating the impact of cyberattacks. In some cases, there are also authorities granting the DoD and other departments within the Department of Justice and the Department of Homeland Security offensive cyber capabilities.

In the corporate world, cybersecurity interests are not much different. Enterprises leverage cyber to run their businesses while protecting their workforce, market systems, and data. Most corporate strategies take a similar approach to the government. More than just investing in the latest anti-virus software, their strategies include threat and risk assessment investments to understand threats (intelligence), learn about emerging trends, and incorporate new capabilities (proprietary and third party) for protecting networks, as well as developing workforce and market resiliency against attacks.

The biggest challenges to the private sector are the cost, speed, and scale of attacks. The World Economic Forum (WEF) reports that smaller companies are unable to afford the investments larger corporations or governments make to prevent and protect against cyberattacks. They must outsource needed capabilities and assume higher risks while trusting deterrence, detection, and resiliency capabilities, which they often cannot verify.

A challenge with cyber is the fine line between cyberwarfare vs cybercrime. The methods are the same, but the difference is in the actors and the intent. The “attack surface” of the cyber ecosystem is porous, and expertise in cybersecurity is democratized without any governance or geographic boundaries. The nature of the ecosystem is that it does not have any traditional governance boundaries. It is therefore dependent on nodes in the system to self-organize and develop defense and resiliency tactics, techniques, and procedures. As cyber threats accelerate and expand, criminals and nation-states can exploit vulnerabilities for illegal and great-power interests. Consider the following points within the WEF 2025 cyber threat assessment:

- AI/ML is driving fundamental change in business and geopolitical competition. Only 37% of respondents have a process to assess security tools before deployment
- Nation-states and Trans Criminal Organizations are partnering to attack governments, companies, and people
- Cybercrime-as-a-Service (CaaS) platforms are emerging that provide nation states and criminal actors basically a “fee for service” capability
- “Harvest Now, Decrypt Later” is a growing strategy for “sleeper cells” to sit undetected in networks waiting for technology to emerge, enabling them to break encryption
- The sector is grappling with a significant workforce shortage – 66% of organizations are vulnerable to sophisticated cyberattacks and breaches due to a lack of critical skills

In today’s interconnected environment, cybercrime and cyberwarfare increasingly overlap, making individuals, organizations, and critical infrastructure potential targets even if they are not active participants in conflict. The economic landscape is a primary target for cybercrime and cyberwarfare effects, so anyone relying on anything dependent on critical infrastructure, from fuel, food, medicine, transportation, water, communications, finance, to government services, is being attacked. Fighting a network requires a network that is fluid, adaptable, aggressive, and resilient. Enterprise policies must include comprehensive cybersecurity strategies for defending the network and building resiliency. Collective and individual readiness of organizations through enterprise-wide efforts are essential steps and must include things like cyber intelligence gathering and sharing, minimizing and protecting attack surfaces, mitigating attack vectors that penetrate defenses, and developing Network policies resulting in individual fieldcraft readiness for identifying and defending against attack vectors.

Additionally, there can be partnerships for a network of networks to share the latest for enterprise and individual readiness and turn over intelligence to the governance organizations for offensive cyber operations. To fight a network, it takes a network, and this is where the public and private sectors must increasingly build resiliency in their cybersecurity frameworks. The FBI is an entry point for partnerships in combating cybercrime and cyberterrorism. It is partnering with health care, entertainment, energy, and agriculture business and industry leaders, developing cyber awareness and security networks to protect businesses, consumers, and the population of the United States.

## National Security Cyber Aspects:

The most modern militaries of the world understand, train, and execute operations with an understanding of how domains are mutually reinforcing. In fact, the ability to integrate operations across multiple domains simultaneously is an indicator of a modern military’s prowess in conducting operations globally. The ability to conduct decisive operations with global reach across multiple domains simultaneously in time and space has become a hallmark of U.S. military prowess and dominance since Desert Storm. As the five warfighting domains have emerged, cyber is highly interconnected with the others and increasingly influential in modern operations. While cyber can significantly enhance capabilities across domains, dominance in cyber alone does not automatically equate to dominance in land, sea, air, or space operations. Together, they (wrapped in the umbrella of cyber) form the cognitive engine of modern warfare, enhancing precision, speed, and integration across all domains.

The importance and complexity of the cyber domain in defending U.S. national interests require the DoD to have robust intelligence gathering and analytical capabilities to understand the global and regional threats within the cyber domain and its interdependencies with all warfighting domains. The criticality of cyber in combat operations also requires the U.S. to have a robust capability for both defensive and offensive cyber to protect assets within the nation's boundaries, as well as the strategic and operational activities of all combatant commands.

To meet the challenge of cyber within the United States, DoD began formally in 1952 with the founding of the National Security Agency. The NSA operates under Title 50 U.S. Code as the DoD organization authorized to conduct foreign intelligence and surveillance. Cyber continued to develop as a domain, and in 2010, U.S. Cyber Command became the warfighting command within the Department of Defense for conducting offensive and defensive cyber operations under Title 10 U.S. Code authorities. The result was a "dual hat" relationship formalizing the coordination and synchronization of cyber intelligence, defense of information networks, and warfighting support requirements.

## Economic Takeaways:

The Cyber domain is a globally interconnected and interdependent ecosystem serving most of the global population to work, transact, communicate, entertain, and protect. Using e-commerce sales as an indicator, in 2024, U.S. sales reached around $1.19 trillion, more than double what they were in the previous five years. COVID-19 certainly contributed to its growth, but indicators predict continued increases.

Cyberspace's scope and importance also make it a significant national and international security target – and its value system and associated "attack surface" includes energy, communication, numerous hardware assets, software, and human talent. Also, public and private enterprises share the responsibility to work together to advance, protect, and secure the cyber domain.
Again, consider the following:

- Understand domain composition, such as policies, strategic objectives, and operations
- Know and anticipate threat actor capabilities, intentions, and capacities
- Possess deterrence capacity and resilience capabilities to mitigate threat activities
- Understand the many attack vectors in the cyber domain (supply chain, malware, phishing, hardware/software, networks, denial of service, insider threat, and so on)
- Educate the entire team that touches your systems and networks – every member must be a cyber-defender, as it can take only one weak link to allow adversary entry into your corporation
- As appropriate, notify government agencies of suspected cyberattacks and crimes, such as the FBI's Internet Crime Complaint Center (IC3), the Cybersecurity and Infrastructure Security Agency (CISA), etc.

Finally, if you have not already, consider partnering with the Domestic Security Alliance Council https://www.dsac.gov/ and National Defense Cyber Alliance https://ndcapartners.org/.

*This information is being provided for information purposes only and should not be construed as an offer to sell or a solicitation of an offer to buy any securities. Nothing in the material should be interpreted as investment, tax, legal, accounting, regulatory or other advise or as creating a fiduciary relationship. Product names, company names and logos mentioned herein are trademarks or registered trademarks of their respective owners.*

*Unless otherwise specifically stated, any views or opinions expressed herein are solely those of the author and/or the specific area from which it originates and may differ from the views or opinions expressed by other areas or employees of Bancroft Capital, LLC. The information described herein is taken from sources which are believed to be reliable, but the accuracy and completeness of such information is not guaranteed by us.*

*Bancroft Capital, LLC is a member of FINRA and SIPC.*