United States Cyber Command
Command Challenge Problems Guidance

UNCLASSIFIED

Edition 3

UNITED STATES CYBER COMMAND

Command Challenge Problem Set

All inquiries should be directed to Engage-with-CYBERCOM@cybercom.mil

UNITED STATES CYBER COMMAND
Command Challenge Problems Guidance

The United States Cyber Command (USCYBERCOM) has published its Command Challenge Problems to provide industry partners with clear insight into the critical technology areas where innovative solutions are needed. As the cyber threat landscape continues to evolve, the Department of Defense must stay ahead of adversaries by integrating cutting-edge capabilities in cybersecurity, artificial intelligence, network defense, and other key domains. By outlining these challenge problems, USCYBERCOM seeks to foster collaboration with industry leaders, ensuring that the nation's cyber forces are equipped with the most advanced tools to protect national security interests. This initiative highlights the Command's commitment to working with external partners who can bring fresh ideas and emerging technologies into the Department of Defense's cyber ecosystem.

For industry partners, the Command Challenge Problems serve as a guide to understanding USCYBERCOM's most pressing operational needs. These problem statements are intentionally broad to encourage a wide range of potential solutions while providing enough context for companies to align their research and development efforts with the Command's priorities. Organizations looking to contribute should assess how their technologies, products, or expertise fit within these areas and consider how they can bring unique, scalable, and mission-relevant capabilities to the table. Companies can leverage these challenge problems to refine their proposals, engage with the right stakeholders within the Command, and position themselves for future opportunities in cyber defense innovation.

To maximize impact, industry partners should approach these challenge problems with a problem-solving mindset rather than just a product pitch. USCYBERCOM is interested in solutions that address capability gaps in a meaningful way-whether through novel applications of existing technologies or the development of entirely new capabilities. Engaging with the Command through Cooperative Research and Development Agreements (CRADAs), pilot programs, or industry days can help companies gain a deeper understanding of operational challenges and refine their solutions accordingly. By leveraging the Command Challenge Problems as a strategic entry point, industry partners can play a crucial role in strengthening the nation's cyber defenses while also fostering long-term collaboration with the Department of Defense.

The USCYBERCOM Command Challenge Problems have been broken into six categories. These categories encapsulate broad areas of technology needed by the Command to accomplish its mission to plan and execute global cyber operations.

CYBERSECURITY THREAT DETECTION AND MITIGATION

NETWORK RESILIENCE AND DEFENSE

AUTOMATION

SUPPORT TO CYBERSPACE OPERATIONS

ENTERPRISE

MODELING, PREDICTIVE ANALYSIS, AND DATA

I. CYBERSECURITY THREAT DETECTION AND MITIGATION

Cybersecurity threat detection and mitigation are foundational to USCYBERCOM's mission, ensuring that networks, systems, and critical infrastructure remain protected from evolving cyber threats. This category focuses on identifying, analyzing, and neutralizing threats before they can cause significant damage. Threat actors ranging from nation-state adversaries to criminal organizations constantly adapt their tactics, requiring advanced threat intelligence, real-time monitoring, and rapid incident response capabilities. Industry partners can contribute by developing solutions that enhance threat hunting, anomaly detection, endpoint security, and proactive defense mechanisms, particularly those leveraging artificial intelligence and machine learning for automated threat recognition and response.

Effective mitigation strategies must go beyond detection, enabling cyber operators to respond dynamically to threats in real time.

Solutions in this space should integrate seamlessly with existing cybersecurity frameworks while offering innovative ways to counter adversarial tactics. For instance, deception technologies, automated remediation tools, and advanced malware analysis platforms can help prevent and contain cyberattacks. The ability to coordinate defensive actions across multiple environments-cloud, on-premises, and hybrid networks-is also a key focus.

Keywords: Threat intelligence, Anomaly detection, Malware analysis, Endpoint security, Intrusion prevention, Zero-day threats, AI-driven cybersecurity, Cyber threat hunting, Behavioral analytics, Incident response.

USCYBERCOM seeks novel and innovative solutions to the following Challenge Problems:

1.1 Detect, Defend, and Counter Threats to the Department of Defense Information Network

USCYBERCOM is currently seeking capabilities to adequately detect, defend, or counter adversary threats. This includes cyberspace-attacks based on exploitation of compromised credentials, phishing attacks, and other identity related accesses.

1.2 Strengthen the Security of Critical Networks

USCYBERCOM is currently seeking to develop capabilities addressing the defense of our Nation's Critical infrastructure and key Resources (CIKR) through the identification and recognition of unexpected activities within CIKR control systems that have potential to create cyber-physical effects to operations.

1.3 Insider Threat Monitoring

USCYBERCOM is currently seeking to design, implement, or enhance solutions for detecting insider threat attacks or unauthorized activities. These solutions should employ advanced real-time analysis of multiple data sources and alert when appropriate.

1.4 Proactive Cyber Defense

USCYBERCOM is seeking implementation plans and technology for incorporating decoy technology, moving target defense techniques, and comprehensive refined approaches to implementation of Defensive Cyberspace Operations – Response Actions.

II. NETWORK RESILIENCE AND DEFENSE

Network resilience is critical for maintaining operational continuity in the face of cyber threats, disruptions, and adversarial attacks. USCYBERCOM seeks technologies that enhance the survivability of networks under stress, ensuring that cyber forces can operate effectively even in degraded or contested environments. This includes solutions for dynamic network reconfiguration, self-healing architectures, and redundancy mechanisms that minimize downtime. Technologies that improve real-time monitoring, adaptive defense, and incident recovery are vital for ensuring that mission-critical operations continue without interruption.

Beyond traditional defense mechanisms, this category also focuses on securing networks against both external and internal threats. Zero Trust Architecture, identity-based access controls, and micro-segmentation can significantly reduce the attack surface and limit lateral movement within networks. Additionally, tools that provide automated risk assessment, continuous compliance monitoring, and cyber deception strategies can help defenders anticipate and neutralize threats before they escalate.

Keywords: Zero Trust Architecture, Network segmentation, Cyber resilience, Redundancy and failover, Self-healing networks, Adaptive security, Cloud security, DDoS mitigation, Secure communications, Continuous monitoring.

USCYBERCOM seeks novel and innovative solutions to the following Challenge Problems:

2.1 Zero Trust

USCYBERCOM is currently seeking the ability to apply zero-trust principles to ensure that every user and device must authenticate themselves at each step.

2.2 Redundant and Distributed Systems

USCYBERCOM is currently seeking solutions that provide redundant and Distributed Systems such as Mobile Ad-hoc Networks and hybrid cloud and edge computing models.

2.3 Automated Network Healing

USCYBERCOM is currently seeking solutions for systems that can be configured to automatically identify and mitigate issues and reconfigure or isolate compromised parts of the network without human intervention.

2.4 Mission Relevant Terrain in Cyberspace (MRT-C) Resilience

USCYBERCOM is looking for ways to secure the Department of Defense Information Network riding over Allied Nation provided networks and ways to share the burden of Joint defense of coalition networks, e.g. CENTRIX. This includes securing CIKR and data pathways, and establishing cyber situational awareness.

III. AUTOMATION

The growing complexity and scale of cyber operations demand automation and artificial intelligence (AI)-driven solutions to enhance decision-making and operational efficiency. AI-powered cybersecurity tools can analyze vast amounts of data in real-time, identifying patterns and anomalies that would be impossible for human analysts to detect at scale. This category focuses on leveraging AI and machine learning (ML) to improve threat detection, automate incident response, and enhance predictive analytics for cyber defense. AI-driven tools can assist in prioritizing alerts, reducing false positives, and accelerating mitigation efforts, ultimately enabling cyber forces to operate more effectively.

Beyond cybersecurity, automation can streamline many aspects of cyberspace operations, from vulnerability assessments to network management and operational planning. Intelligent automation can optimize resource allocation, simulate adversary behaviors for red teaming exercises, and support defensive cyber operations through autonomous decision support systems.

Industry partners developing AI-driven solutions should emphasize explainability, interoperability, and real-time adaptability to ensure seamless integration into USCYBERCOM's mission environment. AI will continue to play an increasing role in cyber warfare, making automation a critical capability for defending against emerging threats.

Keywords: Artificial intelligence (AI), Machine learning (ML), Automated threat detection, Intelligent automation, AI-driven cybersecurity, Neural networks, AI for cyber operations, Decision support systems, Autonomous response.

USCYBERCOM seeks novel and innovative solutions to the following Challenge Problems:

3.1 AI-assisted Cyber Threat Hunting

USCYBERCOM is currently seeking solutions that employ AI-assisted threat hunting to improve our ability to manage and investigate sophisticated cyber threats. Such solutions should drastically reduce false positive alerts and enable drill-down to rapidly find relevant information. This includes support to the defense of CIKR.

3.2 Employ AI for Defensive Cyberspace Operations and continuous monitoring

USCYBERCOM is currently seeking solutions that use AI to discover, quarantine, monitor, and block items including vulnerabilities, illegitimate data flows, suspicious behaviors and AI-based threats.

3.3 Assessing and Mitigating Vulnerabilities of Artificial Intelligence Systems

USCYBERCOM is seeking solutions to measure AI system resilience and mitigate vulnerabilities and weaknesses of our AI systems. This includes the establishment of criteria to asses supply chain integrity of AI systems.

3.4 Defending Against Adversary Use of Artificial Intelligence

USCYBERCOM is seeking capabilities to make our systems more resistant to AI-generated threats. This includes AI-based self-adaptive architectures.

IV. SUPPORT TO CYBERSPACE OPERATIONS

Cyberspace operations require a range of technical capabilities, tools, and infrastructure to support both defensive and offensive missions. This category encompasses solutions that enhance situational awareness, mission planning, and operational execution in the cyber domain. Tools that provide real-time visualization of the battlespace, automate operational workflows, and integrate diverse intelligence sources can significantly improve decision-making and mission effectiveness. Secure communications, data fusion, and collaboration platforms are also essential to ensuring that cyber operators can coordinate effectively in high-stakes environments.

Support to cyberspace operations also includes the development of capabilities for cyber training, simulation, and red teaming. High-fidelity cyber ranges, synthetic environments, and adversary emulation platforms help cyber forces hone their skills and prepare for real-world threats.

Additionally, tools that facilitate rapid software deployment, secure DevSecOps pipelines, and cross-domain solutions contribute to the agility and effectiveness of cyber operations.

Keywords: Cyber situational awareness, Mission planning tools, Secure collaboration, Cyber training and simulation, Red teaming, Adversary emulation, Cyber operations automation, Digital twins, Synthetic environments, DevSecOps.

USCYBERCOM seeks novel and innovative solutions to the following Challenge Problems:

4.1 Target and Affect Closed Networks

USCYBERCOM is currently seeking advanced technology to enable operations in heavily contested spaces. Specifically developing capabilities that will allow cyberspace forces to target and affect closed networks, delivery of these components will aid in the identification of the adversary's primary defensive and economic enablers.

4.2 Operationalize Open Source Intelligence Ecosystem

USCYBERCOM is currently seeking assistance with establishing a Department of Defense-wide Enterprise strategy or solution that operationalizes the Open Source Intelligence (OSINT) ecosystem in support of cyberspace operations and threat intelligence.

4.3 Cryptocurrency

USCYBERCOM is currently seeking to block the ability of threat actors to use cryptocurrency to act against US interests. Counter adversarial use and exploitation of blockchain and cryptocurrencies to protect their identities and their affiliations. As well as prevent adversarial mining of cryptocurrencies.

4.4 Protection of Personnel Identities

USCYBERCOM is currently seeking ways to enhance the ability to secure the real identities of military and intelligence personnel from targeting through personal attacks, social engineering, or identity theft.

4.5 Digital Camouflage

USCYBERCOM is seeking ways to ensure digital activities of Department of Defense personnel do not inadvertently expose sensitive information, locations, or operational intentions. This could involve protecting metadata or using encryption to disguise network activity.

4.6 Un-crewed System Countermeasures

USCYBERCOM is seeking ways to counter adversary Command and Control for the use of un-crewed airborne, ground-based, surface, and subsurface systems. This includes the disruption of Precision Navigation and Timing systems supporting adversary un-crewed systems.

IV. SUPPORT TO CYBERSPACE OPERATIONS

4.7 Partnership Enablement

USCYBERCOM is seeking solutions that will enable seamless collaboration with mission partners. This collaboration platform should unify integration during crisis events, offer ability to suggest new conversations based on relevant or trending activity, and to allow partners to rapidly exchange threat intelligence and reporting at all classification levels.

4.8 Cyber Analysis Tools

USCYBERCOM is seeking a mechanism to compare/coordinate cyber analysis and mitigation tools between agencies.

V. ENTERPRISE

Enterprise solutions play a crucial role in ensuring the efficiency, security, and scalability of Department of Defense-wide cyber infrastructure. This category focuses on modernizing IT architectures, enhancing cloud security, and improving enterprise-wide identity and access management. With the increasing adoption of cloud computing and hybrid IT environments, solutions that enable secure multi-cloud operations, software-defined networking, and robust data governance are essential for maintaining operational security. Industry partners can contribute by developing tools that enhance automation, visibility, and compliance across complex enterprise networks.

Additionally, enterprise solutions must address the growing need for secure collaboration and information sharing across different organizations and mission partners. Technologies that facilitate seamless data sharing while maintaining strict security controls-such as zero-trust architectures, cross-domain solutions, and blockchain-based data integrity mechanisms-can greatly improve the cyber resilience of USCYBERCOM's enterprise infrastructure.

Keywords: Cloud security, Hybrid IT environments, Software-defined networking (SDN), Identity and access management (IAM), Cross-domain solutions, Data governance, Secure DevSecOps pipelines, Multi-cloud security, Enterprise IT modernization, Blockchain security.

USCYBERCOM seeks novel and innovative solutions to the following Challenge Problems:

5.1 Command and Control

USCYBERCOM is currently seeking the ability to scale Command and Control (C2) in contested environments, and enhance the situational awareness of cyberspace forces through the development of enhanced delivery platforms.

5.2 Security Information and Event Manager (SIEM) Integration with Big Data Platforms

USCYBERCOM is currently seeking solutions to integrate SIEM capabilities with big data analytics to correlate and analyze events across all parts of the Command.

5.3 Automated Incident Response

USCYBERCOM is currently seeking Security Orchestration, Automation, and Response Platforms to automate the triage, investigation, and response to common security incidents. This includes the ability to automate playbooks for common threats.

5.4 Cyberspace Partnership Opportunities

USCYBERCOM is currently seeking solutions to characterize cyberspace partnerships with international, interagency, industry, and academic partners in order to inform command and staff decisions. Solutions should ingest, analyze, store, and make sense of disparate data sources, including open source information, classified intelligence, and user-provided information using a relational database (SQL or similar) backend with web application front end. The database will order and prioritize partnership opportunities based on a series of predefined variables and relevant analysis at scale and speed.

5.5 Command organizational effectiveness

The USCYBERCOM would like to explore how to better express cyber mission risk at different organizational levels/echelons for better decision-making. This includes ways to improve risk assessment, management, and remediation across directorates and large-scale organizations.

VI. MODELING, PREDICTIVE ANALYSIS, AND DATA

The ability to analyze large-scale datasets and predict cyber threats before they materialize is a critical advantage in modern cyber defense. This category focuses on leveraging big data analytics, AI-driven modeling, and predictive analysis to enhance cyber situational awareness and decision-making. Advanced analytics tools that process vast amounts of cyber telemetry, network logs, and threat intelligence feeds can help identify emerging threats, detect anomalies, and predict adversary tactics. Industry partners can develop solutions that apply machine learning, behavioral analytics, and cyber threat intelligence to anticipate and mitigate risks proactively.

Beyond threat prediction, modeling and simulation technologies can be used to assess the effectiveness of defensive strategies, conduct cyber wargaming, and optimize resource allocation. Digital twin technology, AI-driven simulations, and automated scenario planning can help cyber operators prepare for various contingencies and refine their operational strategies.

Keywords: Big data analytics, Predictive threat modeling, Cyber wargaming, Digital twins, Machine learning for cyber defense, Real-time monitoring, Behavioral threat analysis, Cyber intelligence fusion, AI-driven simulations, Automated scenario planning.

USCYBERCOM seeks novel and innovative solutions to the following Challenge Problems:

6.1 Persistent Operational Cyberspace Access

USCYBERCOM is currently seeking the ability to perform multi-objective analytics in order to predict which tactics, techniques, and procedures are most likely to be successful in gaining persistent access to networks and nodes. USCYBERCOM is currently required to develop/deliver a capability to conduct remote/distributed global cyberspace operations.

6.2 Synthetic and Threat Representative Training Environments

USCYBERCOM is currently looking to enhance its ability to perform cyberspace data generation and modeling to provide cyberspace forces with consolidated, scalable, and repeatable training packages. These packages should address full spectrum cyberspace operations across all domains as well as ensuring effective training management across the force.

6.3 Big Data Analytics

The USCYBERCOM is currently exploring the ability to enhance data analytics and threat intelligence at scale in order to identify malware, source code, documents, file types, etc. This would include capabilities to identify, extract, summarize, and compare/contrast deep meaning and complex relationships within historical and institutional documentation and datasets at operationally relevant speed and scale.

6.4 Critical Dependency Analysis

USCYBERCOM is seeking modeling and simulation capabilities and tools for a deeper understanding of CIKR dependencies which could have an impact on global logistics. These models should represent all items related to the necessary operations of infrastructure, which include civilian infrastructure and power utilities with cyber equities.

6.5 Data Management

USCYBERCOM needs development of standards or tools to ingest non-Department of Defense Critical Infrastructure data into the Joint Cyber Warfighting Architecture BDP Stack.

All inquiries should be directed to Engage-with-CYBERCOM@cybercom.mil