UNITED STATES CYBER COMMAND

2024 Command Challenge Problem Set

All inquiries should be directed to Engage_with_CYBERCOM@cybercom.mil

UNITED STATES CYBER COMMAND
Command Challenge Problems Guidance

As the nation's cyber warriors, United States Cyber Command (USCYBERCOM) operates daily in cyberspace against capable adversaries, some of whom are now near-peer competitors in this domain. Our forces must be agile, our partnerships operational, and our operations continuous. Policies, doctrine, and processes should keep pace with the speed of events in cyberspace to maintain a decisive advantage. Superior strategic effects depend on the alignment of operations, capabilities, processes, as well as the seamless integration of intelligence with operations.

Given the pace and complexity of our mission and platforms, effective solutions must seamlessly integrate, rapidly scale, and allow each side of the interface to independently evolve. Segmented standard interfaces, as well as automation and autonomy, are key elements of any solution.

If a challenge problem is of interest to an external organization, at a minimum, USCYBERCOM would like to know who is working it and be kept apprised of their progress towards achieving all or portions of the challenge. As solutions begin to materialize, it may be beneficial for the Command to give more detailed guidance to the developers. Successfully addressing a challenge problem will not directly result in funding, but doing so will increase the chances that appropriate acquisition and/or transition processes will be employed.

The 2024 USCYBERCOM Command Challenge Problems have been binned into the below six categories. These categories each encapsulate specific areas of expertise and skill sets in order to align with external commercial and academic research, development, and product portfolios.

VULNERABILITIES AND EXPLOITS

NETWORK SECURITY, MONITORING, AND VISUALIZATION

MODELING AND PREDICTIVE ANALYTICS

PERSONA AND IDENTITY

PERMEABILITY AND AGILITY ACROSS DOMAINS

INFRASTRUCTURE AND TRANSPORT

I. VULNERABILITIES AND EXPLOITS

Vulnerabilities exist in network protocols, web-based services, software implementations of these protocols and services, applications on host machines, and in the machine's hardware itself. A myriad of vulnerabilities are published daily, while others are discovered and kept secret as vectors for zero-day attacks. Not all vulnerabilities are suitable for exploitation, but those that are create a defensive challenge, as well as an offensive opportunity.

Challenge problems in this focus area include discovering exploitable vulnerabilities before adversaries do, decreasing the time to defensive patching, implementing defensive measures, and detecting and attributing specific exploits to adversaries. This category includes reverse engineering, malware fingerprint and signature detection, attribution, binary diversity, offensive opportunities, and defensive patching.

Keywords: vulnerabilities, exploits, Common Vulnerabilities and Exposures (CVE), malware, signature detection, zero-day, binary diversity, reverse engineering, Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA), Internet of Things (IoT), attribution, patching, exploitability, Indicator of Compromise (IOC), binary signature, and binary fingerprint

---

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

1.1 Rapidly Generate Defensive Capabilities

USCYBERCOM is currently seeking to mature its ability to rapidly automate the manner in which it performs vulnerability research across all domains. By reverse engineering and developing attack tree generation tools that operate directly on un-normalized intelligence artifacts, USCC must determine how to identify the most complex attack vectors.

1.2 Strengthen the Security of SCADA and ICS Networks

USCYBERCOM is currently looking to develop capabilities addressing the defense of our Nation's critical infrastructure. Protecting this landscape against the use of our machines and processors by Malicious Cyber Actors (MCA) is a top USCYBERCOM priority. A preferred solution would utilize advanced anomaly detection and machine learning techniques to enable threat hunting analysts to identify potential threats and anomalies within critical infrastructure networks, thereby enhancing overall security posture and response capabilities.

II. NETWORK SECURITY, MONITORING, AND VISUALIZATION

Securing Department of Defense (DoD) infrastructure and defeating adversarial intrusion are core USCYBERCOM responsibilities. Detecting intruders, tracking their movements, estimating risk throughout the network, applying defensive countermeasures, and assessing damage and information exposure all present technical challenges. Sophisticated cyber operations demand understanding of both the home DoD network terrain, and the global network terrain from which adversaries launch their attacks.

Challenge problems in this space involve mapping of network topologies and connections, communities, and influencers, with solutions involving large-scale graph theory/graph analytics and network visualizations at their core. Some problems may involve vulnerabilities and malware, and how they travel across the network; however, the problems in this category primarily focus on node-to-node interactions. Finally, the term "network" is used as shorthand throughout this document to describe both traditional networks, as well as our transformational efforts to focus on protecting data and access to the data.

Keywords: networks, monitoring, visualization, graph theory, graph analytics, risk estimation, intrusion detection, lateral movement, damage assessment, traffic redirection, cyber terrain, Zero Trust, and situational awareness

---

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

2.1 Target and Affect Closed Networks

USCYBERCOM is currently seeking advanced technology to enable offensive/defensive cyber operations in heavily contested spaces. Specifically developing capabilities that will allow Cyberspace Operations Forces (COF) to target and affect closed networks, delivery of these components will aid in the identification of the adversary's primary defensive and economic enablers.

2.2 User Activity Monitoring

USCYBERCOM is currently seeking to design, implement, or enhance User Activity Monitoring (UAM) solutions for detecting insider threat attacks or unauthorized activities. UAM solutions should employ advanced real-time analysis of multiple data sources that take into account predictive monitoring, configuration-less features, and non- dependency on policy based (e.g., allow/deny) monitoring features.

2.3 Detect, Defend and Counter Threats to DOD Information Networks (DoDIN)

USCYBERCOM is currently seeking capabilities to adequately detect, defend, or counter adversary threats. Working with Industry, USCC aims to identify a common data schema, rapidly understand the configuration and state of DoD networks, and develop a full spectrum platform for Computer Network Defense (CND) response actions to protect, hunt, and conduct targeted effects against a Malicious Cyber Actor (MCA).

2.4 Support to Cyber Operations

USCYBERCOM requires an Identity enhancements and management capability.

III. MODELING AND PREDICTIVE ANALYTICS

Modeling may capture physical, virtual, or behavioral based observations, and may be rule-based, mathematical, statistical, or physical. Predictive analytics allow users and decision makers to anticipate possible future states, either as a result of taking no action or from pursuing various alternatives. Modeling spans both host-based and network-based problems. The key here is that there is some notion of mathematical or statistical modeling, time-series analysis, or some other mechanism that contributes to prediction or automated detection and response.

Keywords: modeling, predictive analytics, anomaly detection, exploratory analysis, time series, data science, historical baseline, adversarial movement, machine learning, statistics, artificial intelligence, simulation, emulation, story generation algorithms, decision support, autonomous, automation, and causal learning

---

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

3.1 Disruptively Increase the Scale of Operations

USCYBERCOM is currently seeking capabilities that utilize robust code assistive Large Language Model (LLM) deployments, AI automations, and authoritative documentation repositories to support Cyberspace Operations Forces (COF) scale of operations.

3.2 Synthetic and Threat Representative Training Environments

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

3.3 Persistent Operational Cyber Access (POCA)

USCYBERCOM is currently seeking the ability to perform multi-objective analytics in order to predict which Tactics, Techniques, and Procedures (TTP) 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.

IV. PERSONA AND IDENTITY

Many problems in cyberspace depend on persona and identity intelligence, and similarly related topics. User authentication and behavior-based attribution falls in this category, as do the counterpart offensive activities of spoofing, credential misuse, and identity fabrication.

These offensive activities have become increasingly sophisticated in recent years. Identity fabrication, for example, has moved from human- generated phishing attacks to persona fabrication using artificial intelligence, including deep fakes from adversarial networks. Persona issues may intersect with aspects of network community detection or influencer identification.

There is a certain analogy of persona and identity with malware signatures and attribution; however, this category is primarily about people and cyber actors. Some interactions with other challenge problems are expected in this arena.

Keywords: persona, identity, authentication, behavior-based attribution, spoofing, credential misuse, identity fabrication, deep fakes, cyber actors, phishing, cryptocurrencies, social media, and malign influence

---

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

4.1 Misrepresentation

USCYBERCOM is currently seeking to understand how adversaries use masquerading techniques, on-line personas, and how these techniques avoid identification and detection.

4.2 Cryptocurrency

USCYBERCOM is currently seeking to block the ability of MCA 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

4.3 Operationalize Open Source Intelligence Ecosystem

USCYBERCOM is currently seeking assistance with establishing a DoD-wide Enterprise strategy or solution that operationalizes the OSINT ecosystem.

V. PERMEABILITY AND AGILITY ACROSS DOMAINS

This category addresses the tradeoff between protecting classified sources and methods and leveraging external knowledge, data, and situational awareness of uncleared partners. These partners include those in law enforcement, industry, academia, foreign government, and military stakeholders. Sharing between classified and unclassified environments becomes further complicated due to the need to protect information technology assets from cyber threats and to deny threats from reaching those assets.

Cross-domain challenge problems cover the agility and speed-to-market of advanced cyber solutions, or the lack thereof, due to classification, shareability, or equity concerns, and the infrastructure and security practices that hinder fluidity across the various boundaries.

Keywords: sources and methods, partners, protection, external data, cross-domain development, shareability, security practices, rapid prototyping, sandboxes, stand-alone networks, enclaves, equities, and information sharing

---

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

5.1 Sharing and Collaboration with External Partners

USCYBERCOM is currently seeking to engage in partnerships that align our data strategies with industry, standardizes how we store and tag our data, and enables the Command to scale across all echelons to maximize the power of Artificial Intelligence/Machine Learning (AI/ML) at the edge, and in our data centers

5.2 Integration with Kinetic Operations

USCYBERCOM is currently looking to identify innovative and forward-looking tactics, techniques, and procedures (TTPs) to use cyber capabilities at large scale in support of kinetic operations in the operational environments of the future.

VI. INFRASTRUCTURE AND TRANSPORT

The sheer magnitude of the DoD network terrain, and the volume of service components and agencies involved, present challenges for USCYBERCOM to get data, sensor, compute, personnel, tool, and analytic resources where they need to be and to manage those resources effectively in real-time. USCYBERCOM infrastructure assets must reach across the global network. Beyond network monitoring, challenges in this category concern more global mission management, risk management, global situational awareness, and the command- and-control operations of USCYBERCOM.

In the mission management/situational awareness arena, there is the challenge of moving large amounts of data over unclassified links to provide cyber protection forces and leaders with appropriate insights to enable making risk assessments based on reliable information. Problems in this area involve large-scale data storage, transport, and sharing. This category is largely about hardware platforms, movement and tracking of data, and security and risk surrounding these operations.

Keywords: infrastructure, resource management, mission management, risk management, command-and-control operations, data storage, data transport, hardware, and intelligence, surveillance, and reconnaissance (ISR)

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

6.1 Joint Cyber Warfighting Architecture (JCWA) Integration

USCYBERCOM is currently seeking novel ways to incorporate capabilities into the Joint Cyber Warfighting Architecture that integrate proven and robust enterprise software for scaling, automating, and assuring Artificial Intelligence employment in the cyber battlespace. These capabilities are likely to include inference harnesses, Continuous Integration/Continuous Development (CI/CD) pipelines, fully configurable and scalable test and evaluation software, and live user feedback analytic components.

6.2 Joint Cyberspace Command and Control (JCC2)

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. The platform should take into consideration all modes of communication such as Very Small Aperture Terminal (VSAT), 5G and tactical communications.

6.3 AI and Quantum Computing

USCYBERCOM is currently pursuing enhanced AI/ML and Quantum computing solutions that help scale across both the offensive and defensive cyber operations workforce.


UNITED STATES CYBER COMMAND