UNITED STATES CYBER COMMAND

Command Challenge Problem Set

All inquiries should be directed to https://uscybercomtechoutreach.com

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 decisive advantage. Superior strategic effects depend on the alignment of operations, capabilities, and processes, and 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 provide interfaces which 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 outside organization, at a minimum, USCYBERCOM will want 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.

VULNERABILITIES AND EXPLOITS

NETWORK SECURITY, MONITORING, AND VISUALIZATION

MODELING AND PREDICTIVE ANALYTICS

PERSONA AND IDENTITY

PERMEABILITY AND AGILITY ACROSS DOMAINS

INFRASTRUCTURE AND TRANSPORT

The Challenge Problems have been binned into 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.

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 machine hardware itself. Myriad 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, binary fingerprint

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

1.1 Rapidly Generate Defensive Capabilities

Rapidly generate defensive capabilities, and rapidly patch newly discovered vulnerabilities, i.e., mechanisms deploy patches reliably in an automated or accelerated way to reduce or even eliminate the need for human operators' intervention.

1.2 Vulnerability Discovery

Analytical methods that can rapidly analyze software and its function to identify vulnerabilities in software and hardware of interest.

1.3 Holistic Insight into Adversarial Exploits

Rapidly and accurately discover anomalous activity on a network and other indicators of malicious intrusion. Innovative ways to analyze relevant metadata or Packet Capture (PCAP) files, such as employing automated extraction of essential elements of information, and automated summarization of PCAP files to allow for more efficient and faster triage. Agile capabilities that can plug and play into baseline frameworks.

1.4 Polymorphic Malware/Countering Adversarial Signature Diversity

Enable defenders to recognize polymorphic malware in real-time, at network perimeters or when malware has penetrated perimeter security. New ideas to enhance immediate malware recognition.

1.5 Strengthen the Security of SCADA and ICS Networks

Identify ways to analyze and harden legacy ICS/SCADA systems with minimal impact to operations.

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 visualization 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, situational awareness

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

2.1 Automated Network Mapping

Automated tools that produce physical, logical, and functional network maps integrating multiple data sources and including real-time analysis. Networks are complex in depth and breadth, which create challenges to achieve our intended cyber effects. The ability to overlay these network maps and understand relationships and behaviors are critical.

2.2 Deep Network Knowledge and Awareness

We need tools to describe complex networks (including devices, software/firmware versions, and patch level) and overlay command and control logic, data flow, protocols, and physical locations in near real-time. The ability to observe the aggregate network and select appropriate points enables us to catch adversaries in our midst.

Use Case: Up-to-date interactive documentation and repeatable methods are needed to defend our networks.

2.3 User Activity Monitoring

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.

2.4 Establish a Defendable Network

We need novel approaches to defend both the perimeter and the interior of our networks, while keeping in mind the requirements of implementing Zero Trust within DoD networks.

Use Case: As we redesign our network architectures to focus on protecting data as the new perimeter for cyberspace defense activities, we need methods to augment the implementation of these approaches that are rapid and scalable to help reduce our attack surface and help us to be more agile and responsive.

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, causal learning

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

3.1 Forecasting the Information Environment

Methods for understanding, modeling, and predicting the information environment, both in terms of public sentiment and information consumption (e.g., trending topics), adversarial attempts to steer that sentiment, and their ability to succeed. Cyber Command needs ways to distinguish malicious actors attempting to influence the information space from innocuous contributors causing harmless yet viral responses. Separate challenges involve the marketing of ideas, the detection of fake content, and attribution of that content to the actors.

Use Case: Mechanisms for predicting malign campaigns, how world and current events might open opportunities for those campaigns, and what early indications and warnings are associated with these campaigns.

3.2 Automated Anomaly Detection

Identify anomalous behavior in the offensive and defensive cyber operating environments. Capabilities to determine, measure, and characterize, both accurately and efficiently, the baseline state of a network and systematically specify what constitutes deviation from "normal" activity. The ability to recommend actions based on situations that defenders can quickly understand and implement.

3.3 Automated Threat Discovery

Automated solutions for the repetitive, data-intensive tasks of detecting indicators of possible compromise, to bring them to the analysts' awareness, and when appropriate, to apply mitigations or countermeasures to compensate for low human response time. Leverage automated solutions for vulnerability discovery in systems, and then integrate stronger defenses into those systems.

3.4 Predictive Network Modeling

Identify and characterize adversary behaviors and potential attack vectors to enable both offensive and defensive operations. Automate the modeling of networks using partial knowledge to enable creation of multiple scenarios for operational rehearsals. Generate recommendations or perform evaluations on adversary attack behavior to reduce USCYBERCOM response times.

3.5 Predictive Vulnerability Analytics

Multi-objective analytics to predict which Tactics, Techniques, and Procedures (TTPs) are most likely to be successful in gaining access to networks ensures USCYBERCOM is providing solutions that can be employed for their intended purpose in a timely manner.

III. MODELING AND PREDICTIVE ANALYTICS CONT.

3.6 Synthetic and Threat Representative Environments

Simulate network operating conditions for a variety of purposes, including the education and training of cyber forces on TTPs and the rehearsal of cyber missions. Generate threat-representative environments to conduct simulated Defensive Cyber Operations (DCOs), or hunt exercises. Create synthetic threats in a customizable and re-playable manner, measure and record DCO operator performance and skill level, and increase complexity of the simulated threats based on user setting or on the measured operator's skill level. Create synthetic users and network activity to be used in a customizable and re-playable manner.

Use Case: Current systems used throughout the Command and the greater DoD lack the detail needed to simulate high-fidelity real-world networks. The ideal system would collect and anonymize real-world network and host data for re-use in a simulated environment.

Use Case: Simulations to emulate cyber intruders, as well as cyber adversaries conducting surveillance and reconnaissance using realistic TTPs. The solution would facilitate experimentation to identify DCO best practices and the data needed to conduct effective hunt 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, malign influence

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

4.1 Misrepresentation

Understand how adversaries use masquerading techniques and on-line personas, and how these techniques avoid identification and detection.

4.2 Multi-Factor Authentication Vulnerabilities

Understand the vulnerabilities of multi-factor authentication.

Use Case: Understand the various multi-factor methods used by common applications and determine their security level. Analyze which communication channels, such as email or text-messaging these methods use, if any. Which applications rely on biometrics or synchronized token generation? Can they be circumvented, and what weaknesses exist?

4.3 Cryptocurrency

Block the ability of the adversary to use cryptocurrency to act against US interests. Counter adversarial use and exploitation of blockchain and cryptocurrencies to protect their identities and their affiliations. Prevent adversarial mining of cryptocurrencies globally. Detect and counter adversarial mining of cryptocurrencies on U.S. commercial or cloud infrastructure. Track blockchain entities and permanently link personas of interest to better understand the network effects in play.

4.4 Adversary Attribution through Block-Chain

Analytic techniques that can link adversary entities through blockchain and/or blockchain-based cryptocurrencies.

Use Case: Discriminate nation state adversary activity by applying these techniques to entities could potentially provide game-changing insights.

4.5 Malign Influence

Recognize and attribute malign use of false personas and messaging. Recognize flaws in development and employment of these entities.

V. PERMEABILITY AND AGILITY ACROSS DOMAINS

Address 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, information sharing

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

5.1 Collaborative Capability and Analytic Development Environment

Ability to work collaboratively with other government, industry, and academic entities in and across shared, secure and unsecured environments.

Use Case: Rapidly prototype solutions, test and experiment with unique hardware or online-only services, build and share relevant labeled data sets, as well as manage and update analytic models as mission needs and data characteristics evolve.

5.2 Sharing and Collaboration with External Partners

Technical solutions for sharing large quantities of data with federal, state, and local law enforcement, as well as other partners, while sanitizing data that may contain classified content or otherwise reveal protected sources and methods. Create an automated or semi-automated system that can identify the classified content, or that can lead a human reviewer to the classified content, at an extremely high level of precision, and that obviates the need for thorough manual review.

5.3 Integration with Kinetic Operations

Identify innovative and forward-looking TTPs to use cyber capabilities at large scale in support of kinetic operations in the operating environment 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 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, ISR (intelligence, surveillance, and reconnaissance)

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

6.1 Data Collection and Transport

Dynamic, mission-configurable, anonymized data collection and transport. A tool that can expedite solutions to storage and transfer on the scale of petabytes to exabytes.

Use Case: Moving large amounts of data over unsecured and non-traditional data links is critical to enable defenders and leaders to understand and visualize their area(s) of responsibility in the domain. They need the ability to see their responsible areas, share insights, and gain insights from the larger context.

6.2 Cyber Knowledge Storage System

New approaches to long-term data storage solution with the ability to share, and quickly retrieve relevant information while keeping cost, security, compatibility, and scalability in mind.

6.3 Identification of Critical Assets

Automated solutions, tools, and capabilities to 1) easily decompose missions to identify Task Critical Assets (TCAs); 2) identify and map Mission Relevant Terrain in Cyberspace (MRT-C) supporting Tier 1 TCAs; 3) identify and maintain situational awareness and visualization of Tier 1 TCAs and their associated MRT-C; and 4) secure and defend MRT-C against malicious cyberspace activities.

UNITED STATES CYBER COMMAND

All inquiries should be directed to https://uscybercomtechoutreach.com