UNITED STATES CYBER COMMAND

TECHNICAL CHALLENGE PROBLEM SET

2020

U.S. Cyber Command
2020 Technical Challenge Problems
Guidance

As the nation's cyber warriors, USCYBERCOM operates daily in cyberspace against capable adversaries, some of whom are now near-peer competitors in this domain. We have learned we must stop attacks before they penetrate our cyber defenses or impair our military forces; and through persistent, integrated operations, we can influence adversary behavior and introduce uncertainty into their calculations. 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. Now we must apply this experience by scaling to the magnitude of the threat, removing constraints on our speed and agility, and maneuvering to counter adversaries and enhance our national security.

The following 2020 Technical Challenge Problems describe areas of significant challenge to the Command and reflect our most pressing capability needs. These build upon the initial set of Technical Challenges and as before, will be used to enrich our engagement with capability providers in Industry, Academia, and other Government entities.

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.

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

U. S. CYBER COMMAND
2020 Technical Challenge Problems

Based on the nature of the 2019 Technical Challenge Problems (TCPs), and in light of ongoing, current operational needs, U.S. CYBER COMMAND has developed the following Technical Challenge Problem Set for 2020. The 2020 Technical Problems are binned into six new categories. These categories each encapsulate specific areas of expertise and skill set in order to align with external commercial and academic research, development, and product portfolios. Many of the 2019 Technical Challenge Problems remain unresolved and are folded into the 2020 Technical Challenge Problems. For ease of reference, the 2019 Technical Challenge Problems are mapped to these new categories as well.

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 hardware itself. Myriad vulnerabilities are published daily in the Common Vulnerability Exposures (CVEs); others are discovered and kept secret as vectors for zero-day attacks. Not all vulnerabilities are amenable to exploits, but those that are present both a defensive challenge as well as an offensive opportunity. Challenge problems in this space include discovering exploitable vulnerabilities before adversaries do, decreasing the time to defensive patching, implementing defensive measures, and detecting and identifying specific exploits with attribution to adversaries. Included as part of this category are two particular arenas that present both enhanced risk: Supervisory Control and Data Acquisition (SCADA)/Industrial Control System (ICS) networks protecting critical infrastructure and the burgeoning Internet of Things (IoT) device networks. Skill sets needed in this category include reverse engineering, malware fingerprint and signature detection, attribution, binary diversity, offensive opportunities and defensive patching.

2019 Problems: 1, 2, 3, 4, 8, 9, 21, 23, 24, 25, 45

Keywords: *vulnerabilities, exploits, CVE, malware, signature detection, zero-days, binary diversity, reverse engineering, SCADA/ICS, IoT, attribution, patching, exploitability, Indicator of Compromise(IOC) , binary signature, binary fingerprint*

Key Joint Cyberspace Warfighting Architecture (JCWA) Stakeholders: Tools, Access, Sensors

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

2020 1.1 CHALLENGE PROBLEM: Rapidly Defend and Exploit Vulnerabilities

Rapidly generate defensive capabilities and rapidly patch newly discovered vulnerabilities. We need mechanisms not only to generate viable patches quickly, but also to deploy them reliably in an automated way to reduce or even eliminate the need for human operators to intercede. Correspondingly, we need the ability to rapidly develop means to exploit those vulnerabilities before a patch can be developed or distributed and applied by the adversaries.

2020 1.2 CHALLENGE PROBLEM: Vulnerability Discovery

Analytical methods that can rapidly analyze software and its function to identify vulnerabilities in binaries of interest. For each vulnerability, determine how the vulnerability is exploitable, develop a means to exploit it, mitigate it, and test the exploit in a highly realistic environment.

2020 1.3 CHALLENGE PROBLEM: Identifying Malware

Rapidly and accurately discover anomalous activity on a network and other indicators of malware. Hunt missions are a growing tool in our defense arsenal. We can look for anomalous activity and look for evidence of malware.

Finding and recognizing these potential nefarious activities is challenging. Assessing the evidence is essential to understand the true threat. Reverse engineering malware to gain such insights can be time intensive. We need 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. We also need agile capabilities that can plug and play into baseline frameworks.

2020 1.4 CHALLENGE PROBLEM: Leverage Malware

USCYBERCOM needs an improved or innovative way to quickly and effectively reverse engineer malware to discover novel Tactics, Techniques, and Procedures (TTPs) that can be extracted and incorporated into US tools. Techniques for exploitation, local privilege escalation, and persistence are of particular value. Similarly, USCYBERCOM needs an improved workflow for observing what vulnerabilities adversaries are exploiting for initial access and rapidly developing exploits for those same vulnerabilities. This will allow USCYBERCOM to rapidly contest adversary activities as part of its persistent engagement mission.

2020 1.5 CHALLENGE PROBLEM: Agent Persistence

Keep exploit code or functionality persistent within network devices, endpoints, and mobile devices. Many capabilities presently do not survive system update or reboot. Persistence must be achieved without further USCYBERCOM operator involvement.

2020 1.6 CHALLENGE PROBLEM: Polymorphic Malware/Countering Adversarial Signature Diversity

Enable defenders to recognize polymorphic malware in real-time, at the perimeter of our networks or when malware has penetrated our perimeter security. Adversaries are increasingly avoiding anti-virus detection tools by rapidly morphing their signatures or evading heuristic based detection. Small changes by adversaries create an asymmetric advantage by significantly increasing the work factor to defeat existing malware. What are some innovative new ideas to enhance immediate malware recognition?

2020 1.7 CHALLENGE PROBLEM: Auto Installer

We need the ability to remotely change, upgrade, or install software within a network enabled device through automated means when a human operator is incapable, doesn't have time, or doesn't have the knowledge to make the necessary changes while the system is operational.

2020 1.8 CHALLENGE PROBLEM: SCADA/ICS Vulnerabilities

Strengthen the security of Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) networks. Effective mitigations are constrained by the need to have limited system impact and low-cost. We also need to expose vulnerabilities and develop mitigations.

2020 1.9 CHALLENGE PROBLEM: Internet of Things (IoT) Defense

Reduce the risks associated with IoT devices. Identify IoT devices on networks, identify vulnerabilities arising from the presence of IoT devices, and identify specific entry points and opportunities for lateral movement, and pivoting, in a network due to the presence of IoT devices. The rapid growth of IT enabled things in the IoT has increased vulnerabilities in networks. USCYBERCOM personnel are not increasing at a corresponding pace. Solutions must keep pace with the increasing threat and the non-linear growth of personnel.

USCYBERCOM needs a means to identify and exploit IoT vulnerabilities in order to protect its networks, and gain access to adversary networks in order to move laterally, pivot, and achieve dominance.

2020 1.10 CHALLENGE PROBLEM: Survivability/Implementing Signature Diversity for Offense

Survivable offensive capability. The frequency of tool roll ups is increasing due to leaks, the expansion of cyber security reporting and researchers publishing. Tool reuse, common libraries, shared infrastructure, common persona management tactics, techniques and procedures can lead to more significant impacts from these exposures. In turn, every small exposures damages increasingly greater aspects of our mission space. How can we reduce the risk? What can we do to manage risk better across missions? This need applies to development and operations. It spans capabilities, infrastructure and personas.

2020.1.11 Adversary Weapon Systems

Like other embedded systems, exploiting adversary weapon systems will require novel approaches. While exploiting Platform IT may be similar to other missions, gaining access to the Platform and exploiting the weapons system itself may require unique access and other tools.

II. Network Security, Monitoring, and Visualization

Securing Department of Defense infrastructure and simultaneously defeating corresponding adversarial measures present a number of key challenges. Cyber intruders may gain access to a network through gateway nodes and subsequently move laterally through the network over the course of many days, months, or even years. Detecting intruders, tracking their movements, estimating risk throughout the network, applying defensive countermeasures, and assessing damage and information exposure all present technical challenges. Monitoring and visualizing the network terrain through both manual and automated means is key. Offensive and defensive operations demand understanding of both the home DoD network terrain as well as the global network terrain from which adversaries launch their attacks. Operations may also rely on knowledge of adversarial entities and their communities, as well as ways in which those entities and communities may exert influence through social media and information campaigns. Challenge problems in this space involve 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.

2019 Problems: 12, 20, 30, 32, 47, 49, 50

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

Key JCWA Stakeholders: Sensors, Joint Operations Center (JOC), Joint Cyber Command and Control (JCC2)

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

2020 2.1 CHALLENGE PROBLEM: Automated Network Mapping

Automated tools that produce physical, logical, and functional network maps of DoD networks and for adversaries' networks. Understanding our own networks is key to securing our networks. Understanding our adversaries' networks and how to reach them is key to enabling our ability to defend forward and conduct offensive operations. At best, both these networks are complex in depth and breadth which create challenges to achieve our intended cyber effects. The ability to overlay these networks is critical.

2020 2.2 CHALLENGE PROBLEM: Information Environment Visualization

Understand adversary activities in the information environment. Visualizing forces and campaigns in the information environment is complex. Tying information operations and cyber activity demonstrates the confluence of adversary actions. We need tools to filter out the noise, understand the critical elements, and enable proactive mission execution.

2020 2.3 CHALLENGE PROBLEM: Deep Network Knowledge and Awareness

Tools that will not only describe complex networks (including devices, software/firmware versions, and patch level) but also overlay command and control logic, data flow, protocols, and physical locations in near real-time. We need to be able to observe the aggregate network in order to select appropriate points that would enable us to catch adversaries in our midst.

2020 2.4 CHALLENGE PROBLEM: User Activity Monitoring

Design, implement, or enhance User Activity Monitoring (UAM) solutions for detecting live and recent insider threat attacks or unauthorized activities. We need to identify UAM solutions that employ advanced real-time analysis of multiple data sources, which includes predictive monitoring, configuration-less features, and non-dependency on policy-based (e.g. allow/deny) monitoring features.

2020 2.5 CHALLENGE PROBLEM: Establish a Defendable Network

Secure and defend USCYBERCOM current and legacy networks from inside and outside threats. Automatically remediate vulnerabilities and insecure configurations. Flip the defender/offense paradigm, enable defenders to have least cost in the battle to maintain confidentiality, security, and integrity. As we redesign our network architectures to focus on protecting data as the new perimeter for cyberspace defense activities, we need methods to rapidly assist the implementation of these approaches to help reduce our attack surface and help us be more agile/mobile in what we do. Implement self-healing approaches. Implement effective deterrence. We need novel approaches and as game-changing ideas to enhance defense-in-depth.

2020 2.6 CHALLENGE PROBLEM: Network Traffic Redirection/Obfuscation

Methods to obfuscate or redirect selected network traffic in novel ways.

III. Modeling and Predictive Analytics

Modeling may capture past 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.

2019 Problems: 13, 14, 15, 16, 17, 19, 37, 38

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*

Key JCWA Stakeholders: Sensors, Persistent Cyber Training Environment (PCTE)

USCYBERCOM seeks novel solutions to the following Technical Challenge Problems:

2020 3.1 CHALLENGE PROBLEM: Forecasting the Information Environment

Methods for 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 information space from innocuous contributors causing harmless yet viral response. It also needs mechanisms for predicting malign actors influence campaigns, how world and current events might open opportunities for those campaigns, and what early indications and warnings there may be. Separate challenges involve the marketing of ideas, the detection of fake content, and attribution of that content to the actors. A major constraint in this space is that Cyber Command cannot, and must not even be perceived as trying to, influence U.S. or allied public sentiment nor monitor that sentiment for illegal or nefarious purpose.

2020 3.2 CHALLENGE PROBLEM: Normal and Abnormal Operating Conditions

Recognize anomalous from normal behavior in the offensive and defensive cyber operating environments. As U.S. Cyber Command digs deeper into the data available, we learn new information and gain new insights. We need to determine, measure and characterize, both accurately and efficiently, the baseline state of a network and systematically specify what constitutes deviation from ‘normal’ activity. We need to recommend actions to situations that defenders can quickly understand and take.

2020 3.3 CHALLENGE PROBLEM: Automated Exploit and Capabilities Discovery

Augment its limited personnel resources with meaningful technology and automated processes. Today's mission environment can be analyst intensive - it takes staff resources to analyze and synthesize network conditions. However, too much analyst time is spent performing manual and repetitive processes instead of focusing on actual analysis of the threats and opportunities. This problem is further compounded by the fact that those threats and opportunities are hidden in a sea of innocuous background data. U.S. Cyber Command needs automated solutions for the repetitive, data-intensive tasks. It needs solutions to detect indicators of possible threats, to bring them to the analysts' awareness, and, when appropriate, to apply appropriate mitigations or countermeasures to compensate for low human response time. Automated solutions may address many of the technical challenges facing Cyber Command, from timeliness of vulnerability and exploit discovery to network mapping and visualization to command and control of infrastructure and transport. Automated solutions may link some of these challenges together. For example, how can we leverage automated solutions for vulnerability discovery in real systems and then integrate stronger defenses into those systems? The particular constraint here is how U. S. Cyber Command can augment personnel resources in a meaningful and constructive manner. Specifically, how could U. S. Cyber Command deploy automated solutions as a natural and necessary tool in the analyst's arsenal rather than as a bulky and cumbersome distraction that is perceived as getting in the way?

2020 3.4 CHALLENGE PROBLEM: Predictive Network Modeling

Methods to augment limited resources to identify and characterize adversary behaviors and potential attack vectors to enable both offensive and defensive operations. U.S. Cyber Command has limited resources to defend our networks and effectively conduct offensive operations. These limitations affect timeliness and latency of our defensive and offensive posture as well as our coverage. Today this is largely reliant on experts to guide future efforts. Are there ways to leverage computer modeling, graph structures, game theory, and machine learning to generate recommendations or evaluations of behaviors and adversary attacks to reduce the time for USCYBERCOM to respond?

2020 3.5 CHALLENGE PROBLEM: Predictive Vulnerability Analytics

Tools to predict or estimate the exploitability of vulnerabilities. Fuzzers frequently produce many more crashes and potential vulnerabilities than can be evaluated by skilled vulnerability researchers. Moreover, the majority of these crashes are not exploitable. Tools to automate this analysis process, reduce the time it takes to develop exploits, and reduce the skill barrier for vulnerability research.

There are typically many potential vectors to access an adversary's network. Analytics to predict which TTPs are most likely to be successful to gain access to a network will ensure we are providing solutions that can be employed for their intended cyber effect in a timely manner.

2020 3.6 CHALLENGE PROBLEM: Effective Automation and Analytic Methodology

Holistic, scientific, and reproducible methodologies for getting the optimal capabilities and analytics applied to the correct use cases. Analytics can certainly reduce the burden on our operators. However, too often we jump to solution without stepping through a thoughtful and rigorous process of analytic development methodology. We need to create a data submission/handling process. We need to build tools around desires of the

experienced operator and build what-if case studies to merge previously un-compared or disparate datasets for new insights. We need to ask ourselves what about this job may be automated to enable future discovery or analytic pursuit. The solution to this challenge may be more an abstraction of how we do things rather than a system that emulates those processes. The particular constraint to this challenge is the need to understand how operators function without taking too much of their time, without getting in their way, and perhaps without being physically on site.

2020 3.7 CHALLENGE PROBLEM: Synthetic Users

A mechanism for simulating network operating conditions for a variety of purposes, including the education and training of cyber forces on tactics, techniques, and procedures (TTPs) and the rehearsal of cyber missions. Current systems used throughout the Command and the greater Department of Defense lack the detail needed to simulate real world networks at high fidelity. A desired solution would be a system that creates synthetic users and network activity to be used in a customizable and re-playable manner. The ideal system would collect and anonymize real-world network and host data for configurable and adjustable, and deterministic or stochastic, re-use in a simulated environment.

2020 3.8 CHALLENGE PROBLEM: Threat-Representative Environment

Mechanism for generating a threat-representative environment to conduct simulated defensive cyber operations (DCOs), or hunt exercises. Such simulations would generate simulated cyber intruders as well as cyber adversaries conducting surveillance and reconnaissance using realistic tactics, techniques, and procedures (TTPs). The sought solution would facilitate experimentation to identify DCO best practices and the data needed to conduct effective hunt operations. Such a system would also create synthetic threats in a customizable and re-playable manner, would measure and record DCO operator performance and skill level, and would increase complexity of the simulated threats based on user setting or on the measured operator skill level.

IV. Persona and Identity

A perhaps surprisingly large number of problems in cyberspace depend on persona and identity intelligence, as well as 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 so-called deep fakes from generative adversarial networks. Persona issues may intersect with aspects of network community detection or influencer identification; however, problems in this category primarily focus on the individuals and their characteristics and not on cross-network interactions and propagations. 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.

2019 Problems: 22, 34, 35, 36, 51, 52, 53

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

Key JCWA Stakeholders: Access

USCYBERCOM seeks novel and innovative approaches to the following Technical Challenge Problems:

2020 4.1 CHALLENGE PROBLEM: Misrepresentation

Understand how adversaries use masquerading techniques and, in general, on-line personas. Adversaries use these techniques to gather information and gain access to information systems. We need to know what masquerading techniques avoid identification and detection. Also, it is important to know if results are different for various network devices.

2020 4.2 CHALLENGE PROBLEM: Two-Factor Authentication Vulnerabilities

Understand the vulnerabilities of two-factor authentication. What are the various two-factor methods used by common applications? How secure are they? What communication channels, such as email or text-messaging, do they use, if any? Which applications rely on biometrics or synchronized token generation? Can they be circumvented? Open source research to help answer these questions is needed by the Command.

2020 4.3 CHALLENGE PROBLEM: Defensive Cryptocurrency

Leverage open source research and experimentation to counter adversarial use of block-chain and block-chain cryptocurrencies to protect their identities and their affiliations. We also seek to counter adversarial mining of cryptocurrencies. Is it possible to develop analytics in this space? Are there ways to detect and counter

adversarial mining of cryptocurrencies on U.S. commercial or cloud infrastructure? How do we track block-chain entities and attempt to permanently link personas of interest?

2020 4.4 CHALLENGE PROBLEM: Adversary Attribution through Block-Chain

Analytic techniques that can link adversary entities through block-chain and/or block-chain based cryptocurrencies. Today we recognize some actors in cyberspace, but not all. The work is painstaking especially with adversaries using advanced tradecraft to obfuscate entities and actions. How do we discriminate nation state adversary activity? Applying these techniques to entities adds extra complexity but could potentially provide game changing insights. Where does block-chain create challenges and opportunities in our ability to attribute or identify actors in cyberspace?

2020 4.5 CHALLENGE PROBLEM: Malign Influence

Recognize malign influence use of false personas, false messaging, and attribute them. Recognize flaws in development and employment of these entities. Use commercial digital ecosystem to detect and attribute.

V. Permeability and Agility across Domains

A particular challenge area posed to USCYBERCOM is the tradeoff between protecting classified sources and methods and leveraging the external knowledge, data, and situational awareness of uncleared partners. These partners include those in law enforcement, industry, the external hacking community, and foreign government and military stakeholders. Sharing between classified and unclassified environments becomes further compounded by the need to protect information technology assets from cyber threats and to quarantine particular threats from reaching those assets. Malware analysis provides one particularly salient example, whereby we typically relegate detected malware to an isolated safe sandbox environment prior to performing a time-bound and resource-intensive analysis using state-of-the-art tools and techniques, the collaborative nature of which is lost or severely impacted by the quarantine environment. 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.

2019 Problems: 6, 7, 10, 11, 18, 26, 28, 33

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

Key JCWA Stakeholders: Unified Platform

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

2020 5.1 CHALLENGE PROBLEM: Unclassified Operations Using Classified Insights

An ability to operate on the Internet in an unclassified manner while also leveraging insights gained from classified sources and methods. The particular challenge here is for cyber teams to perform operations out on the open network terrain within potential view of the adversaries while not indicating intentions, not raising suspicions, and not revealing their own methods nor the sources and methods used to acquire classified insights. Such activities might involve conducting cyber intelligence, surveillance, and reconnaissance (ISR) on adversarial networks, acquiring adversary access credentials, or analyzing cyber actors on social media platforms. This challenge includes being able to federate queries of unclassified data from a classified enclave. It also involves probing for information without revealing what information is of interest, and with the assumption that the adversary has full visibility into both the probe and the results. We must be able to provide time-limited access to data with timely authorization of the data owner.

2020 5.2 CHALLENGE PROBLEM: Efficient and Secure Environment for Malware Analysis

Appropriate environment for malware analysis. Today we have a cumbersome process to access malware for analysis. We isolate the malware in standalone sandboxes. This enables us to examine the malware without risk to mission networks. Current policies make intentional cross-domain transfers of new and known malware cumbersome and at times impossible. We want to be able to analyze individual instances of malware in the

global context of related malware. The analysis environment needs to support many instances of malware and be replete with collaboration tools for our analysis. Preferably in the same environment, we need to be able to assess countermeasures realistically. Our current quarantine efforts are both time- and resource-intensive and cannot keep up with increasing scale. Are there technical solutions which could enable the fast and intentional movement of malware by authorized individuals across domains into appropriately controlled environments?

2020 5.3 CHALLENGE PROBLEM: Special Hardware and Services Testing Environment

Flexible and accessible operational test environments while still protecting our equities. Currently U.S. Cyber Command develops and tests in secure environments, which precludes operating certain devices. This in turn limits our understanding of the challenges and opportunities for potential proposed solutions. We need to emulate hardware or network services to evaluate the risk of implementing new technologies outside our secure environments. We need to host virtually or emulated architecture rapidly. We need to code on alternative hardware to reduce the risk of compromise to the system or network.

2020 5.4 CHALLENGE PROBLEM: Realistic Capability Development and Testing Environment

Rapidly employ and develop obfuscators, fuzzers and signature variants to diversify capabilities. We need tools and techniques to ensure we can evade detection in order to create the desired cyber effects. Being elusive is increasingly difficult - we must not only design and develop tools with risks in mind, we must also test our tools before we use them to ensure they perform as expected and do not reveal their presence. We must ensure tools do not have unique or expected signatures. We need modular testing environments that can emulate commercial Personal Security Products (PSPs) presence in target spaces.

2020 5.5 CHALLENGE PROBLEM: Collaborative Development Environment

An environment and process to collaborate effectively with other government, industrial, and academic entities to leverage and contribute to cutting-edge research concepts and prototypes as well as to polished, ready-for-deployment analytics and systems. Cyber Command would benefit from such collaboration in that there is a wealth of external research and development in large-scale data analytics and data management, to include advanced and specialized knowledge in statistics, machine learning, graph analytics, high performance computing, and artificial intelligence, to name but a few such areas. External partners would benefit from Cyber Command's unique data sets, mission use cases, and potential purview to much of the network terrain. A major challenge in this space is matching the specific Cyber Command needs and operating environments with the prototypes and turnkey systems developed for other government, commercial, and academic use cases – the expectation being that adaptation from both ends (i.e. mission environment and developed solution) would be needed. Another challenge, but definite opportunity to the collaborators, is the building and sharing of relevant labeled data sets, as well as the management and updating of analytic models and labeled data as mission needs and data characteristics drift.

VI. Infrastructure and Transport

The sheer magnitude of the Department of Defense network terrain and the volume of service components and agencies involved present particular 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 to adversarial terrain. 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 particular challenge of moving large amounts of data over unclassified links to provide cyber protection forces and leaders with insights from a larger context and of making risk assessments based on outdated and incomplete information. Additionally, operations must be coordinated across our cyber forces and those of our partners; offensive actions must not impact U.S. network resources nor those of our allies and bystanders. 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.

2019 Problems: 27, 29, 39, 40, 41, 42, 43, 44, 46, 48

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

Key JCWA Stakeholders: JCC2, Unified Platform

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

2020 6.1 CHALLENGE PROBLEM: Data Collection and Transport

Dynamic, mission-configurable, anonymized data collection and transport. Moving large amounts of data over unclassified links is critical to enable defenders and leaders to rapidly consume, analyze, and understand and visualize their area of responsibility in the domain. Not only do they need to see their responsible areas but need to share insights and gain insights from the larger context. USCYBERCOM needs a development effort that can expedite large and sensitive data sets solutions to storage and transfer on the scale of petabytes to exabytes.

2020 6.2 CHALLENGE PROBLEM: Infrastructure/Platforms

Tools to provide cyber effects. We consistently need new tools that can be deployed from our platforms and ride across the infrastructure. What specific tools, frameworks, and techniques would be game changers in this demanding field?

2020 6.3 CHALLENGE PROBLEM: Network and Device Knowledge Storage System

Store, share, visualize, and act on massive amounts of cyber data. Cyber is a complex domain with billions of information data points. There are many different software tools running various versions of software operating on many different hardware devices using a variety of protocols. In addition, the dynamic state can reveal new

vulnerabilities and other dependencies. The scale and complexity (volume, variety, and velocity) is ever increasing. What approaches would be useful to storing, sharing, and quickly retrieving relevant information?

2020 6.4 CHALLENGE PROBLEM: Global Malware Tracking

Detect malware in our network. Today it is difficult to track adversaries' maneuver of malware on our own infrastructures. When we lack this insight, it limits our ability to understand the specific goals and objectives of the malware, let alone the user's intentions. We need file and log level details distilled to meaningful data for comparison to a global viewpoint. We need an automated link and link-type discovery application that can form associations useful in attribution. We need to see the software versions employed and observe malware ecosystems through evolution and in the context of it being a managed environment ultimately attributable to an actor.

2020 6.5 CHALLENGE PROBLEM: Automated Mission Risk Management

Understand the risks to mission execution and we need to be able to effectively convey those to our partners and those we support. Leaders can take calculated risks, if they are known. What are the key risk components, how should they be tracked, visualized and how can they be effectively communicated? How do we calculate and include 2nd and 3rd order of magnitude effects of risk alternatives and preposition for adversary contingencies to mitigate risk exposure?

2020 6.6 CHALLENGE PROBLEM: Coordination of Mission Needs Across Partners

Coordinate operational cyber actions in neutral and adversarial cyberspace. We must shift our approach from deconfliction to operationally coordinate living in adversary space. Coordination must also preclude unintentional exposure of operational mission facts 24/7/365. We also need to coordinate exploitation tools, capabilities we purchase or develop, infrastructure we leverage and personas we intend to use to carry out our missions. These diverse aspects require quick resolution in response to mission demands across the DoD and Intelligence Community (IC). Cyber coordination must enable sharing of knowledge about key facts without unnecessarily revealing operational and development secrets.