59-0001

CRIS Cyber Range Lexicon
Version 1.0

A Product of the Cyber Range Interoperability Standards (CRIS) Working Group (WG)

Prepared under the direction of the U.S. Department of Defense; Office of the Secretary of Defense for Acquisition, Technology, and Logistics; Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation/ Test Resource Management Center

10 November 2015

Editors: Dr. Suresh K. Damodaran, MIT Lincoln Laboratory
Ms. Kathy Smith, GBL Systems Corporation

This work is sponsored by the Test Resource Management Center under Air Force contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government.

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
244 Wood Street, Lexington, MA 02420-9108

TABLE OF CONTENTS

LIST OF FIGURES

1.0 PREFACE

Numerous organizations have created tailored processes for conducting cyber-range events. Such events may require, in addition to cyber, integration with kinetic and networked infrastructure assets and capabilities. Several kinds of tools have been designed and used in these events. The variety of tools have made the process of conducting events longer and more expensive than necessary due to semantic and syntactic mismatches among the myriads of tools used.

Cyber Range Interoperability Standards Working Group (CRIS WG) was founded in 2012 to identify the requirements, and to recommend the standards necessary to accomplish the goals stated above. The CRIS WG consists of cyber-range practitioners from government, industry, and academia and is sponsored by the Department of Defense (DoD) Test Resource Management Center (TRMC). The CRIS WG is open to all participants from the United States Government or its contractors who conduct or support cyber-range events currently, or plan to do so in the future. Communities supported by the CRIS WG include, but are not limited to, Science & Technology (S&T) experimentation, Developmental and Operational Test and Evaluation (DT&E, OT&E), cyber force training, and mission rehearsal.

To facilitate discussions among these related communities, the CRIS WG is establishing a common cyber-range lexicon. This document contains the current version of this lexicon. This publication supplements standard English-language dictionaries and standardizes cyber range and associated terminology to improve communication and mutual understanding of cyber range activities within the DoD, and possibly with other federal agencies of the United States and its allies.

1.1 SCOPE

The Cyber Range Lexicon defines standard terminology to describe all the activities associated with Cyber Ranges. This lexicon has been discussed and refined by the participants of the Cyber Range Interoperability Standards Working Group. The CRIS WG recommends the use of the terminology defined in this lexicon for Cyber Range Events.

1.2 POLICY OF INCLUSION OF TERMS

Cyber Range Lexicon is defined to aid cyber range practitioners, and may define or refine terms already defined in other widely used publications. Wherever possible, such inclusion of terms is accompanied by a reference to the source publication. If a term is defined substantially differently than another widely used publication, CRIS WG will do its best to clarify any such differences.

1.3 DOCUMENT ORGANIZATION

This lexicon includes concept graph(s) to help users understand the relationship among the terms. The concept graph(s) are not normative parts of the lexicon, and are included only to enhance the understanding and use of the terms. Explanatory notes provided with a definition are meant to describe the applicability of the term. The document is separated into sections to facilitate electronic searching and readability.

1.4 UPDATE PLAN AND AVAILABILITY

The CRIS WG has adopted a tiered plan to create and update this lexicon. The first and current version is 1.0, and the version number will be advanced incrementally until the CRIS WG has considered terminology for all the basic activities associated with cyber ranges. To support this tiered plan, this publication will be updated and extended with new terminology periodically as the CRIS WG considers additional areas related to cyber ranges.

The latest released version and latest working version of this lexicon are available from CRIS WG Technical Lead, listed in the "Acknowledgements" section. Any comments and corrections should be directed at CRIS WG Technical Lead or to feedback@tena-sda.org.

2.0 CYBER RANGE TERMINOLOGY

2.1 SUMMARY (NON-NORMATIVE)

A Cyber Range is a type of Range that has a designated set of assets and capabilities to conduct an Event in cyber space. A Range contains a set of assets and capabilities located at one or more sites. A Range has a single Range Manager. A capability may be infrastructure elements (e.g., hardware, networks, etc.), instrumentation, tools (e.g., visualization, traffic generation, etc.), processes, facilities, and/or workforce. A Logical Range provides an interoperable set of networked assets and capabilities through a Secure Interconnection of capabilities within one or more Ranges. An Event is conducted according to an Event Process using Cyber Range Support Tools and infrastructure. The Cyber Range Support Tools and Infrastructure are hardware or software that are not targetable during an Event, and are not considered part of the Event Operating Environment. On the other hand, tools used in Event Operating Environment are targetable, since these tools are considered part of Event Operating Environment.

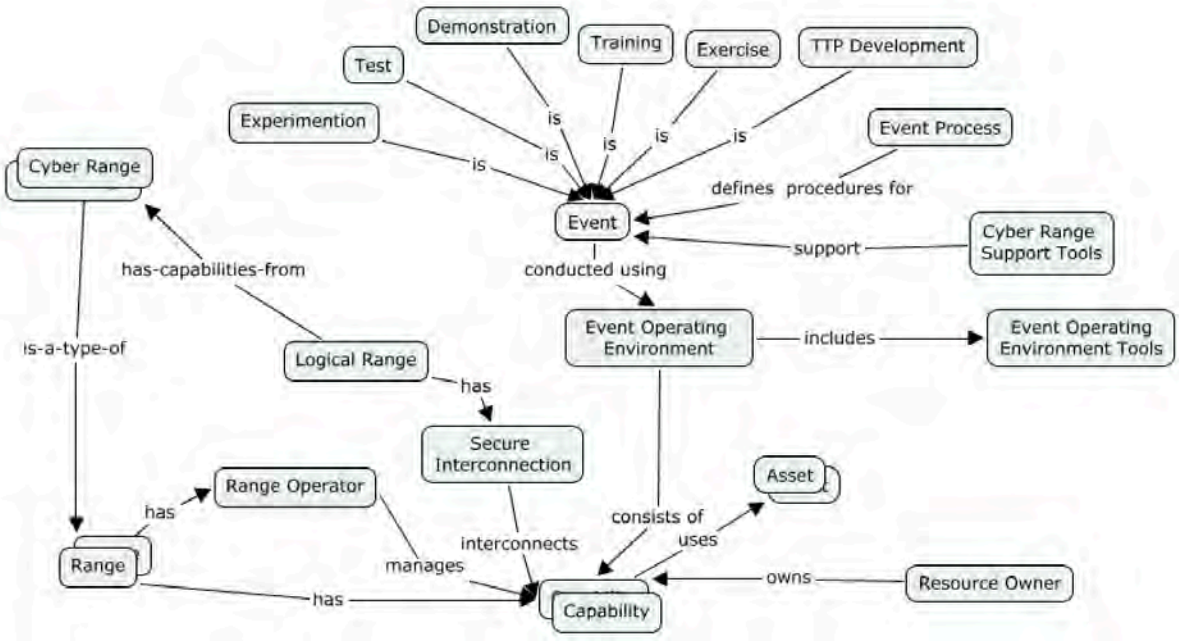

Figure 1: Concept Map of Lexicon Terms (Non-Normative)

2.2 DEFINITION OF TERMS (NORMATIVE)

Asset: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems consisting of hardware, software, instrumentation, infrastructure elements, tools, processes, facilities, and workforce. Source: Adapted from [CNSSI-4009]

Asset Verification: The process of verifying that the Assets deployed in an Event satisfy their respective specifications.

Authorizing Official (AO): A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Source: [NIST.SP.800-53r4]

Background Traffic Plan: The plan that describes the characteristics of the background traffic Simulation. This plan is created during the Planning phase.

Baseline Event Operating Environment: The initial state of the Event Operating Environment for an Event execution. There may be multiple Baseline Event Operating Environments if an Event is executed multiple times with altered initial states.

Blue Team: (1) The group of individuals that represent the U.S. or its allies in a Cyber-Range Event, and either defend against an adversary attack or exploit/attack adversary systems in order to protect Cyber Key Terrain, (2) The group of individuals that conduct vulnerability evaluations of an Event Operating Environment. Source: Adapted from [CNSSI-4009]

Command & Control (C2): The act of controlling the execution of an Event through commands issued during Event Execution.

Capability: A specific service or technique, realized using Asset(s) that addresses a specific need. Capabilities can be integrated with other capabilities in an Event Environment.

Capability Developer: The organization or entity that develops a specific Capability that may be used in an Event.

Checkpoint: The process of creating a snapshot so that an execution can be restarted using the snapshot, if needed.

Cyber Key Terrain (CKT): The physical and logical elements within the Event Operating Environment that enable mission essential warfighting functions. Source: Adapted from [BGJF-2012]

Capability Provider: The organization or entity that provides a specific Capability that may be used in an Event.

Constructive Simulation: See Live, Virtual, and Constructive (LVC).

Control Data: The detailed content of the issued commands and their order and timing during an Event Execution.

Control Data Exchange Model: This model consists of a set of Control Data definitions along with a protocol for exchanging the control data definitions.

Explanatory Notes (Non-Normative): This model may come with a standard software infrastructure for automating the data exchange on the control plane.

Control Environment: The tools and systems used to manage the Event Operating Environment and the actions of human participants on the Event Operating Environment.

Explanatory Notes (Non-Normative): The tools within the Control Environment include the C2 tools for monitoring and managing the progress of MSEL executions. When a traffic generator is used, it is also placed in the Control Environment.

Control Plane: Control Plane includes the people, process, and tools used during the execution phase of an Event to ensure smooth progress of Event Execution by applying Control Data to all the planes, especially to the Event Plane.

Control (Plane) Network: The network that connects the control tools, such as used by the White Team, to the software and hardware used in the event. This is usually a completely separate network from the Event Plane Network so that the control activities do not in any way interfere with Event execution.

Cyber Range: A designated set of assets and capabilities which can be integrated at the appropriate classification levels and controls to conduct research, development, demonstration, testing, or evaluation of military capabilities supported in, through, and from cyberspace, or to train military personnel in conducting cyber operations.

Explanatory Notes (Non-Normative): The assets and capabilities in a Cyber Range may be entirely from a single Range or from multiple Ranges. If the capabilities are from multiple Ranges, they must be integrated into a Logical Range prior to conducting an Event.

Cyber-Range Event (or Event): A planned, controlled, and scheduled set of activities conducted on a Cyber Range to meet specific goals, objectives, or requirements. Events include, but are not limited to, experimentation, test and evaluation (S&T, DT&E, OT&E, LFT&E), Tactics, Techniques, and Procedure (TTP) development, Concept of Operations (CONOPS) development, demonstration, mission rehearsal, training, or exercise.

S&T: Science & Technology

DT&E: Development Testing & Evaluation

OT&E: Operational Testing & Evaluation

LFT&E: Live Fire Testing & Evaluation

Cyber-Range Event Operating Environment (or Event Operating Environment): The combination of representative operational environment elements, including Systems Under Test (SUT), emulations and simulations, and related Event Operating Environment Tools that satisfy the requirements of a specific Event. Examples of representative operational environments are air defense operations centers, battalion command posts, etc.

Cyber-Range Event Operating Environment Tools (or Event Operating Environment Tools): Event Operating Environment Tools are hardware and/or software (e.g., instrumentation, asset emulators, simulators, mission traffic emulators, etc.) that are part

of an Event Operating Environment. An Event Operating Environment Tool may be targeted during Event execution.

Explanatory Notes (Non-Normative): Event Operating Environment Tools are distinguished from the Cyber Range Support Tools in two significant ways: 1) Different Cyber Range Support Tools may be used at different Cyber Ranges. Event Operating Environment Tools (such as scanners) are specified within the Event Operating Environment and are ideally expected to remain the same or provide an equivalent capability no matter where the Event is conducted; 2) Cyber Range Support Tools cannot be targeted during the execution of an Event. In contrast, Event Operating Environment Tools may be targeted.

Cyber-Range Event Process (or Event Process): An established, documented, and repeatable set of procedures, along with entrance and exit criteria, for conducting Events. The Event Process workflow includes but is not limited to event planning, design, configuration, and execution; data collection, data management, analysis, and archiving; and range sanitization.

Cyber-Range Event Support Environment (or Event Support Environment): The combination of Cyber Range Support Tools and infrastructure elements used to support a specific Event, including Control Environment and Instrumentation Environment.

Explanatory Notes (Non-Normative): Cyber Range Support Tool is defined below. The infrastructure elements include the hardware (e.g., servers) and software on which an Event Support Environment is created or instantiated.

Cyber Range Support Tools: Hardware and/or software used to support an Event but are not part of the Event Operating Environment. Cyber Range Support Tools include tools for conducting pre-event execution activities (design, set-up, configuration, site asset management, asset scheduler, range validation, etc.), event execution (health and status monitoring, visualization, etc.), and post-event execution activities (data analysis, after-action reporting, data archive/storage, range sanitization, etc.). A Cyber Range Support Tool must not be targeted during an event execution.

Data Analysis: Analysis of the Event Data in conjunction with the Event Model. This activity includes report generation and is conducted by Event Analysts, and happens in the Post-Execution Phase.

Data Aggregation: The process of collecting event data from multiple sources including Probes and Data Collection Logs for the purpose of monitoring, correlating, and analysis.

Data Archival: The process of compressing and storing event data for the purpose of analysis at a later time.

Data Collection Plan: The plan that describes where, how, and when data should be collected and stored during an Event, specifically during Event Execution, to support calculation of Event Metrics and Data Analysis.

Data Collection Log: Where the event data collected by a Probe is stored. There can be one or more Data Collection Logs associated with one or more Probes.

Deployment Phase: See Event Phase.

Designated Approval Authority (DAA): A Designated Approval Authority is a person responsible for approving the security aspect of a system, a site, a range, or the entire event. This term has been replaced by the term Authorizing Official (AO).

Explanatory Notes (Non-Normative):

There are many DAAs that collaborate on creating and approving the security architecture used in an event. DAAs are designated by either the event sponsor, a site, or a range to authorize aspects of the event to operate at specific security levels in accordance with approved security procedures of the cognizant security agencies (e.g., DIA, DSS, DNI, etc.) They have final approval authority over security plan for their element of the event environment and event cases. They define the security role each cyber range will play in the event based on event plan requirements and each range's capabilities. This typically involves review and contribution to the Interconnect Security Agreement (ISA) that documents a local range's asset, protection levels, and security procedures. The Event DAA adjudicates resource and design conflicts among Range DAAs as needed, and produces the Interconnect Security Agreement (ISA), and obtains approval of the cognizant security agencies.

Demonstration Event: See Event.

Emulation: See Simulation.

Event (or Cyber-Range Event): An Event is conducted in a Logical Range by bringing together people, process, capabilities, and infrastructure to achieve specific objectives whose success can be quantified with key metrics. Examples of types of Event are test and evaluation, training, experimentation, exercise, TTP development, and mission rehearsal.

Explanatory Notes (Non-Normative):

A Test & Evaluation Event is conducted to verify and validate against specific criteria or requirements. An Exercise Event is conducted for the purpose of evaluating operational readiness with the current Tactics, Techniques, and Procedures. A Training Event is conducted for the purpose of training personnel. An Experimentation Event is conducted for the purpose of exploring new hypotheses, or evaluating a hypothesis. A Demonstration Event is conducted to demonstrate a capability to a target audience. A TTP development event is conducted to develop Tactics, Techniques, and Procedures for a mission.

Event Agreement: Event Agreement is a document authored by the Event Coordinator, and signed off by all of the participating sites and physical ranges constituting the Logical Range. The person signing off from each such site/range must have the authority to commit resources. This document also includes basic schedule commitments.

Event Analyst: The individual or organization that defines during the event design phase what data needs to be collected during the execution of an Event, and also analyzes the collected Event Data and produces Event Reports.

Event Architect: The person(s) responsible for designing, implementing and validating an Cyber-Range Event Operating Environment and Cyber-Range Event Support Environment in coordination with the Event Coordinator, and according to the Event requirements.

Explanatory Notes (Non-Normative): The Event Architect must take into consideration performance requirements such as adequacy of bandwidth between distributed sites, potential stress and loading implications due to the Event design, in addition to functional requirements. Event Architect baselines the Cyber-Range Event Operating Environments, and also designs and implements health and status monitoring throughout the cyber event process.

Event Coordinator: The person(s) who coordinate with the Event Architect, Event Director, Event Sponsor, and Resource Owners to ensure the required assets and capabilities are provisioned for an Event.

Event Command and Control Team: This team supports the Event execution, and exists in the Control Plane. The Range Support team and White teams are two components of this team.

Event Data: This is the data that is collected during the execution of an Event, including packets, logs, events, state and status. A portion of this data (defined in the data collection plan—a part of the analysis plan) may be available for real-time analysis. Some data may only be available after execution. This data is defined in the analysis plan and the format is described in the event model and event plan.

Reduced Data: Data that has been created by the post-processing process, which may include summary data and overview of important metrics.

Reusable Data: Data that has been created for generated in an Event that may be of value to future Events. This data may include initialization data, scenario definitions, Event Model definitions, scripts, etc.

Initialization Data: Data that is used to initialize the Event Operating Environment at the start of the Event execution.

Instrumentation Data: Data that is collected using instrumentation over entities in Event Operating Environment. While Instrumentation Data form an important subset of Event Data.

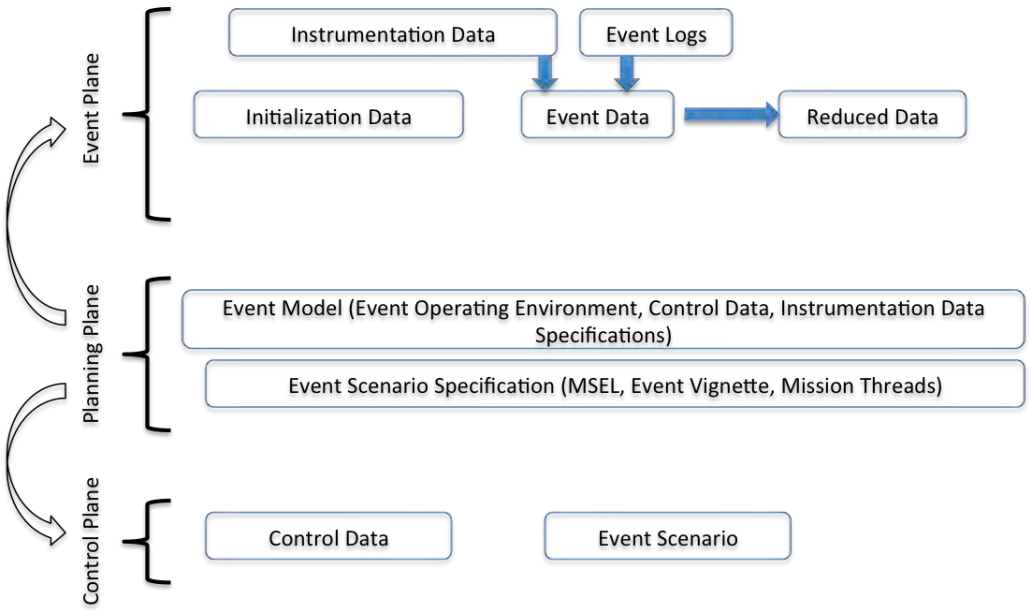

Figure 2: Data View

Event Director: The person is designated by the Event Sponsor to be in charge of all phases of the event. The Event Director has the final approval authority over the technical design of the Event Operating Environment and Event Scenarios. Event Director defines the role each participating Cyber Range in the Logical Range will play in the Event based on Event Engineering Plan requirements and each Cyber Range's capabilities; and delegates the design of the event to the Event Architect and the specific Range Engineers responsible for instantiating the event. The Event Director adjudicates resource and design conflicts among Range Engineers in accordance with each range's role, and approves the final Event Plan Document.

Figure 3: Event Team

Event Engineering Plan (or Event Plan): The Event Engineering Plan, written by the Event Architect and Event Director, describes in detail how the event is going to be executed. The Event Plan includes the event schedule, the Event Environment specification, the Event Scenario specification, the set of Event Metrics to be calculated, the requirements for instrumentation and data storage, and the responsibilities of each range that is part of

the Event. The final Event Plan document is the final version of this document is approved by the Event Sponsor.

Event Environment: A term used to collectively refer to (Cyber Range) Event Operating Environment, (Cyber Range) Event Support Environment, Control Plane elements, and Instrumentation Plane elements.

Event Execution: The execution of the Event Scenarios during the Execution Phase.

Event Goal: See Event Objective.

Event Metrics: Metrics for the Event such as Measures of Effectiveness (MOE), Measures of Performance (MOP), and Measures of Survivability (MOS), Key Performance Indicators (KPI), or Critical Success Factors.

Event Model: A precise specification of Event Operating Environment, Control Data, and Instrumentation.

Event Objectives (or Event Goals): The objectives of an Event as specified by the Event Sponsor.

Event Operating Environment: See Cyber-Range Event Operating Environment.

Event Phase (or Phase): A Cyber-Range Event Process consists of four phases: Planning, Deployment, Execution, and Post-Execution. Some or all of these phases may be iterated through or activated multiple times in a single Event.

Planning Phase: To begin this phase, requirements for the Event are defined by the Event Sponsor. Subsequently, the Event Team clarifies these requirements, designs the Event, and creates the Event Engineering Plan. All the artifacts necessary for the subsequent Event Phases are created in this phase.

Deployment Phase: In this phase, the assets and capabilities are acquired, verified, deployed, configured, and validated. All necessary preparations to execute the Event, including deployment of the Control Plane and Instrumentation Plane happen in this phase.

Execution Phase**:** In this phase, the Event is executed over the Event Operating Environment, monitored, and Event Data is collected and saved for future data analysis. Some Events may have multiple Event Execution Phases in parallel, or in series.

Post-Execution Phase: In this phase, Event Data is analyzed and the Logical Range is sanitized. Optionally, the Logical Range, and the constituent Physical Ranges are also dismantled. The Data Analysis activity may happen long after the Event Execution Phase.

Event Plan: See Event Engineering Plan.

Event Plane: Event Plane includes the entities in Event Operating Environment. The Blue Team and the Red Team operate in the Event Plane. The Event Plane is always separate from the Planning Plane. In many situations, the Event Plane is also separated from the Control and Instrumentation Planes.

Event Plane Network (or Event Network): This network exchanges all the information generated within the Event Operating Environment. The Event Network is used to exchange cyber information, attacks, defenses, background traffic, etc. This also may be the

"network under test" itself. In a tactical environment this network contains all the tactical messages. In a simulation environment this network contains all the simulation state and event messages.

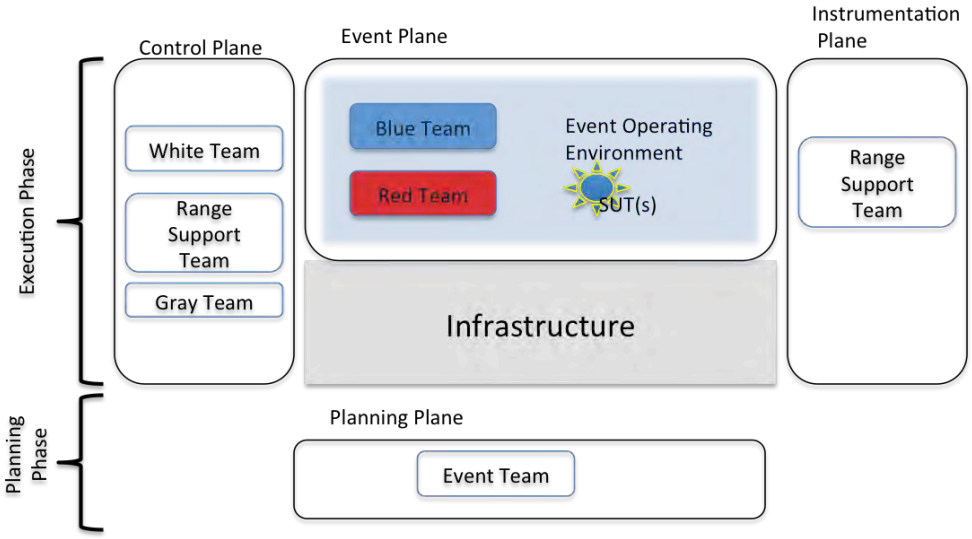

Figure 4: Planes and Teams

Event Plane Team: This team has participants in Event Scenarios, and these participants interact with the Event Operating Environment during Event Execution. The Event Plane Team consists of two separate teams: the Red Team and the Blue Team.

Event Reports: Reports generated in the Post-Execution phase such as the Final Event Report, After Action Report, Fact Sheet, Take Home Package, and the Quick Look Report.

Event Requirements Document: This document defines the Event Sponsor's needs in terms of operational, technical, and mission requirements, metrics, and event objectives to be achieved, questions to be answered, conclusions to be drawn, and constraints on the event.

Event Scenario: A "scenario" for a cyber event is the planned sequence of actions and events that must take place during the event execution in the Event Plane.

Explanatory Notes (Non-Normative):

The Event Scenario description includes relevant operational organizations, resources, missions, and threats that will interact with the SUT(s). The Event Scenario provides insight into what operational entities are required and how they interact as an Event is executed. Any operational constraints imposed by requirements should be specified, such as organization behaviors and rules of engagement. An Event Scenario can be specified in the form of a Master Scenario Event List (called the MSEL). An Event Scenario consists of a set of Mission Threads that may be constrained by Event Vignettes.

Event Sponsor: The organization(s) or designated person(s) funding and specifying the goals, objectives, or requirements of an Event.

Event Team: The personnel (such as the Event Architect, Event Director, Capability Provider) assigned to an Event and responsible for executing the Event under the direction of the Event Director.

Explanatory Notes (Non-Normative): The Event Team does not include human role players or agents or proxies; they are referred to as capabilities.

Environment Validation: The process of ensuring that the Event Environment to be deployed, or already deployed, satisfies the functional and non-functional requirements in Event Requirements document. The functional requirements may include specific Asset type requirements, and connectivity needs. The non-functional requirements may include specific performance needs.

Event Vignette: See Mission Thread.

Execution Phase: See Event Phase.

Exercise Event: A military maneuver or simulated wartime operation involving planning, preparation, and execution that is carried out for the purpose of training and evaluation. Source: Adapted from [JP 1-02]

Experimentation Event: See Event.

Final Event Report: This report assesses the actual event execution in comparison with the event plan. Any data collection problems are documented and the results of the quick-look assessments and analysis goals are documented. Conclusions are drawn based on the collected event data understood according to the principles, metrics, and objectives elucidated in the analysis plan.

Force Action Verification: White Cell confirmation that the Blue and Red Force actions and reactions conform to the MSEL.

Green Team: See Range Support Team.

Gray Team: In some events, these teams conduct non-malicious activity, but do not play an offensive or defensive role. Gray teams may include operators creating realistic network communications/traffic, and providing, often high fidelity, simulations within the Event Plane. This role may be automated through the use of traffic generators, and in such situations the operators of the traffic generators are included in the Gray Team.

Health and Status Monitoring: Confirming that the support infrastructure for event execution is operating within the established configuration specifications.

High-Level Scenario: A description of the vignettes and/or mission threads of the event in the customer's operational terms and generally without regard to how the scenario will be implemented.

High-Level Schedule: This schedule gives high-level guidance on when the activities and steps are performed, including time lines, and milestones.

Initialization Data: See Event Data.

Instrumentation Data: See Event Data.

Instrumentation Environment: This environment includes the probes and other instruments aimed at collecting data from the entities in the Event Operating Environment, data collection systems, data pre-processing systems, and data archival systems.

Instrumentation Plane: The Instrumentation Plane includes the people, process, and environment used for instrumenting, i.e., installing probes, and collection of data from the Event Operating Environment.

Instrumentation (Plane) Network: This network is used to collect data from instrumentation attached to the computers and software participating in the event. This network is conceptually distinct from the others so that the data collection process (from instrumentation) can be done without interfering with the cyber event itself. The Instrumentation Network may be logically and physically separate from the Control and Event Networks to prevent any impact to Event execution and its control due to the instrumentation and data collection.

Instrumentation Team – The Team responsible for the probes, and the data collection process. This team may also deploy real-time monitoring tools to support the White Cell in specific aspects such as shot validation. This team is also responsible for archiving the data collected.

Joint Exercise Control Group: White Cell is called Joint Exercise Control Group in some exercises. Provides all administrative command and control for a given training event. The Joint Exercise Control Group provides control functions during exercise execution to manage and synchronize event scenarios (MSELs), conduct observation and data collection of event and team performance, and record observations, lessons learned, and identifies issues for after action reporting. The Joint Exercise Control Group coordinates efforts and provides overall control of the exercise, monitors and controls exercise execution, and provides ground truth and real-time feedback. Adapted from [UST-36-36]

Lessons Learned Document: This document provides insight into the relative merits of any implementation and configuration options explored in the event. It also describes any problems encountered in the planning and execution of the cyber event and, from hindsight, describes how the event could have been better constructed.

Live Simulation: See Live, Virtual, and Constructive (LVC).

Live, Virtual, and Constructive (LVC) Cyber: A term used to qualify a simulation or assets that support Live, Virtual, and Constructive cyber simulation.

Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. Source: [DMSO] (Defense Modeling and Simulation Office)

Simulation**:** A method for implementing a Model over time.

Emulation: Simulation of a Model that accepts the same inputs and produces the same outputs as a given system. Source: [SISO-REF-002-1999]

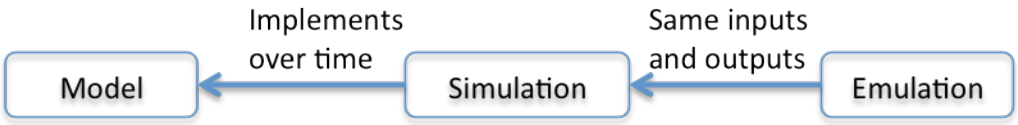

Figure 5: Simulation, Emulation, and Model

Live Cyber Simulation: In this type of simulation, real-world Assets operate on/with real-world systems and protocols. These Assets are vulnerable and reachable by attacks, exploits, and performance degradation from the physical, electromagnetic, and/or digital domains. Even though real-world Assets are used, these are considered simulations because the scenario is simulated and attacks are not conducted against a live enemy.

Examples:

- Actual operators, actual network devices, actual machines, actual non-emulated/simulated software
- Packet, protocol, or frequency level attack and response launched by actual systems and/or live attackers

Virtual (Cyber) Simulation: In this type of simulation, actual Assets may interact with simulated or emulated systems, and simulated or emulated Assets may interact with actual systems. When actual Assets interact with protocol-level fidelity representations of real-world systems, where ease of (re)configuration, replication, restoration and physical limitations make a virtual system preferred over the live one, there is no physical representation of the real-world system, so a virtual system only provides a cyber "attack surface," i.e., protocol/packet interfaces are provided, but not asset internals susceptible to non-cyber attacks.

Examples:

- Asset emulators running on virtual machines
- Automated response of a virtual machine to an attack
- Replay of a logged live attack onto the live or virtual systems
- Automated or semi-automated attack simulators that replicate the actions of a live red team or real world threat
- Simulated users (Assets) in a traffic generator using actual systems to generate traffic
- Accurate (high-fidelity) representations of sysadmin GUIs

Constructive (Cyber) Simulation: In this type of simulation, simulated or emulated Assets interact with parameterized simulated or emulated systems. The simulated systems are not vulnerable to direct live or virtual exploits and manipulation; characterized by lower fidelity global/enterprise-level networks and effects representations.

Examples:

- Simulated internet-scale traffic generation, background noise and high-volume grey-space
- Virus infection & worm propagation simulations
- Asset representations with simulation interfaces that must be translated or bridged to connect with virtual and live assets

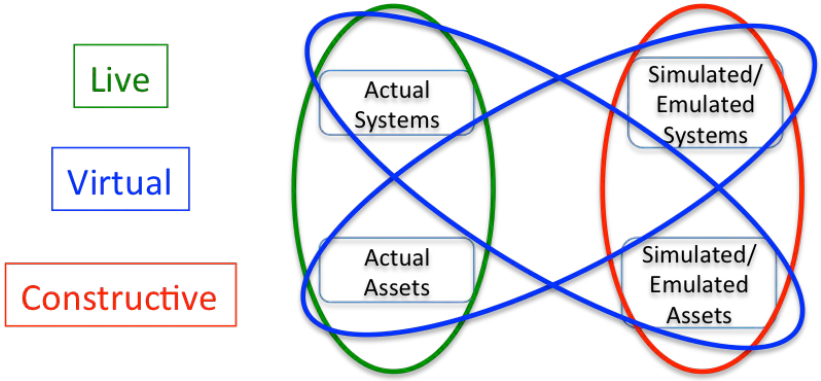

Figure 6: Live, Virtual, Constructive Simulations (Non-Normative)

Notes:

1. Emulation may go beyond input-output matching, and could also include partial or complete cyber representation of internals of a system.
2. Actual Assets may also interact with simulated systems in a constructive simulation to provide Control Data, at the start, or during Simulation. Actual Assets may change parameters to such simulations, but are not involved in determining the outcomes.
3. A simulated or emulated Asset may also be an Agent that embodies the behavior of a human.

Logical Range: A designated set of interoperable assets and capabilities within one or more ranges interconnected through a Secure Interconnection. A Logical Range provides isolation to the Event Environment to prevent accidental interactions with entities outside the Logical Range.

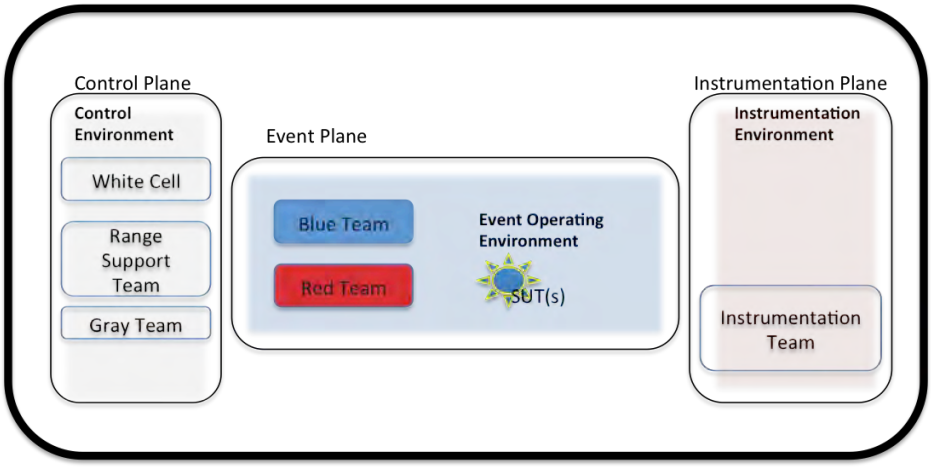

Figure 7: Logical Range

Explanatory Notes (Non-Normative):

1) Logical Range (LR) may have attributes such as security levels as requirements. LRs may be able to operate at multiple classification levels (e.g., *Multiple Independent Levels of Security)*, compartments, and releasability levels, and are established by Range Manager *without the specific knowledge or awareness of* any adjacent site, users or event activities.

2) When capabilities from only one Cyber Range are used to conduct an Event, a de facto Logical Range may be created to provide sufficient isolation. In this case, Secure Interconnection refers simply to the connection and isolation of capabilities within that Range. Please refer to Fig. 8, below.

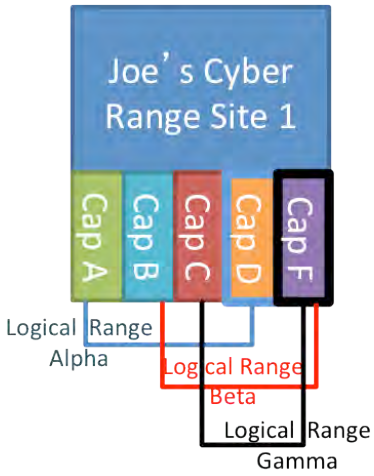

Figure 8: Logical Ranges at a Single Site

3) Isolation of a Logical Range through Secure Interconnection also enables simultaneous execution of Events in multiple LRs, either in a single Cyber Range or across multiple Ranges. Please refer to Fig. 9, below.

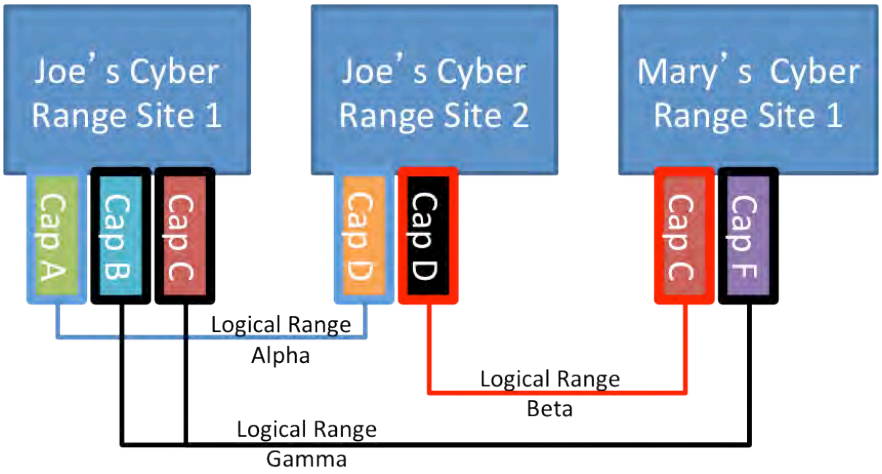

Figure 9: Logical Ranges from Multiple Sites and Multiple Ranges

Mission Rehearsal Event: See Event.

Master Scenario Event List (MSEL): MSEL guides an exercise or training event toward specific outcomes by defining a sequence of time or dependency ordered Mission Threads. MSELs specify desired outcomes for focused observation, analysis, and debrief and reporting. Source: Adapted from [CJCSM 3500.03]

Explanatory Notes (Non-Normative):

A MSEL corresponds to the flows in a Use case, whereas an Event Scenario corresponds to a Use Case.

Mission Thread: A Mission Thread defines a subset of Event Scenario that occurs within the constraints of one or more Event Vignettes. A Mission Thread typically begins with a Cyber Network Attack (CNA), or Cyber Network Defense (CND) activity, and ends with battle damage assessment.

Event Vignette: Event Vignettes are subsets of the overall Event Scenario. Each vignette is focused on one or more Event Goals or Objectives. An Event Vignette consists of one or more Mission Threads.

Explanatory Notes (Non-Normative):

1. Using an analogy, a vignette is a scene and the scenario is the movie or play. Each vignette will be comprised of sets of combinations and event conditions, i.e., controlled variables (or factors) under which the event systems and participants will be subjected to a event trial or set of event trials to measure system performance and Joint Mission Effectiveness (JME).

2. Figure 10 describes three Mission Threads in an Event Scenario. Each of the Mission Threads may be executed under constraints imposed by different Event Vignettes at different times. Three Event Vignettes, EV1, EV2, and EV3 are shown in the diagram.

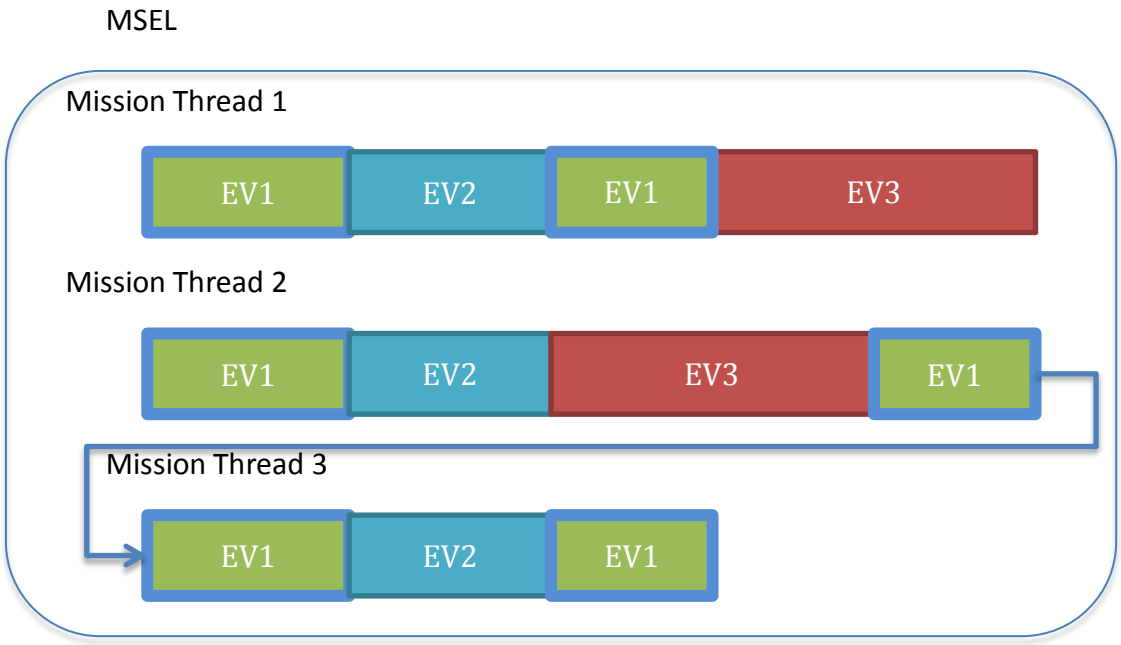

Figure 10: MSEL, Mission Thread, and Event Vignette

MSEL: See Mission Scenario Event List.

Phase: See Event Phase.

Planning Phase: See Event Phase.

Explanatory Notes (Non-Normative): This phase answers the following questions (not all inclusive): What resources are required? What resources are available? What can be emulated? What requires actual physical devices? Will external resources be required? Is an appropriate security plan in place? What needs to be instrumented? Will the instrumentation add any test artifacts? Are those artifacts acceptable or are there alternative methods? What risks are involved?

Planning Plane: Planning Plane includes the people, process, and infrastructure used for the planning phase of an Event.

Planning Network (or Planning Plane Network): Network where planning tools and planning information are stored and exchanged, and planning processes are executed by Event Participants in the Planning Phase of an Event. The Planning Network is always separated from the Control, Instrumentation, and Event Networks.

Post-Execution Phase: See Event Phase.

Probe: Hardware or software sensor deployed to collect event or infrastructure data.

Quick Look Report: These reports are the result of rapid and mostly cursory analysis of event activities in real-time or near-real-time. The information content and format of the quick-look reports is specified in the analysis plan. These reports are generally based on monitoring "health and status" indicators and identifying anomalies of event execution.

Range: A Range contains a designated set of assets and capabilities located at one or more sites and is managed by a Range Manager.

Range Engineer: Individuals who monitor, manage, operate, and/or create hardware, software, or networking elements of a cyber range for the purpose of engaging in a cyber event. Range Engineers are not in the Event Plane.

Range Manager: The organization that manages and operates a Range. A Range Manager manages assets and capabilities that may be used to conduct an Event that is owned by it or provided by other Resource Owners. A Range Manager also manages physical security, physical access, equipment maintenance, and decides what events to dedicate its ranges capabilities to, besides defining and managing all processes required to operate the range.

Range Support Team: These individuals operate the range infrastructure and support tools systems. Range Engineers are part of the Range Support Team. This team is also sometimes referred to as "Green Team."

Red Team: An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. Red Team is in the Event Plane. Also known as a Cyber Opposition Force (OPFOR).

Reduced Data: See Event Data.

Resource Owner: The organization that owns and makes available assets and capabilities that may be used to conduct an Event.

Explanatory Notes (Non-Normative): In most cases, the Range Manager also owns the assets and capabilities used in Events, and thus, the Resource Owner and the Range Manager are the same.

Reusable Data: See Event Data.

Rules of Engagement (RoE): Directives issued by the White Cell that delineate the circumstances and limitations under which Red and Blue forces will initiate and/or continue to operate. Source: Derived from [JP 1-04].

Secure Interconnection: A self-contained and unique interconnection of capabilities from one or more Ranges to provide an end-to-end networked environment with adequate physical, geographical, logical, or cryptographic isolation. Such isolation permits the creation of a secure and contained environment that can be accredited by appropriate authorities.

Explanatory Notes (Non-Normative):

1) A Secure Interconnection defines the secure and isolated boundary within which an interconnection of capabilities exists.

2) A Secure Interconnection supports the interconnection of capabilities across multiple sites or within the same site.

3) Logical isolation does not necessarily require physical isolation, and the same hardware may support multiple Secure Interconnections.

Security Engineer: An individual who will monitor, manage, configure the security devices and controls associated with the Event.

Shot Validation: The process conducted by the White Cell to confirm a deployed cyber capability had the intended effect.

Snapshot: A storable image of the current event execution state. An "event snapshot" refers to a snapshot of an event execution.

(Synthetic) Traffic Generation: Sustained creation of synthetic traffic in the Event Operating Environment during Event Execution.

SUT: System(s) Under Test (e.g., technology, network, personnel, processes) that may be evaluated through an Event.

Explanatory Notes (Non-Normative): SUT may include threat targets, instrumentations, Environment Tools, or other types of systems, procedures, methodologies, or personnel that are the subjects of study or training in a cyber event.

Take Home Package: This document provides all the information generated during the event that the Event Sponsor needs to continue their work. For an Event, the take home package could represent the entire contents of the collected data. For a training event, the Take-Home Package represents that information, described by training doctrine, that the training audience brings back to their home station to reinforce the training received during the exercise.

Test-bed: A term sometimes used to refer to a Logical Range at a single site in a testing or experimentation event.

Test & Evaluation Event (or T&E Event): See Event.

TTP Development Event: See Event.

Training Event: An event that focuses primarily on improving individual or collective ability of a team to perform. Training events are less focused on evaluation than Exercise Events. Source: Adapted from [JP 1-02].

Vignette: See Mission Thread.

Virtual Simulation: See Live, Virtual, and Constructive (LVC) Simulation.

White Cell/Team: This team is responsible for administrative management (command and control), monitoring of an Event for compliance, and assessment of the performance of the event and teams. This team is usually given the power to influence execution of event scenarios (MSEL) and or make modifications to execution. Also see Joint Exercise Control Group for exercise events.

2.3 REFERENCE DOCUMENTS

[BGJF-2012] B.G.J. Franz III, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," 14 August 2012. [Online]. Available: http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtW arfighter_forpublicrelease.pdf

[CJCSM 3500.03] Chairman of the Joint Chiefs of Staff, "The Joint Training System: A Guide for Senior Leaders," CJCS Guide 3501, 8 June 2012

[CNSSI-4009] Committee on National Security Systems, "CNSS Instruction No. 4009: National Information Assurance (IA) Glossary," April, 2010

[DMSO] DoD Modeling and Simulation (M&S) Glossary, March 2010

[JP 1-02] Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," 15 December 2014

[JP 1-04] Joint Publication 1-04, "Legal Support to Military Operations," August 2011

[SISO-REF-002-1999] D.C. Gross, "Fidelity Implementation Study Group Report," Spring Simulation Interoperability Workshop, Orlando, FL, March 1999. [Online]. Available: http://www.sisostds.org

[NIST.SP.800-53r4] National Institute of Standards and Technology, "NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations," April 2013

[UST-36-36] United States Transportation Command, "USTRANSCOM INSTRUCTION 36-36," 21 November 2012

3.0 ACKNOWLEDGMENTS

The CRIS WG acknowledges the contribution of the following individuals in the creation of this version of this document. In addition, the CRIS WG also acknowledges several reviewers across many organizations for improving the quality of this document.

CRIS Working Group Chairperson:

Mr. Arjuna Pathmanathan – Test Resource Management Center (TRMC)

CRIS Working Group Technical Lead:

Dr. Suresh K. Damodaran (MIT Lincoln Laboratory)

Document Editors:

Dr. Suresh K. Damodaran (MIT Lincoln Laboratory)

Ms. Kathy Smith (GBL Systems Corporation)

Contributors:

Mr. Mark A. Bradbury (Raytheon)

Mr. Bernie Clifford (Sandia National Laboratory)

Ms. Laura E. Feinerman (MITRE)

LTC Brian Hittner (JS J7)

Mr. Patrick Lardieri (National Cyber Range (NCR)/Lockheed Martin)

Mr. Scott M. Lewandowski, (National Cyber Range (NCR)/The Wynstone Group)

Dr. Katherine L. Morse (Johns Hopkins University Applied Research Laboratory)

Dr. Edward Powell (Test and Training Enabling Architecture (TENA)/Leidos)

Mr. Zachary Weber (MIT Lincoln Laboratory)

Mr. Mike Wee (Cyber Test & Evaluation (T&E) Support Cell, TRMC/Northrop Grumman)

Dr. David “Fuzzy” Wells (USPACOM)

Mr. Bennett Wilson (NAVSEA GOV – CDSA, Damneck)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10 November 2015	Technical Report	

4. TITLE AND SUBTITLE

CRIS Cyber Range Lexicon Version 1.0

5a. CONTRACT NUMBER
FA8721-05-C-0002

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. Suresh K. Damodaran, MIT Lincoln Laboratory (Editor)
Ms. Kathy smith, GBL Systems Corporation (Editor)

5d. PROJECT NUMBER
1553

5e. TASK NUMBER
273

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

MIT Lincoln Laboratory
244 Wood Street
Lexington, MA 02420-9108

8. PERFORMING ORGANIZATION REPORT NUMBER
59-0001

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Test Resource Management Center
3000 Defense Pentagon
Washington, DC 20301-3000

10. SPONSOR/MONITOR'S ACRONYM(S)
TRMC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Numerous organizations have created tailored processes for conducting cyber-range events. Such events may require, in addition to cyber, integration with kinetic and networked infrastructure assets and capabilities. Several kinds of tools have been designed and used in these events. The variety of tools have made the process of conducting events longer and more expensive than necessary due to semantic and syntactic mismatches among the myriads of tools used.

Cyber Range Interoperability Standards Working Group (CRIS WG) was founded in 2012 to identify the requirements, and to recommend the standards necessary to accomplish the goals stated above. The CRIS WG consists of cyber-range practitioners from government, industry, and academia and is sponsored by the Department of Defense (DoD) Test Resource Management Center (TRMC). The CRIS WG is open to all participants from the United States Government or its contractors who conduct or support cyber-range events currently, or plan to do so in the future. Communities supported by the CRIS WG include, but are not limited to, Science & Technology (S&T) experimentation, Developmental and Operational Test and Evaluation (DT&E, OT&E), cyber force training, and mission rehearsal.

To facilitate discussions among these related communities, the CRIS WG is establishing a common cyber-range lexicon. This document contains the current version of this lexicon. This publication supplements standard English-language dictionaries and standardizes cyber range and associated terminology to improve communication and mutual understanding of cyber range activities within the DoD, and possibly with other federal agencies of the United States and its allies.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Suresh Damodaran
Unclassified	Unclassified	Unclassified	Same as report	24	19b. TELEPHONE NUMBER *(include area code)* 781-981-8457

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18