The Cyber Range: A Guide

Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training

Prepared by the National Initiative for Cybersecurity Education (NICE)
Cyber Range Project Team

The Cyber Range: A Guide

Table of Contents

Executive Summary 3

Purpose 3

- Approach 4
- Audience 4

Problem Definition 4

- Why are Cyber Ranges Necessary? 4
- Who needs a Cyber Range? 5

Features of a Cyber Range 6

- *Technical Components* 6
  - **Range Learning Management System** 6
  - **Orchestration Layer** 7
  - **Underlying Infrastructure** 7
  - **Virtualization Layer** 8
  - **Target Infrastructure** 8
- *Realism & Fidelity* 8
- *Accessibility & Usability* 9
  - **Location** 9
  - **Sophistication** 9
- *Scalability & Elasticity* 9
- *Curriculum & Learning Outcomes* 10
  - **Cyber Range Curricula** 10
  - **The NICE Framework** 11
  - **The NSA/DHS CAE Knowledge Units** 12

Types of Cyber Ranges 12

- Simulation Ranges 12
- Overlay Ranges 13
- Emulation Ranges 13
- Hybrid Ranges 13

Summary & Conclusion 14

Executive Summary

Cybersecurity is a twenty-first century challenge requiring a twenty-first century workforce. The current cybersecurity workforce lacks sufficient professionals with the skills, training and credentials to meet this cutting-edge challenge. Market studies predict that this talent and skills gap will continue to widen among current and prospective cyber professionals over the coming years. This cybersecurity workforce gap presents tremendous risk to business, government and society.

A key tool and platform for reducing the skills gap and securing society is the cyber range. Cyber ranges are interactive, simulated platforms and representations of networks, systems, tools, and applications. Cyber ranges can:

- Provide performance-based learning and assessment
- Provide a simulated environment where teams can work together to improve teamwork and team capabilities
- Provide real-time feedback
- Simulate on-the-job experience
- Provide an environment where new ideas can be tested and teams can work to solve complex cyber problems

This document first defines cyber ranges and explores key use cases. It then outlines the approach the project team took to define cyber range audiences, capabilities and features. Finally, the paper describes several current cyber range types and summarizes a criteria checklist for use in cyber range selection.

Purpose

Cybersecurity professionals require hands-on and specialized education and training. The cyber range is a valuable tool and catalyst to be utilized in these efforts. This document describes the capabilities and features found in the cyber range models and implementations.

Providing these descriptions of cyber range platforms is intended to enable an informed comparison of the offerings in a way that will allow educators, users, or organizations to more confidently explore their options when seeking a “best fit” cyber range for their needs. The document does not assert a scoring or ranking system for any of the features described, nor does this document provide recommendations relative to a particular platform, product, or vendor.

The value of this document centers on the exploration and analysis of the various technologies and methodologies deployed by cyber ranges as the diversity of their use and specifications continue to grow within the ecosystem of cybersecurity training, education, and workforce development. This document aims to be a reference resource about the key capabilities and features found in cyber ranges.

Approach

The efforts of the Cyber Range Working Group began with the task updating the sole NIST Cyber Range one-page document and further defining a taxonomy that describes cyber ranges. After several meetings and much discussion, this task expanded to creation a guidance document that would provide cyber range users the various features and capabilities by which to evaluate which range type and functionality best suits their needs. This task now also includes the creation of a formal checklist for potential users to deploy in their efforts relating to cyber range search and selection.

Audience

A goal of this document is to provide actionable guidance to individuals and organizations -- including governments, for profit and not for profit entities -- looking to close the cybersecurity workforce gap by engaging, implementing, or utilizing a cyber range. Here are potential audiences for cyber ranges and this document:

- Educators seeking curricula and/or infrastructure for hands-on exercises;
- Individuals seeking workforce training and continuing education;
- Organizations seeking training, skills validation, or range exercises;

While the generalized list above is not exhaustive, it provides a basic framework by which to view the problems cyber ranges seeks to solve and potential use cases of value for cyber range stakeholders.

Problem Definition

Why are Cyber Ranges Necessary?

Organizations or individuals seeking cybersecurity education, workforce development, training or skills face a dearth of simulated environments like those found in professional fields like aerospace, business or medicine. Compounding this challenge for the cybersecurity profession include a multitude of factors, including but not limited to: the realism of training, the legality of potential training exercises, the capabilities of training platforms, the customizability of training methods, the accessibility of training environments, and the scalability of training models.

Cyber ranges are interactive, simulated platforms and representations of networks, systems, tools, and applications. They typically provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security-posture testing. Cyber ranges can and must play a central role in facilitating and fostering cybersecurity education, training and certification. These critical tools may include actual hardware and software or may be a combination of actual and virtual components. This document will detail the function and utility of cyber ranges for academia, business and government in addressing the cyber workforce gap that plagues them.

Who needs a Cyber Range?

Individuals or organizations seeking to implement, purchase, or utilize a cyber range must first understand their own purpose and objectives. The table below outlines the potential but not exhaustive list of cyber range use cases --

	Cyber Range Use Cases
1	Educators seeking to implement basic and advanced cybersecurity education courses and curricula
3	Organizations or individuals seeking training and continuing education for security operations, analysis, and forensic specialists
4	Organizations seeking “situational operations” testing for new products, software releases, and organizational restructuring
5	Organizations or individuals seeking cybersecurity skills validation to evaluate candidates for cybersecurity positions
6	Individuals seeking workforce training for people moving into cybersecurity-related fields and positions

These use cases could serve a number of potential objectives: improving individual and team knowledge and capabilities from diverse groups; applying knowledge in a simulated network environment, developing cyber skills, working as teams to solve cyber problems, preparing for cyber credentialing examinations or assessments; evaluating cyber capabilities, testing new procedures, and training teams on new organizational and technical environments and protocols.

Features of a Cyber Range

Conventional education and training models are insufficient to fill the cybersecurity skills gap. Cyber ranges provide enabling technology to operationalize, predict, and monitor the training and performance of cybersecurity professionals. Cyber ranges instill confidence in cybersecurity workforce seekers and cybersecurity workforce employers that training will predict job success. This section of this guide identifies the critical features of cyber ranges as catalysts in closing the cybersecurity workforce skills gap, including: technical components, realism & fidelity, accessibility & usability, scalability & elasticity, and curriculum & learning outcomes.

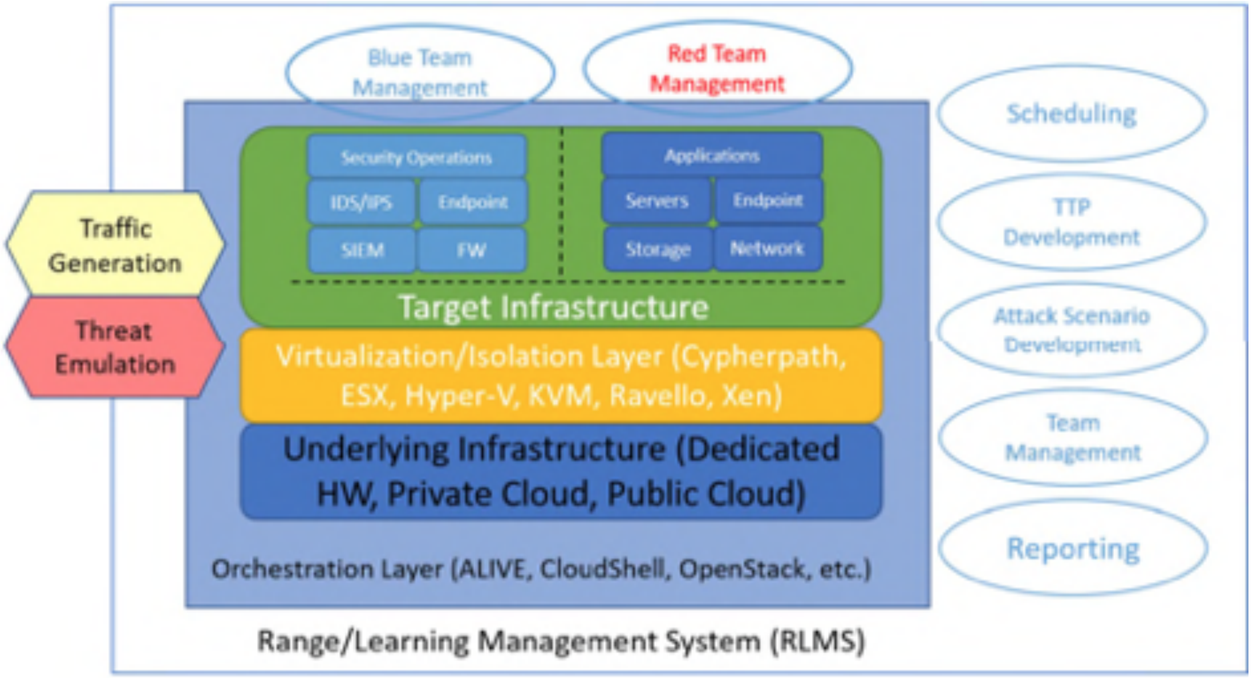
Technical Components

Cyber ranges have many moving parts, but the essential core technological components include –

Range Learning Management System

A central feature for many cyber ranges is the range learning management system. As the name suggests, a range learning management system (RLMS) contains the standard features of an LMS and the unique characteristics of a cyber range.

The diagram below illustrates both the technical components of a range combined with several RLMS features.


Blue Team Management
Red Team Management
Scheduling
TTP Development
Attack Scenario Development
Team Management
Reporting
Traffic Generation
Threat Emulation
Security Operations
IDS/IPS
Endpoint
SIEM
FW
Applications
Servers
Endpoint
Storage
Network
Target Infrastructure
Virtualization/Isolation Layer (Cypherpath, ESX, Hyper-V, KVM, Ravello, Xen)
Underlying Infrastructure (Dedicated HW, Private Cloud, Public Cloud)
Orchestration Layer (ALIVE, CloudShell, OpenStack, etc.)
Range/Learning Management System (RLMS)

Orchestration Layer

Taking input from the RLMS, the orchestration layer pulls together all the technology or service components of the cyber range. Many cyber ranges use an in-house developed orchestration layer.[1] Some ranges utilize a commercial product for this layer.[2] The orchestration layer can provide "the special sauce" of cyber ranges because it facilitates the meshing of the underlying infrastructure, virtualization or isolation layer, and the target infrastructure. This layer also enables dynamic cyber range extensibility that supports public cloud, private cloud, and dedicated hard wire infrastructures.

Underlying Infrastructure

All cyber ranges are on top of an infrastructure of network, servers, and storage. Some dedicated ranges are built directly on top of physical infrastructure (switches, routers, firewalls, endpoints, etc.) in a rack, though this is typically expensive and not scalable. For scalability, cost, and extensibility reasons, many range providers are shifting to software-defined virtual infrastructure.[3] Infrastructure drives the realism or fidelity of the

[1] In-house orchestration layers are often based on OpenStack.

[2] For example, Quali's CloudShell.

[3] This shift would likely including standardizing on Open vSwitch as the virtual switch with OpenFlow as the management protocol.

cyber range. In addition, a determining factor around infrastructure selection and use centers on how much legacy hardware or software must the cyber range support to meet the client's use cases. In addition, and though not exactly part of the underlying infrastructure, many cyber range employ use-cases that require traffic generation and attack emulation.

Virtualization Layer

Most cyber ranges look to some level of virtualization to shrink the physical footprint. Here are two general approaches: hypervisor-based solutions and software defined infrastructure. Regardless of the virtualization approach, the level of disintermediation between underlying physical infrastructure and target infrastructure affects the realism of the cyber range due to unwanted and unpredictable jitter and latency. On the other hand, economically viable cyber ranges would not be possible without this virtualization layer. It also acts as a firewall between the target infrastructure (with associated attack vectors) and the underlying infrastructure (dedicated, public cloud, private cloud).

Target Infrastructure

The target infrastructure is the simulated environment in which students train. Based on the use case, the target infrastructure can in some cases match the student's real-world IT and security infrastructure. Advanced cyber ranges contain profiles of commercially available servers, storage, endpoints, applications, and firewalls. Based on student interaction, the RLMS will generate scripts to instruct the orchestration layer to create the target infrastructure. These scripts might include client-specific configuration information including IP Address ranges, routing information, server stacks, and endpoint software.

Realism & Fidelity

The accuracy with which the cyber range represents the real world is important to developing predictive operational and learning outcomes. A high-fidelity simulation does not always mean a real-world simulation. In general, emulation may create a more realistic environment with high fidelity (both operational and functional), but simulation is often a more practical option. In other words, individuals and organizations must find a balance among three competing interests – cost, practicality, and reality. Teaching or training individual skills may even benefit from a less realistic scenario to allow the trainer and student to focus on the skill to be mastered. Integrating that skill into more realistic environments can come later in the training cycle.

Accessibility & Usability

Another central question around the capabilities of a cyber range depends on how users access the features of or gain access to the activities of the range. Accessibility and usability can largely be divided into two categories: location and sophistication.

Location

The answer to this question centers largely on whether the deployed range platform is either an on-premises or cloud-based solution. Users, instructors and range owners must all understand how and under what circumstances they can access the range technology and applications. For example, for educators, it should be understood how access differs at the school, county and state levels. In addition, how can the selected location, whether on-premises or via the cloud, be impacted by bandwidth issues. If range environments are internet-accessible, client hardware and software requirements are also a consideration. Some remote virtualization solutions require the installation of client-side software while others can be accessed via a web browser.

Sophistication

The question of accessibility also requires analysis relative to the sophistication of the users. Cyber range owners must understand the amount of effort necessary relative to installation, use, and implementation. Operators, trainers and faculty members must understand the modules, levels and tools within each platform or system.

Scalability & Elasticity

Scalability refers to the ability of the cyber range to support the target population of the system. Elasticity refers to the time required to increase capacity to support additional users. Ideally, a range is able to simultaneously support its entire potential user population and can increase capacity to support additional users immediately (or nearly so) upon request. Cyber ranges that rely on local hardware infrastructure are limited by the amount of RAM and hard drive space supported on the available hardware. These ranges can only scale to the point where local resources are exhausted, and they tend to be very inelastic; increasing capacity to support users beyond the provisioned capacity requires purchase and configuration of new hardware and software. This can take weeks or months. Public cloud-based ranges should generally scale extremely well because they can leverage additional cloud provider systems upon request. They can also be very elastic if they heavily leverage automation and rely on the underlying public-cloud infrastructure to support system provisioning for additional users.

Beyond computer and storage infrastructure, scaling requires sufficient server-side bandwidth to allow a high volume of user access during peak periods. Limited scalability and/or elasticity causes some commercial range solutions to limit simultaneous access by requiring instructors or students to reserve timeslots or by simply refusing access until sufficient resources are freed.

Curriculum & Learning Outcomes

Cyber range-based curricula and learning outcomes are central to all possible use cases and stakeholder objectives for utilizing a cyber range. Not surprisingly, this is a rapidly evolving and difficult to navigate field. This section outlines the emerging trends and models.

Cyber Range Curricula

Two broad categories or models represent the majority of curricula: pre-packaged curriculum and ad hoc curriculum. The pre-packaged curriculum has a syllabus that includes low-medium fidelity content, testing, and gamification with a standardized path to completion. The ad hoc curriculum on the other hand is highly customizable and differs for each client, often requiring a persistent, integrated, and high-fidelity experimentation space. The table below outlines potential and likely curriculum customization for the various use cases:

	Cyber Range Use Cases	Curricula
1	Educators seeking to implement basic and advanced cybersecurity education courses and curricula	Pre-Packaged Ad Hoc
2	Organizations or individuals seeking training and continuing education for security operations, analysis, and forensic specialists	Pre-Packaged Ad-Hoc
3	Organizations seeking “situational operations” testing for new products, software releases, and organizational restructuring	Ad-Hoc
4	Organizations or individuals seeking cybersecurity skills validation to evaluate candidates for cybersecurity positions	Pre-Packaged
5	Individuals seeking workforce training for people moving into cybersecurity-related fields and positions	Pre-Packaged

The next central question for a range operator or user to understand is how the curricula (pre-packaged or ad-hoc) aligns or maps to leading industry frameworks and standards.

The NICE Framework

The United States Department of Commerce is home to one of the federal government's lead agencies for creating and outlining cybersecurity frameworks, the National Institute of Standards and Technology (NIST), and inside NIST sits the cyber education effort known as the National Initiative for Cybersecurity Education (NICE). This essential initiative "is a partnership between government, academia and the private sector" with a mission to "energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development."[4] The NICE mission seeks to "coordinat[e] with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure."[5]

As a part of this mission, NICE engaged its various stakeholders in order to create a comprehensive cybersecurity workforce framework, known as the NICE Framework, in order to establish a taxonomy and common lexicon to describe cybersecurity work and workers.[6] The NICE Framework is intended to be applied in the public, private, and academic sectors.[7] In order to serve the needs of these stakeholders, the Framework outlines the following core components: categories, specialty areas, work roles, knowledge, skills and abilities (KSA), and tasks.

The NICE Framework is a potentially essential tool for use and integration in Cyber Ranges. Cyber Range administrators could utilize the Framework core components in order to appropriately map their Range-related curricula and activities. For example, curricula and activities could be tied to Workforce Categories, including: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate. In addition and for consistency and the benefit of industry, the programming of cyber ranges could focus on education and training of KSAs

[4] *See* the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, available at: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[5] Id.
[6] *See* the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, available at: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[7] Id.

related to, or centered on, these workforce categories. For more on the NICE Framework, visit --

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

The NSA/DHS CAE Knowledge Units

The National Security Agency (NSA), in cooperation with the U.S. Department of Homeland Security (DHS), administers the National Centers for Academic Excellence program (CAE).[8] This program includes designations for Cyber Defense Education, Cyber Defense Research, and Cyber Operations and covers programs at the Associates, Bachelors, Masters, and Doctoral level.

The Information Assurance Directorate at the NSA defines a set of *Knowledge Units* (KUs) as part of the criteria for CAE designation[9]. A set of foundational KUs are required in programs seeking any of the designations, while optional KUs apply to specific designations. Many KUs refer to specific skills that must be demonstrated by students in certain programs and a range that maps hands-on content to KUs could help schools find content that maps to skills required to meet CAE certification requirements.

Types of Cyber Ranges

Cyber ranges have developed into a variety of types with each type holding a variety of the features and capabilities previously outlined. In general, there are four main types of cyber ranges: simulations, overlay, emulation, and hybrid ranges. Though the differences may appear insignificant, these differences become important when matching the type of cyber range to the use case of an individual or an organization.

Simulation Ranges

Starting in 2002 by the United States Air Force, simulations were the cyber range of choice for most environments. The concept behind simulation is recreating a synthetic network environment based on the behavior of real network components. Simulations run in virtual instances and do not require any physical network gear. In a typical simulation

[8] See "National Centers for Academic Excellence," available at: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

[9] See "2019 Knowledge Units," available at: http://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

environment, virtual machines (VM) replicate specific server, network, and storage of a particular IT infrastructure (small, medium, large, etc.).

These VM templates are standardized and thus, somewhat limited in how closely they simulate real IT infrastructure. Though quick to spin-up, the closer the cyber range matches the target exercise infrastructure, the higher the fidelity of the exercise. So, the granularity with which the simulation can match the target environment is directly proportional to the successful simulation outcome. For this reason, cyber ranges should require a strong orchestration layer.

The upside of a simulation environment is the speed of reconfiguration and the ability to use generic server and storage equipment. The primary downside of a simulated network is unpredictable and unrealistic latency and jitter of network performance.

Overlay Ranges

Overlay ranges are cyber ranges running on top of real networks, servers and storage. Overlay cyber ranges have a significant fidelity advantage over simulation ranges, but they come at a considerable cost of hardware and the cost of potential compromise of the underlying network infrastructure. Typically, overlay networks are set up as global testbeds, one of the largest being the Global Environment for Network Innovations (GENI), sponsored by the National Science Foundation.

Emulation Ranges

Emulation is running the cyber range on dedicated network infrastructure, mapping as-built network/server/storage infrastructure onto physical infrastructure: a physical infrastructure that becomes the cyber range. An emulation provides closed-network experiences with multiple interconnected environments. Emulation includes traffic generation that emulates numerous protocols, source patterns, traffic flows, attacks, and underlying internet connectivity. When done right, emulation creates true-to-life experiences, rather than pre-programmed actions and response. A key differentiator for accurate emulation has URLs that resolve to the cyber range's DNS and virtualized Internet IP addresses using real-world geo-IP addresses. The National Cyber Range (NCR) is probably the most significant emulation initiative.

Hybrid Ranges

As the name suggests, hybrid ranges emerge from a customized combination of any of the above types. The Virginia Cyber Range is an example of range that utilizes multiple features above and listed throughout this document. Another hybrid range is the European Future Internet Research & Experimentation, started in 2008.

Summary & Conclusion

Bridging the cybersecurity workforce gap in order to reduce cyber threats to industry and enterprise demands new, dynamic, and practical methods for educating and training both existing and potential cybersecurity specialists. Traditional academic methods and on-the-job training are necessary but no longer a sufficient means for meeting the demand and increasing the supply of qualified workers. The cybersecurity profession requires professionals with the necessary knowledge, skills, and abilities in order to complete essential tasks and fulfill work roles. In this rapidly changing landscape, a key tool and platform for reducing the skills gap and securing society is the cyber range. This document outlines actionable guidance to individuals and organizations looking to close the cybersecurity workforce gap by engaging, implementing, or utilizing a cyber range.

Appendix A

Cyber Range Checklist

Attached

Appendix A

The Cyber Range: A Checklist

This Checklist outlines key features, considerations and options and can be used by an individual or an organization in evaluating the various vendors and providers of Cyber Range platforms, tools and technologies.

Features	Considerations & Options
Use Case(s) of the Cyber Range	The Cyber Range is focused on the following audiences and/or use cases (more than one selection is possible) -- □ Educators seeking to implement basic and advanced cybersecurity education courses and curricula □ Organizations or individuals seeking training and continuing education for security operations, analysis, and forensic specialists □ Organizations seeking “situational operations” testing for new products, software releases, and organizational restructuring □ Organizations or individuals seeking cybersecurity skills validation to evaluate candidates for cybersecurity positions □ Individuals seeking workforce training for people moving into cybersecurity-related fields and positions
Location of the Range	The Cyber Range is located -- □ On-Premises (fixed or limited users) □ On-Premises (with cloud capability) □ Cloud-Based □ Hybrid (blend of on-premises and cloud-based)

Curriculum Type	The activities and assessments of the Cyber Range are – □ Pre-Packaged (no customization) □ Pre-Packaged with Options (some customization) □ Ad-Hoc (full and significant customization)
Learning Outcomes & Standard Alignment	The Cyber Range aligns with or utilizes the following standards or certifications – □ The NICE Framework □ NSA/DHS National Centers for Academic Excellence Knowledge Units □ Other ____ □ Other ____
Assessment & Debriefing Tools	The Cyber Range utilizes the following functions to aid in assessment and debriefing of users -- □ Recording and Replay Functionality □ Assessment or Rating/Scoring Functionality □ Assessment of Team Performance Functionality □ Assessment of Individual Performance Functionality
Scalability & Elasticity	The Cyber Range is able to support – □ Limited Number of Users for a Limited Time Period □ Limited Number of Users for an Unlimited Time Period □ Unlimited Number of Users for a Limited Time Period □ Unlimited Number of Users for an Unlimited Time Period
Training and Support	The Cyber Range operator or vendor provides – □ Initial Support and Training □ Periodic Support and Training □ On-Call Support and Training
The Special Sauce	The Cyber Range includes other features and capabilities such as –

	□ Industry-Specific Customization □ A Scheduling Component □ Specialized LMS or RLMS □ Other ______________________________ □ Other ______________________________ □ Other ______________________________ □ Other ______________________________ □ Other ______________________________