Software Engineering Institute
Carnegie Mellon University

R-EACTR: A Framework for Designing Realistic Cyber Warfare Exercises

Geoffrey B. Dobson
Thomas G. Podnar
Adam D. Cerini
Luke J. Osterritter

September 2017

TECHNICAL REPORT
CMU/SEI-2017-TR-005

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0004438

Table of Contents

List of Figures

List of Tables

Executive Summary

For a team to be effective, it must practice. Consider a sports team preparing for an upcoming season. All team members have unique individual skills that are refined and perfected through repetitive drills. The pinnacle of practice is the scrimmage—where all parts of the team work together to achieve a singular goal: score more points than another team. Sporting organizations go to great lengths to make the scrimmage experience as realistic as possible. The field is exactly the same dimensions as the real game field. The equipment is nearly identical to real game equipment. The rules of the game are equivalent. Referees are added to scrimmages to ensure everyone follows the rules. The scrimmage is the most important rehearsal before the real event. Without a scrimmage, it is difficult for coaches to assess the team's strengths and weaknesses. Similarly, it is difficult without a scrimmage for team members to understand how their part fits into the whole.

This is precisely the mindset that military planners must take when planning cyber exercises for U.S. military cyber teams. Military exercises serve many purposes. Team tactics, techniques, and procedures are rehearsed and evaluated. More importantly, team members build and refine trusting relationships. In order to get the most out of these engagements, exercises must be built with realism as a primary concern.

In this report, we introduce a design framework for cyber warfare exercises called Realistic - Environment, Adversary, Communications, Tactics, and Roles (R-EACTR). This framework ensures that when designing team-based exercises, realism is factored into every aspect of the participant experience. The authors have employed this framework in the delivery of approximately 30 live-fire cyber warfare exercises—iteratively improving and documenting the details that lead to optimal realism. The framework is most useful in the planning and design stages of the exercise build process. It forces conversations between planners, engineers, training leads, and participants. It encourages a full understanding of what the exercise is to accomplish and specific details of how it will occur. The conversations garner details about the upcoming engagement that are critical for producing a rewarding experience for exercise participants.

Abstract

As the cyberspace domain expands into nearly every aspect of military operations, leaders are challenged to provide valuable training and exercises to a growing number of cyber units. In order to be valuable, the exercise experience must feel realistic. This report introduces a design framework for cyber warfare exercises called Realistic - Environment, Adversary, Communications, Tactics, and Roles (R-EACTR). The R-EACTR framework places realism at the forefront of every cyber warfare exercise design decision. This report also describes challenges involved in creating military cyber exercises, a framework for building realism into each aspect of the exercise, and a case study of one exercise where the framework was successfully employed.

1 Realism Is the Key to Elite Cyber Warfare Exercises

Forbes Magazine Contributor John Laudicina predicts that 2017 will be the "Year of Cyber Warfare"—citing increased vulnerabilities from the Internet of Things, infrastructure attack rehearsals, and shifting global power politics [Laudicina 2016]. Nation states are primed for cyber warfare. In December 2016, an attack targeting South Korea's Cyber Command was attributed to North Korea [BBC 2016]. It would be naive to think that these cyber attacks will cease. In fact, many experts believe that full-scale cyber warfare is all but inevitable. In response to this reality, military leaders are actively preparing troops for cyber warfare.

How should our military prepare? The CERT Cyber Workforce Development (CWD) directorate at the Software Engineering Institute (SEI) has trained significant numbers of U.S. government cyber professionals. In 2010, CWD researchers published an SEI technical report detailing our approach to cybersecurity workforce development [Hammerstein 2010]. The report describes three main development phases: knowledge building, skill building, and experience building. Initially, CWD spent the majority of its time improving the first two phases: knowledge building and skill building. This was mainly achieved using a virtual training environment – providing individuals custom-designed cyber security course materials combined with hands-on labs. Since publication of that 2010 technical report, CERT researchers have been increasingly involved in the "experience building" phase of this pedagogy. Experience building is achieved through team-based cyber exercises. Since 2011, CERT researchers have delivered over 125 cyber exercises to over 8,000 Department of Defense (DoD) participants—representing all military service branches including the Reserve and Guard.

According to Joint Publication 1-02, the definition of exercise is "A military maneuver or simulated wartime operation involving planning, preparation, and execution. It is carried out for the purpose of training and evaluation" [DTIC 2017]. Nearly all military units participate in at least one team-based exercise per year, ensuring that the members are capable of carrying out their assigned mission-essential-task list (METL). The cyber units that we support are engaging in a variety of cyber exercises, from the large scale (e.g., Cyber Flag, Cyber Guard, and Cyber Knight) spanning weeks, to the small scale (e.g., Cyber Forge and Mercury Challenge) spanning just several hours. In all of these exercises, we are either leading or directly assisting the military in the planning, building, delivering, and reporting efforts.

Over the past half-decade, we've paid close attention to the feedback that emerges from exercises. The most frequent feedback is a desire for "realism." Teams want to maximize realism in every aspect imaginable. After one of the large-scale exercises, an after-action report noted that some of the tools available in the exercise environment were not the same as the tools that would be used in real-world operations. Coming out of one of the small-scale exercises, a Cyber Protection Team (CPT) member told us that the interfacing between the team and external organizations was not being simulated realistically. During 2016, our cyber exercise design team assigned to the U.S. Army Network Enterprise Technology Command (NETCOM) training and exercise branch began collecting survey data after each exercise. With each survey response, we learned more specific details of realism that could be designed into the exercises. As we responded to each lesson

learned and increased the level of realism in the exercises, other benefits emerged. Team leaders reported that the value of the exercise increased and participants became more engaged.

As we design realism into the exercises, one must account for the simple fact that as realism increases, so does the cost of the exercise. Therefore, we conduct cost/benefit analyses on the various realism details to determine where investments should be maximized or minimized. The key is to find the point where we've made concessions to keep the cost minimal, but made the exercise realistic enough to meet the desired training effect.

In his book, *Team of Teams*, General Stanley McChrystal wrote about SEAL team training. "… a team fused by trust and purpose is more potent. Such a group can improvise a coordinated response to dynamic, real-time developments" [McChrystal 2015]. Increased realism also results in a more complicated and dynamic environment. We observed that, in order to prevail in this increasingly realistic cyber warfare exercise environment, teams learn to operate as a whole and build trust among each other—rather than rely on individual skill sets. We codified our observations and notes into a design framework called the Realistic – Environment, Adversary, Communications, Tactics, and Roles (R-EACTR) framework. We now apply R-EACTR to every cyber warfare exercise that we design, develop, and deliver.

2 The R-EACTR Framework

In our experience, all design decisions fit into one of the following five aspects of the exercise experience: environment, adversary, communications, tactics, and roles. From the perspective of the participant, each aspect must be realistic enough to provide a satisfactory (and valuable) exercise experience. Leaving out any one aspect could sabotage the perception of realism for the entire exercise. For example, there could be a realistic adversary. Without realistic tactics, however, there is limited value when countering the realistic adversary's move. In another example, the environment may be realistic, but without a realistic mechanism of communications, the sense of realism is lost when it becomes time to report threat mitigation recommendations. We believe that an exercise that does not cover all five aspects will result in a sense of the exercise being unrealistic. The next five sections define each segment and identify the elements and sub-elements that holistically cover that specific segment.

R-EACTR FRAMEWORK		
REALISTIC	Environment	Physical
		Virtual
		Psychological
	Adversary	Threat
		Resources
	Communication	Internal
		External
	Tactics	Individual
		Collective
	Roles	Red
		White
		Blue

Figure 1: R-EACTR Framework

2.1 Environment

The "Environment" segment refers to the aggregate of conditions, observations, and access to information that the participant experiences. The first element is the physical space from which the team will be exercising, which includes environmental and office space concerns. The second element is the virtual space, which is composed of the network, access, and configurations of systems with which the team will interact. The final element is the psychological. This is generally the most difficult to simulate, but should be attempted nonetheless. We simulate psychological realism by putting the team into familiar schedules, reporting protocols, and mental pressure. The elements and sub-elements of the Environment segment are defined in Table 1.

Table 1: Environment Segment

Element	Sub-Elements
Physical	Office Space: table and chair arrangements, whiteboards, printers, phones
	Environmental: proximity to facilities, uniforms, meals
Virtual	Network: architecture, infrastructure devices, security applications
	Access: console, remote desktop protocol (RDP), logins
	Configurations: versioning, patching, Security Technical Implementation Guide (STIG) levels
Psychological	Battle Rhythm: schedule, hotwash, shift turnover, end-of-day reporting
	Pressure: pace, complexity of exercise, assessments, feedback from leadership

2.2 Adversary

The "Adversary" segment refers to the aggregate of opposing forces simulated throughout the exercise. The first element is threat, which we realistically simulate by modeling specific types of attacks from known adversaries. The threat must have a complexity, which, when coupled with the threat type, is realistic. The second element of the Adversary segment is resources. An adversary will be realistic if the sub-elements of financial, human, and technological are well designed into the overarching scenario narrative. The elements and sub-elements of the Adversary segment are defined in Table 2.

Table 2: Adversary Segment

Element	Sub-Elements
Threat	Type: nation-state, hacktivist, crime family, unknown, blended
	Complexity: difficulty level of attacks, obfuscation efforts, deception, noise
Resources	Financial: purchasing power, bribes, hiring mercenaries
	Human: insider threat, intelligence sources, social engineering
	Technological: tools, systems, skill

2.3 Communications

The "Communications" segment refers to the aggregate of the mechanisms and methods the team will use to communicate throughout the exercise. We generally divide that segment into two elements: internal and external. When designing the communications segment, we're concerned with replicating the communications that the team uses in real-world operations as closely as possible. This segment also includes modeling any communications that will move outside of the team boundaries to external organizations. We've found that careful attention should be paid to how the team will communicate externally, as this will enable exercise facilitators to realistically inject information (orders, reports, tasks, etc.) that will drive team behaviors. The elements and sub-elements of the Communications segment are defined in Table 3.

Table 3: Communications Segment

Element	Sub-Elements
Internal	Voice: Voice over Internet Protocol (VoIP), teleconferencing, cellular phones, face to face
	Electronic: email, instant messaging, file share
External	Directive: operational orders, fragmentary orders, commander's critical information requirements (CCIRs)
	Collaborative: incidents, threats, mandated, requests for information (RFIs)

2.4 Tactics

The "Tactics" segment refers to the aggregate of the team's internal tactics, techniques, and procedures. When designing the Tactics segment, there will be a substantial amount of dialogue between the cyber operations team and exercise developers in the design phase of the exercise development. Although all teams are operating from the same METL, how they execute the tasks varies greatly. This fact makes this segment the most difficult to model correctly. The first element of the Tactics segment is *individual*, in which we consider specific skills, tools, and responsibilities. The second element of the Tactics segment is *collective*, where we focus more on processes that enable the successful completion of mission objectives. The elements and sub-elements of the Tactic segment are defined in Table 4.

Table 4: Tactics Segment

Element	Sub-Elements
Individual	Specialty: military occupational specialty (MOS), certifications, experience
	Leadership: resource allocation, briefings, prioritization
Collective	Mission: METL, objectives, reports
	Process: team-specific procedures, military instructions, regulations, the military decision making process (MDMP)

2.5 Roles

The "Roles" segment refers to the aggregate of the roles that must be played within the exercise to provide a realistic mission. When designing the Roles segment, we'll script all of the possible interactions that might occur and ensure that each individual is available inside the exercise. When designing this segment we use the familiar *red*, *white*, and *blue* elements that are used in nearly all cyber exercises. The elements and sub-elements of the Roles segment are defined in Table 5.

Table 5: Roles Segment

Element	Sub-Elements
Blue	Team: Battle Captain, host, network, emulation, logging, reporting
	Supporting: computer network defense service provider (CNDSP), intelligence, reach-back, higher headquarters
White	Controlling: injecting, timekeeping, master scenario event list (MSEL) controller
	Assessment: embedded observer, assessor, inspector

Element	Sub-Elements
Red	Opposing force (OPFOR): military, criminal, political, civilian
	OPFOR Support: technical, financial, logistical

3 Case Study – Cyber Forge 11

The CWD directorate has collaborated with the U.S. Army Network Enterprise Technology Command's Training and Exercise Branch to provide team-level exercises to various cyber units since 2012. One series of exercises is called "Cyber Forge." The Cyber Forge exercise series consist of unclassified, fictional, collective training events designed to allow the Cyber Protection Brigade to assess Cyber Protection Team performance. The exercise is facilitated by several exercise developers who act as the Mission Owner, Computer Network Defense Service Provider (CNDSP), adversarial forces ("Red Team"), out-of-game facilitators, and other roles as necessary. The exercise is delivered remotely through the CERT Private Cyber Training Cloud (PCTC)—an instance of the Simulation, Training, and Exercise Platform (STEP). In this case study, we describe one such Cyber Forge exercise that was designed and delivered to a Cyber Protection Team in September of 2016. In the next five sections, a table summarizes the design details of each segment for Cyber Forge 11.

3.1 Environment

In regards to the physical element of the Environment segment, the CPT was able to exercise in a conference room on post that was familiar to the team. This greatly increased the realism of the physical element, since the CPT is in familiar facilities and normal surroundings. In regards to the virtual element of the Environment segment, the virtual network of Cyber Forge 11 was a complex infrastructure that accurately represented the deployment of a CPT to a joint base—with connections to a Network Enterprise Center (NEC) and Regional Cyber Center (RCC). Team members were provided access to realistic tools and enterprise systems that were similar to those used in recent CPT operations. For the psychological element of the Environment segment, we designed realistic pressure injects through the use of forced briefings to the simulated Mission Owner. This produced expected psychological responses resulting from rushing to provide in-depth technological information about as many aspects of the defended cyber terrain as possible. Table 6 details the most important sub-element details of the Environment segment design for Cyber Forge 11.

Table 6: Cyber Forge 11 Environment Segment Design Details

Element	Sub-Elements	Cyber Forge Details
Physical	Office Space	• utilized home station, with access to both non-classified Internet protocol router (NIPR) and commercial Internet • separate rooms for Red/White/Blue players • team laptops, printers, white boards, telephones available • ready access to communication mechanisms
	Environmental	• normal meal options, Uniform of the Day (UOD) required • normal transportation, weekly PT requirements
Virtual	Virtual Network	• simulated interconnected forward operating base(FOB), network enterprise center (NEC), regional cyber center (RCC), and Defense Information Systems Agency (DISA) • simulated internet with multihop border gateway protocol (BGP) routing, internet sites, root servers for Domain Name Service (DNS)

Element	Sub-Elements	Cyber Forge Details
		• realistic Internet based HTTP & DNS network traffic generation against defended assets • defined and dynamic adversary/red team IP addresses and ranges
	Virtual Access	• RDP or secure shell (SSH) access to all servers, appliances, and network gear • console access to all end-user workstations, servers, appliances and network gear
	Configurations	• Windows Server 2008 • Windows Sever 2008 Active Directory (AD) domain level • Active Directory populated with hundreds of real user accounts • Active Directory restrictive Group Policy • Updated Windows workstations and server OS and app patches • Windows 7 and Ubuntu Desktop user workstations • Microsoft Office 2011 with Microsoft Outlook client for email • Simulated Windows 7 user logins, email, MS Office activity • Windows 2008 IIS and Apache Linux web servers • Microsoft AD and Linux BIND DNS • HBSS/McAfee ePolicy Orchestrator • Cisco routers • Blue Coat Proxy Servers • Palo Alto firewalls with realistic firewall rules • Cisco SourceFire and Security Onion • Arcsight SIEM • SiLK NetFlow traffic collection and analysis • Forensics tools: SIFT, REMnux, and ADHD • ACAS/Nessus security scanner • ELK stack • Kali Linux
Psychological	Battle Rhythm	• daily STARTEX 0800, PAUSEX 1600, hotwash • daily operations at discretion of Battle Captain
	Pressure	• survey briefing to simulated Mission Owner Day 2, 1500 • Mission Owner directed tasks, intended to cause stress • Battle Captain instructed and expected to move quickly • simulated CNDSP technical and specific interactions • rapid fire OPFOR injects and intel during Day 4

3.2 Adversary

For the threat element of the Adversary segment, we decided to introduce two potential opposing forces to the CPT during Cyber Forge 11. One was a regional crime family and the other was a regional, belligerent nation state. The opposing forces represented different types of threats possessing varying levels of complexity, intent, and interests. For the resources element of the Adversary segment, we considered realistic interactions between the OPFOR and supporting characters. This included money laundering, conspiracy, and geo-political posturing. The CPT was made aware of various scenario-based injects by receiving intelligence reports and interfacing with simulated external agencies. Table 7 provides Adversary Segment sub-element design details used for Cyber Forge 11.

Table 7: Cyber Forge 11 Adversary Segment Design Details

Element	Sub-Elements	Cyber Forge Details
Threat	Type	• Aspiring separatist army, seeking independence, receives coordinated help from a neighboring hostile nation-state. • Transnational criminal organization seeking to influence geo-political events for its own financial gain and increase areas of control. • Both groups are capable of coordinating with one another, as well as the hostile nation-state.
	Complexity	• The aspiring separatists have enhanced their cyber capabilities due to their coordination with the hostile nation-state. • The crime family has the most capabilities and has recently acquired mercenary hackers. • The crime family is also known for additional crimes like kidnapping and extortion. • All are capable of conducting multiple simultaneous cyber attacks. • All are capable of gathering operational intelligence for cyber attacks.
Resources	Financial	• Transnational criminal organization is well funded due to gains from recent successful cyber attacks against regional banking assets.
	Human	• Training: All members are technology savvy and English speaking as a second language. • Key personnel were educated in Western universities. • Several have multiple established cyber call signs and known reputation to be effective in cyber warfare activities. • All are trained in advanced social engineering techniques.
	Technological	• Reconnaissance: port and service enumeration • Spear Phishing: multiple techniques • browser exploitation attacks • malware placement capable of remote admin, privilege escalation, and lateral movement • establishment of covert connectivity persistence, once foothold gained • data exfiltration and information harvesting • system integrity degradation • denial-of-service/distributed denial-of-service (DoS/DDoS) attacks • advanced persistent threat (APT)-level attacks

3.3 Communications

For the Internal element of the Communications segment, we ensured that CPT members were able to utilize all of their normal mechanisms: email, voice, and chat. Since the CPT was collocated, members were able to communicate face to face. For the External element of the Communications segment, all external agencies were connected virtually to the CPT exercise systems. Table 8 provides Communications Segment sub-element design details used for Cyber Forge 11.

Table 8: Cyber Forge 11 Communications Segment Design Details

Element	Sub-Elements	Cyber Forge Details
Internal	Voice	• leveraged direct face-to-face communications in same room
	Electronic	• used email and online chat with simulated network operations center (NOC) • used online chat for intra-team: all with dedicated channels/rooms (Spark Chat) • used Windows file sharing among team for all documents • used Redmine web app for submitting RFIs and responses with the CNDSP
External	Directive	• received Operational Orders and Fragmentary Orders at STARTEX and throughout duration of exercise
	Collaborative	• used email and online chat with simulated NOC/CNDSP/Mission Owner, and Cyber Fusion Center • used online chat for white-cell, intel team, moderators, and helpdesk • established dedicated channels/rooms for creating communication silos

3.4 Tactics

For the Individual element of the Tactics segment, we examined the roster of the participants and ensured that each skillset would be utilized in some way when we designed the exercise—including leadership positions and intelligence analysts. For the Collective element of the Tactics segment, we selected specific items from the unit's METL that would be exercised and ensured that the OPORDER would employ those collective actions. We then designed interactions that would occur between the various organizations simulated within the exercise, so that each collective task had a specific inject ready to trigger it. Table 9 provides Tactics Segment sub-element design details for Cyber Forge 11.

Table 9: Cyber Forge 11 Tactics Segment Design Details

Element	Sub-Elements	Cyber Forge Details
Individual	Specialty	• reviewed configurations and tool setups based on specific technical skills • reviewed security tools data for malicious activity • reported specific infrastructure findings to team
	Leadership	• team lead tasked to prepare situation reports (SITREPS) • squad leads prioritized operations amongst team members
Collective	Mission	• reviewed all provided information and confirmed credential and network connectivity success • verified key terrain cyber assets being defended • deployed team custom security tools and sensors • determined network/configuration baselines • conducted current security risk assessments of infrastructure • monitored, detected, responded to adversary activities • made mitigation recommendations for configuration to CNDSP • hunted any rogue adversary activity • engaged directly with active adversary threats • produced daily Network Activity Reports (NAR)

Element	Sub-Elements	Cyber Forge Details
		• generated daily Situation Reports (SITREP)
	Process	• exercised internal team process for identifying threats and funneling to Battle Captain • exercised internal team processes for threat discovery and mitigation techniques • exercised internal team process of submitting RFIs to Mission Owner and CNDSP • exercised internal team process surrounding MDMP as new threats/reports/orders were received

3.5 Roles

For the Blue element of the Roles segment, all team members worked within their normally assigned roles and responsibilities. Supporting blue forces (i.e., Cyber Fusion Center, Area of Responsibility Intelligence Units, locally stationed CNDSP, and assigned Mission Owner) were simulated by character actors. For the Red element of the Roles segment, several adversarial forces were also simulated by character actors. For the White element of the Roles segment, the exercise developers took care of all aspects of control. The assessment sub-element was the responsibility of a training non-commissioned officer (NCO) within the CPT. Table 10 provides Roles Segment sub-element design details for Cyber Forge 11.

Table 10: Cyber Forge 11 Roles Segment Design Details

Element	Sub-Elements	Cyber Forge Details
Blue	Team	• Battle Captain was present and provided team leadership. • Cyber Protection Team size was 21 members.
	Supporting	• CNDSP/NOC role existed and was available via online chat and telephone to answer questions and provide operational support. • Intel team role existed to provide Intel “tippers” to help the flow of the exercise. • Intel team also answered Intel-related questions that arose after the Intel “tippers” were supplied to the team.
White	Controlling	• identified and assigned white cell members to exercise roster roles • pre-STARTEX logistics coordination of all teams and components • managed the “game clock” for STARTEX/PAUSEX/ENDEX • controlled the flow of the MSEL • conducted in brief at STARTEX • conducted hotwash at ENDEX • monitored the team’s progress and status and adjusted the MSEL as necessary based on strengths and weaknesses • leveraged screen “following” tools to monitor end-user activities/clicks • managed the timing of the release of Intel information • managed the timing of the deployments of the Red Team injects
	Assessment	• Embedded observer was placed in the same room as the Blue team participants. • Embedded observer provided real-time feedback and summary reporting.
Red	OPFOR	• deployed custom RAT (Remote Administration Tool) APT

Element	Sub-Elements	Cyber Forge Details
		• created and used Slowloris DDoS Botnet attack against defended assets • leveraged malware based beacons for data exfiltration delivered via Spear Phishing • used lateral movement to compromise the AD domain • used SQL injection for data exfiltration • infiltrated malware via rogue CD
	OPFOR Support	• provided simulated sensitive information access to regional Internet service provider • provided simulated leaked information regarding troop movements • provided simulated leaked information from regional banking assets

4 Conclusion

In this report, we introduced the R-EACTR Framework as a guide for desiging and building adequate realism into military cyber warfare exercises. In our experience building and delivering cyber warfare exercises, we've found that the key ingredient to maximizing value is realism. With a solid framework for creating great scrimmages, teams can practice their way to becoming elite.

References

URLs are valid as of the publication date of this document.

[BBC 2016]
British Broadcasting Corporation. *North Korea 'hacks South's military cyber command.'* BBC News. December 5, 2016. http://www.bbc.com/news/world-asia-38219009

[DTIC 2017]
Defense Technical Information Center. *Joint Publication 1-02: Dictionary of Military and Associated Terms.* DTIC. March 2017. http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf

[Hammerstein 2010]
Hammerstein, Josh & May, Christopher. *The CERT Approach to Cybersecurity Workforce Development*. CMU/SEI-2010-TR-045. Carnegie Mellon University, Pittsburgh, PA. Software Engineering Institute, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9697

[Laudicina 2016]
Laudicina, John. 2017 Will Be The Year Of Cyber Warfare. *Forbes Magazine*. December 16, 2016. https://www.forbes.com/sites/paullaudicina/2016/12/16/2017-will-be-the-year-of-cyber-warfare/#74c6c86a6bad

[McChrystal 2015]
McChrystal, Stanley; Collins, Tantum; Silverman, David; & Fussell, Chris. *Team of Teams: New Rules of Engagement for a Complex World.* Penguin, 2015. https://mcchrystal-group.com/teamofteams/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	September 2017	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
R-EACTR: A Framework for Designing Realistic Cyber Warfare Exercises	FA8721-05-C-0003

6. AUTHOR(S)

Geoffrey B. Dobson
Thomas G. Podnar
Adam D. Cerini
Luke J. Osterritter

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2017-TR-005

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

As the cyberspace domain expands into nearly every aspect of military operations, leaders are challenged to provide valuable training and exercises to a growing number of cyber units. In order to be valuable, the exercise experience must feel realistic. This report introduces a design framework for cyber warfare exercises called Realistic - Environment, Adversary, Communications, Tactics, and Roles (R-EACTR). The R-EACTR framework places realism at the forefront of every cyber warfare exercise design decision. This report also describes challenges involved in creating military cyber exercises, a framework for building realism into each aspect of the exercise, and a case study of one exercise where the framework was successfully employed.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Realistic - Environment, Adversary, Communications, Tactics, and Roles	23

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102