Carnegie Mellon University
Software Engineering Institute

GHOSTS in the Machine: A Framework for Cyber-Warfare Exercise NPC Simulation

Dustin D. Updyke
Geoffrey B. Dobson
Thomas G. Podnar
Luke J. Osterritter
Benjamin L. Earl
Adam D. Cerini

December 2018

TECHNICAL REPORT
CMU/SEI-2018-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. FA8702-15-D-0002 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/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM18-0553

Table of Contents

List of Figures

List of Tables

Abstract

This report introduces the GHOSTS ((G)eneral HOSTS) framework, the purpose of which is to create a high level of realism in cyber-warfare exercises by establishing and building behaviorally accurate, autonomous non-player characters (NPCs). The report outlines how the GHOSTS framework accomplishes the creation of simulations in which NPCs realistically represent a vast array of possible encounters and outcomes. The report concludes with a discussion of a case study in which the GHOSTS framework was used. Participants in the exercise reported high levels of realism, which in turn correlated with higher ratings for training value. These results indicate that the GHOSTS framework can be used to create training of the highest quality, effectively preparing cyber-warfare teams for success in real-world situations.

1 Introduction

This report describes some of the challenges associated with the creation of cyber-warfare exercises through the simulation of characters, contexts, and situations across large-scale computer networks. These simulations are often used in the training of cyber-warfare teams. Addressing the challenges involved with the creation and delivery of cyber exercises can improve how these service members prepare for real-world operations.

In the sections that follow, we introduce a framework called GHOSTS, which stands for (G)eneral HOSTS. The purpose of the framework is to build simulations that exhibit exceptional realism. Realism is the central component for creating effective and high-quality training opportunities. If a cyber exercise can simulate realistic characters within a lifelike scenario, then cyber-warfare teams will have the opportunity to train more like they fight. Realism within a learning environment is a driving factor in the development of team confidence.

GHOSTS is the CERT Division's framework for creating highly realistic, observable network traffic as a consequence of simulated-human non-player characters (NPCs) trying to achieve a specific objective related to their role within a cyber exercise. For exercise researchers and developers, GHOSTS provides the ability to imagine and construct a rich player experience that mimics real-world environments that today's cyber operators are intimately familiar with assessing, securing, and monitoring. This framework provides a unified context for the overall exercise storyline, including specific network traffic resulting from the behaviors of realistic characters that is traceable down to the lowest levels of exercise machinery.

The first sections of this report outline the difficulties involved in creating realistic cyber-warfare exercises and explain how GHOSTS can establish behaviorally accurate, autonomous NPCs within a cyber-warfare exercise. A case study using GHOSTS follows that discussion to provide an overview of how GHOSTS was successfully deployed in a training exercise. The case study includes reports derived from the data we collected from exercise participants. Finally, the conclusion discusses the importance of realism for creating effective training and future development possibilities using the GHOSTS framework.

The authors of this report are CERT Cyber Workplace Development (CWD) researchers within the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU). We employed this framework in the delivery of several cyber-warfare-scenario exercises as we iteratively improve the platform in the endless quest for optimal exercise realism.

2 Background and Platform Goals

Historically, both academic and commercial entities have made significant efforts to create realistic user simulations and network traffic generation. Our goal was to build on the progress made by these entities by setting a new level of simulation realism where participants could not detect any appreciable difference between human- and computer-controlled activities on a network. To that end, we aimed to create exercise traffic patterns that would realistically mimic typical human behavior. Those patterns would be random enough to match a healthy cross-section of different activity that one finds on an organization-wide computer network, yet not so random that the traffic could only be computer generated. Furthermore, we aimed for a level of realism that allows participants to sufficiently determine and associate the intent of particular traffic with a particular person. The goal is to construct complex scenarios where different people can play different roles within an exercise. With these details in place, our scenario can tell a sophisticated story of persons and their activities that provides an entirely realistic experience, from the exercise storyline, to the actual packets of network traffic found within the environment. This is the background from which the GHOSTS framework was born.

Achieving this level of simulation realism in a cyber-warfare exercise presents many challenges. Any dynamic and reasonable facsimile of a large-scale computer network introduces a broad variety of characters, contexts, and situations that are difficult to reduce, limit, or otherwise classify without compromising the high-fidelity player realism that remains the hallmark of a premium exercise experience.

Within a simulation, interactions can occur between any combination of player and non-player characters, where

- A player is an active participant in the exercise.
- A non-player character (NPC) is any character that is not controlled by a player within a simulation. For our purposes, this usually means a character controlled by software, having some predetermined persona and corresponding behavior.

One goal of the GHOSTS framework is to produce in-exercise NPCs that represent multiple realistic personas and engage in a vast array of possible activities that a player can observe or interact with. NPCs included in an exercise can range from neutral office administrators to hostile enemy operators. While NPC intentions drive activity that aligns with specific exercise objectives, these intentions also translate down to the actual network traffic moving across the wire. In other words, "Ultimately, observed network traffic is a consequence of human actors trying to achieve an objective" [Berk 2012].

Creating sufficiently realistic activity on even a small-sized network involves routers, switches, firewalls, servers, workstations, and connectivity. Within a cyber exercise, machine information, network traffic, and a broad range of machine events remains in plain view of players, much as one would expect to see in the day-to-day management of a typical computer network.

However, similar information regarding machines, traffic, and activity used by exercise facilitators needs to stay beyond the view of players within the simulation. For example, information

about network health, network user orchestration, and malicious code status should explicitly not be seen by players on a network. The orchestration of such information needs to happen outside of participants' purview so that any resulting artificial network traffic does not interfere with simulation realism.

Lastly, exercise facilitators administer injects–activities ranging from malware, to insider threat, to intelligence chaff meant to disorient a player team. These injects enter the exercise via some reasonable storyline where any network activity appears to players just as it would in the real world. The GHOSTS framework approaches engineering challenges from a player's viewpoint of what is reasonable in the real world.

As the development team reflected on GHOSTS features, the question they most often asked was, "Is that reasonable to see if I were looking over your shoulder while sitting at the computer?"

To address these challenges and background, the GHOSTS framework strives to adhere to the following guiding principles:

- The software should make the administration and facilitation of variable-sized cyber exercises easy to set up and manage through smart defaults and automation of any repetitive or sensitive task.
- The software should enable further research and development by making micro-event information readily available in some centralized manner, where that information highlights something about the real-time interactions occurring within the event. Eventually, the platform will fully support the building of further applications atop this data store.
- The software should always aspire to mimic real human-computer interactions on a network. In doing so, exercise participants are unable to detect specific GHOSTS behavior.

3 The GHOSTS Framework

The following sections provide an overview of how the GHOSTS framework meets the goals outlined in Section 2, Background and Platform Goals. The features below help to establish the groundwork for creating deeply realistic simulations.

3.1 NPCs and Agents

GHOSTS is a general, all-purpose orchestration platform with regards to character behavior, capabilities, and functions. However, no network activity within an exercise traces back to GHOSTS software directly. Rather, activity is executed through a software agent that is represented in-simulation via a character. If an agent is the raw binary client executing commands on a machine, the layer above it brings the NPC to life by infusing it with human-like characteristics, beliefs, and intentions.

For context, we implement Wooldridge and Jennings' definition of agents as being autonomous, sociable, reactive and proactive, and conceptualized with human qualities [Wooldridge 1995]. We use the term to inform our vision for any platform implementing the GHOSTS framework.

The NPC layer supports a myriad of human personas within an exercise and is largely configurable. Where an agent might be able to perform many actions, the NPC is provided specific tasks to complete, ranging from Internet research, to creating spreadsheets or other office documents. From a network perspective, this aspect gives a realistic impression of what network administrators might see daily in the real world. This aspect also enables facilitators to recreate the scenario with a high level of realism, telling the story of what an NPC was specifically doing on their computer at any given time.

NPCs can be friendly, neutral, or openly hostile. The system makes provisions for the existence of all aforementioned types. While it is true that NPCs managed by GHOSTS could, in fact, be a hostile foreign national spreading malware on an unsecured network, the activity traces to the logged-in NPC account and not the specific software agent running on the NPC's machine. GHOSTS treats and handles all agent functionality the same, regardless of intent, so that it is impossible to determine friendly, neutral, or hostile activity by passive observation. GHOSTS remains entirely neutral when viewed from a player perspective within any exercise. It does not directly engage in hostile behaviors, and it does not plot against human players.

Lastly, NPCs have an alignment not found in the agent. An NPC might be aligned to a certain cause, it might set out to do the player team harm, or it might remain entirely neutral throughout the simulation. Agents have no such bias.

Table 1 summarizes the contrasts between agents and NPCs with regard to actions, capabilities, and alignment.

Table 1: Distinctions Between GHOSTS Agent and NPC Concepts

Layer	Represents	Actions	Capabilities	Alignment
Agent	Raw Software	General	Automated	Neutral
NPC	Human Persona	Specific	Reasoned	Biased

3.2 Knowledge Horizon

A key challenge with simulating human activity is sufficiently constructing what an NPC might know as it performs certain actions. Compounding this problem is that the knowledge of an NPC (or a group of NPCs) should not be static in time or confined to a finite space. To address these difficulties, GHOSTS builds on the Game Theory term "horizon," which addresses a game player's knowledge of how long a game has been played and when it might end [Osborne 2009]. The following combination of items comprises the knowledge horizon of GHOSTS: (1) what an NPC knows, (2) what an NPC could realistically know, (3) an NPC's awareness of simulation time remaining, and (4) an NPC's knowledge of simulation time elapsed. Specifically, this measurement of NPC knowledge for everything in-exercise at any point in time is different per character and is ever-changing, just as in the real world.

Since NPCs currently communicate with a central application programming interface (API), careful controls must be in place for what each NPC can know at any time within an exercise. These controls also allow for realistic knowledge-horizon growth over the whole of the exercise so that, while an NPC begins with some set of baseline knowledge, that initial set grows as events unfold and communication with other characters occurs throughout the exercise.

GHOSTS currently tracks each construct's horizons separately for decision purposes, from individual NPCs, to groups, to the entire simulation's NPC population.

3.3 User Operations

Given some persona coupled with some knowledge-horizon context, NPCs perform activities, including operations using different kinds of applications. Operations are a finite set of potential actions that an NPC might perform, currently limited only by the technical capability to interface with some specific computer function.

Table 2 outlines the main operational capabilities currently available in GHOSTS.

Table 2: GHOSTS Capabilities List

Capability	User Action	Methods
Web browsing	Browse Enter text Click link or button	Random, specific, looping
Terminal commands	Execute cmd commands Execute Powershell commands	Random, specific, looping

Capability	User Action	Methods
Inter-NPC communication	Email creation and management	Specific, looping
Office document management	Common file formats for word processor, spreadsheet, and presentation documents created and saved locally or on a network drive	Random, specific, looping

It should be noted that these capabilities are always built in a manner that most closely mimics a user actually performing some action. Therefore, while there are many ways to programmatically construct a web request to some other machine, GHOSTS chooses to use and control the actual web browser application installed on the host computer to browse to the desired location. This action presents some difficulty for capability applications that lack a comprehensive API for interactions. This difficulty might be further compounded by a complex UI model for interacting with certain functionality. We believe, however, that attempts to shortcut or mimic how actual user functionality occurs on a host machine will be detected by real players and that it will certainly detract from exercise realism.

In the future, GHOSTS will pursue a plug-in strategy for agent operations so that specific application functionalities can be built where necessary without the overhead of modifying the GHOSTS application directly.

Possible actions that an NPC can take also include no activity at all. A period of no activity is when the agent goes into a waiting state until some predefined time, or until something specifically happens on the network to which the NPC might have a response strategy.

3.4 Scenario

Scenarios within a cyber exercise are storylines–the construction of a series of events playing out in a certain manner. Creating a scenario is key for establishing realism because scenarios form the crux around which NPCs come to life. Scenarios define NPCs' intentions, collaborations, and eventual actions throughout the exercise, while ensuring the narrative remains cohesive throughout, regardless of how players interact with NPCs or their organizations. Additionally, scenarios are the basis for effective training, giving facilitators a means to meet training objectives, provide instruction, and create trust with player teams by supporting them during a realistic combat scenario.

When developing scenarios, exercise developers can target different kinds of training objectives. They might want to focus on the identification and quarantine of specific types of malware on a network, or on insider threat and the communications between fellow inside and outside operators. Some of this design work is dependent on the rules of engagement (ROE) for the exercise, typically defined in conjunction with CWD researchers and exercise sponsors. Scenarios can also be driven by a team's need to confirm its competency with specific tools or fulfill interests in specific training topics.

After an exercise, facilitators will often walk participants through a scenario, or certain parts of it, to outline specific details of what happened, why it happened, who was involved, and how player

teams could have identified, contained, and quarantined specific in-exercise technical events. Researchers construct the scenario in great detail before an exercise, maintaining reference documentation used to describe locations, NPCs, groups, and other elements in high fidelity.

Building a realistic scenario involves players who understand the lay of the land, who know their specific roles therein, who can quickly identify threats, and who can prescribe proper mitigation. A realistic scenario tends to build trust with exercise facilitators and between cyber operators themselves as they work together. This trust is paramount for soldiers to get the most out of an exercise experience. Network anomalies, inexplicable security practices, or network "magic" that mysteriously produces exercise events can quickly deteriorate the realism of any exercise. As we continue to train more experienced, elite cyber teams, expectations for realism continue to rise. GHOSTS was, in part, born out of the desire to meet these rising player expectations.

4 Case Study

CWD researchers have been leading the construction of high-fidelity cyber-warfare exercises since 2011, delivering over 125 cyber-warfare exercises to over 8,000 Department of Defense (DoD) participants spanning all military service branches, including the Reserve and Guard [Dobson 2017].

In this case study, we describe a scenario using the GHOSTS framework that was designed and delivered to three Cyber Protection Teams using an exercise series built by CWD researchers called Cyber Forge. This particular series consists of unclassified, fictional, collective training events designed to assess Cyber Protection Team (CPT) performance. The exercise encompasses mission owners, a Computer Network Defense Service Provider (CNDSP), opposing forces ("OPFOR"), out-of-simulation facilitators, and other necessary roles.

The three instances of the exercise were delivered through the CERT Private Cyber Training Cloud (PCTC), which forms part of the Simulation, Training, and Exercise Platform (STEP). Each training consisted of a two-week engagement and they were conducted on December 4-15, 2017, March 5-16, 2018, and April 5-19, 2018, respectively.

This Cyber Forge exercise implemented GHOSTS to orchestrate over 100 NPCs across multiple network subnets to simulate appropriate user behavior.

When bringing a network online, there is often some amount of calibration of activity involved with honing the number of machines, network dynamics, and the intent of the exercise. For this Cyber Forge, the graph in Figure 2 shows an initial spike of NPC timeline activity in the first week. After collecting feedback from observers, participants, and the network itself, researchers made the decision to decrease the frequencies of timeline activity. As the data collected in second week shows, a reasonable activity equilibrium was reached and maintained through the remainder of the exercise.

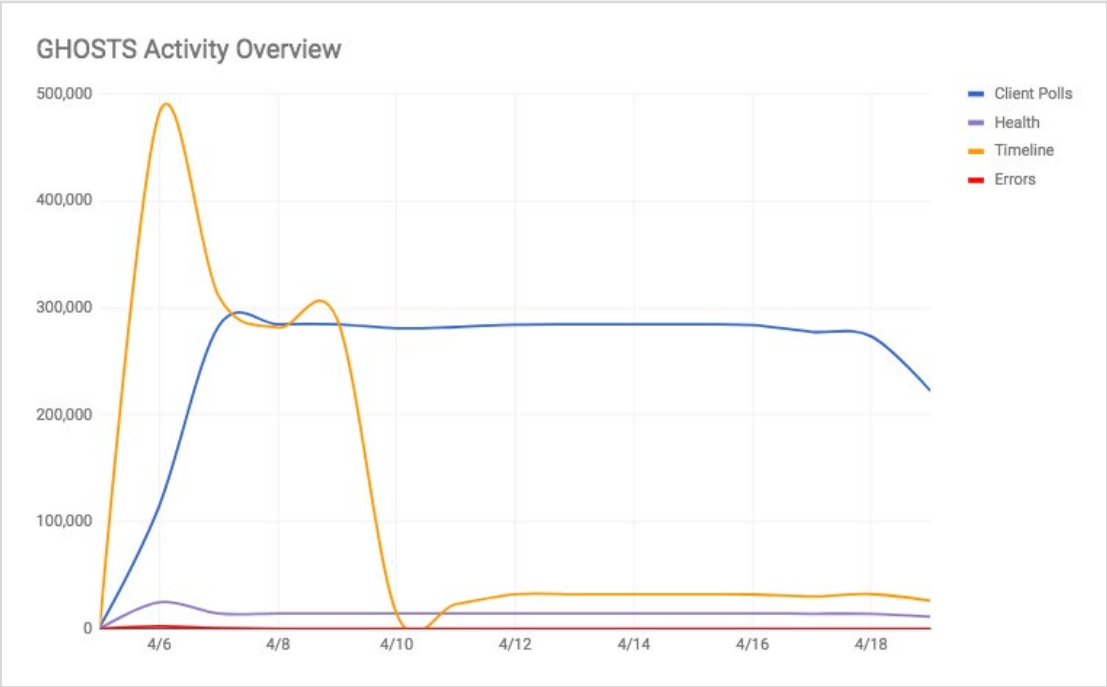

Figure 1: GHOSTS Cyber Forge Activity Overview

A summary GHOSTS performance data for this Cyber Forge, shown in Table 3, provides a breakdown of client operations over the exercise period.

Table 3: GHOSTS Cyber Forge Exercise Performance Summary

NPC Hours Managed	34,579
NPCs Tracked	100
NPC Timeline Operations	1,652,958
NPC Health Operations - Health Issues Identified	205,598 2,775
NPC Polling Events - Requested NPC Updates - Posted NPC Results	3,726,842 1,864,773 1,862,069

With respect to NPC activity, CWD researchers were entirely hands off after initial deployment in terms of administration and made no modifications to client configurations throughout the exercise. For specific injects, researchers were able to send individual machines new configurations that ran specific browser, script, and PowerShell commands as outlined by the inject timeline. From a player point of view, these injects played out just as if someone sat at their computer workstation and did the specific timeline commands themselves.

The number of active participants in each Cyber Forge exercise were 18, 20, and 24 people. At the end of each exercise, we asked each participant to complete a comprehensive survey on their

team and individual experiences. Participants were asked to rate the exercise for realism, team training value, and individual training value from 1 to 5, with 1 being the lowest score and 5 the highest. Ultimately, we had 5, 7, and 10 survey entries submitted across the three exercises. Figure 2 details the averages for these submitted scores.

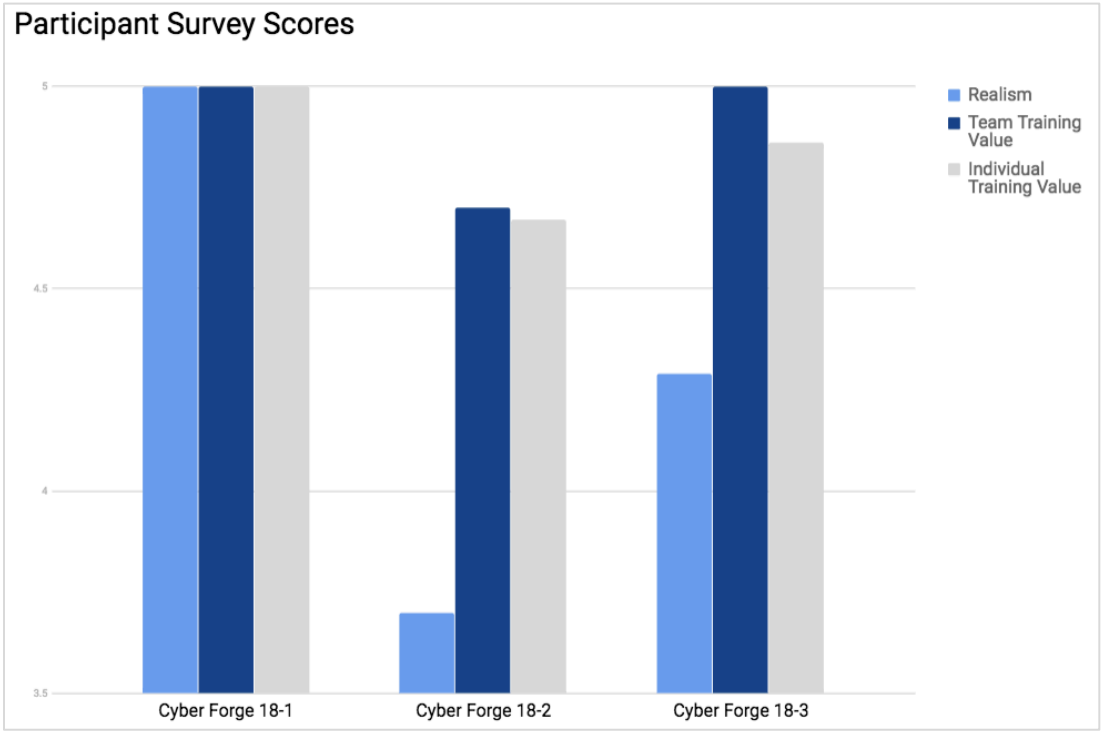

Figure 2: Cyber Forge Exercise Participant Survey Scores

The results obtained above show that participants reported that the exercises provided a high level of realism. Moreover, higher realism scores correlated with higher perceived value for both individual as well as team training.

Because each Cyber Forge exercise is sufficiently different than any other, from team experience to participant expectations of training focus, variance in the survey scores was expected. However, CWD researchers remain focused on providing high levels of realism and training value. Therefore, these scores are monitored appropriately.

5 Conclusion

This report outlined some of the challenges involved in creating cyber-warfare exercises, and proposed CERT's GHOSTS framework as a method for achieving highly realistic scenarios for those exercises. The case study we outlined showed that participants equated higher realism with greater training value.

CWD research has found, throughout the process of supporting exercises with player teams, that a strong undertone of trust emerges among players and facilitators. This trust is in large part born out of the realism of the exercise and our strict adherence to both the scenario and the ROE. When facilitators explain the GHOSTS framework and how it presents human-like NPCs on a network that engages in various activities, but is not directly responsible for dubious activity, the discussion sets player expectation for realism. They do not expect exercise events to happen via some sort of network 'magic' that cannot be accounted for at the end of exercise debrief. As a result, higher player expectation for realism leads to greater trust and, ultimately, greater training value for cyber-warfare exercises.

Further, the GHOSTS framework shows promising possibilities for future research and development. Researchers believe that collecting a rich set of client telemetry data across all machines and making that data available via a robust server API enables orchestration, machine-learning, and eventually artificial intelligence applications that use the range data to better coordinate timelines of activity of individual NPCs. In so doing, NPCs could deliver complex exercise scenarios requiring the coordination of multiple events to accomplish – such as large-scale distributed denial of service (DDoS) attacks.

References

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

[Berk 2012]
Berk, Vincent H.; Gregorio-de Souza, Ian; & Murphy, John P. Generating realistic environments for cyber operations development, testing, and training. In *Proc. SPIE 8359, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, 835908*. June 2012.

[Dobson 2017]
Dobson, Geoffrey B.; Podnar, Thomas G.; Cerini, Adam D.; & Osterritter, Luke J. *R-EACTR: A Framework for Designing Realistic Cyber Warfare Exercises*. CMU/SEI-2017-TR-004. Software Engineering Institute, Carnegie Mellon University. 2017. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=505224

[Osborne 2009]
Osborne, Martin J. *An Introduction to Game Theory.* Oxford University Press. Page 155. 2009.

[Wooldridge 1995]
Wooldridge, Michael & Jennings, Nicholas. Intelligent Agents: Theory and Practice. *The Knowledge Engineering Review*. Volume 10. Issue 2. June 1995. Pages 115-152.

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 2018	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
GHOSTS in the Machine: A Framework for Cyber-Warfare Exercise NPC Simulation	FA8702-15-D-0002

1. AUTHOR(S)

Dustin D. Updyke, Geoffrey B. Dobson, Thomas G. Podnar, Luke J. Osterriter, Benjamin L. Earl, Adam D. Cerini

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2018-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)

This report introduces the GHOSTS ((G)eneral HOSTS) framework, the purpose of which is to create a high level of realism in cyber-warfare exercises by establishing and building behaviorally accurate, autonomous non-player characters (NPCs). The report outlines how the GHOSTS framework accomplishes the creation of simulations in which NPCs realistically represent a vast array of possible encounters and outcomes. The report concludes with a discussion of a case study in which the GHOSTS framework was used. Participants in the exercise reported high levels of realism, which in turn correlated with higher ratings for training value. These results indicate that the GHOSTS framework can be used to create training of the highest quality, effectively preparing cyber-warfare teams for success in real-world situations.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Cyber warfare, simulation, non-player characters	19

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