ARL-TR-7999 • Apr 2017

US Army Research Laboratory

Terra Defender Cyber-Physical Wargame

by Edward J Colbert, Daniel T Sullivan, John C Patrick,
Jason W Schaum, Ralph P Ritchey, Mark J Reinsfelder,
Nandi O Leslie, and Rosheim C Lewis

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-TR-7999 ● Apr 2017

US Army Research Laboratory

Terra Defender Cyber-Physical Wargame

by Edward J Colbert
Computational and Information Sciences Directorate, ARL

Daniel T Sullivan, Nandi O Leslie, and Rosheim C Lewis
Raytheon Company, Dulles, VA

John C Patrick, Jason W Schaum, Ralph P Ritchey, and Mark J Reinsfelder
ICF International, Columbia, MD

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* April 2017	**2. REPORT TYPE** Technical Report	**3. DATES COVERED (From - To)** 06/2016–12/2016

4. TITLE AND SUBTITLE Terra Defender Cyber-Physical Wargame	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Edward J Colbert, Daniel J Sullivan, John C Patrick, Jason W Schaum, Ralph P Ritchey, Mark J Reinsfelder, Nandi O Leslie, and Rosheim C Lewis	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) US Army Research Laboratory ATTN: RDRL-CIN-S 2800 Powder Mill Road Adelphi MD 20783-1138	**8. PERFORMING ORGANIZATION REPORT NUMBER** ARL-TR-7999
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The US Army Research Laboratory (ARL) “Terra” Wargame was conducted by the ARL Computational and Information Sciences Directorate, Network Science Division in December 2016. It helped to achieve a better understanding of how Army supervisory control and data acquisition (SCADA) system and device security can be modeled and managed. Terra game players obtained first-hand experience in attacking and defending a live (“operational”) SCADA system that was located in a testbed facility at the ARL Adelphi Laboratory Center, Maryland. In this report, we present an overview of the cyber-physical wargame events and provide a detailed record of the game events and team strategies.

15. SUBJECT TERMS

SCADA, supervisory control and data acquisition, ICS, industrial control system, CPS, cyber-physical system, cyber security, simulation, wargame

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Edward Colbert
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	54	**19b. TELEPHONE NUMBER (Include area code)** 301-394-1674

Contents

List of Figures

List of Tables

Acknowledgments

A special thanks is offered to the RED and BLUE team players who contributed freely in the December 2016 Terra wargame for their enthusiastic participation and very helpful feedback and advice for future US Army Research Laboratory wargames.

1. Background and Motivation

The general mission of the US Army Research Laboratory (ARL) is to discover and develop innovative research ideas and methods that are relevant to the US Army. As such, the Terra wargame provides sample "data" that may be encountered in an actual attack of a supervisory control and data acquisition (SCADA) system. The Computational and Information Sciences Directorate, Network Science Division is interested in creating security models (e.g., game-theoretic security models) that may be able to assist SCADA operators in protecting their system. Ideally, the security model would allow useful estimates of system security and performance metrics that prove to be otherwise challenging to define, since SCADA systems have such a diverse array of hardware, software, and corresponding vulnerabilities.

1.1 General Overview and Philosophy

The general idea for the Terra wargame was for the BLUE team (the "defenders") to guard a corporate SCADA system in a realistic setting. In our game, the Blue Corporation is a startup company that invented a revolutionary new wine decantering process using centrifuges controlled by programmable logic controllers (PLCs). The chief executive officer (CEO) of Blue Corporation financially supports a security team (the BLUE team) to defend against attacks on the decantering process. The BLUE team mission is to defend the industrial control system (ICS) and the relevant corporate network connected to the ICS.

An additional company, Red Corporation, who is in competition with Blue Corporation, decides to hire a team of experts (the RED team, or the "attackers") to stop the Blue Corporation decantering process by any means possible (e.g., cyber or physical attacks). Our game scenario included a "Red Team Funding Source" (RTFS), who, in real life, could be equivalent to the Red Corporation CEO, but may also be a third party that funds and directs the attacks. In our game, the RTFS financially supported the RED team in the same manner that the Blue Corporation CEO supported the BLUE team.

A third team (the WHITE team) organized and managed the activities of the Terra wargame. The intention of the WHITE team was to provide a wargame environment that was as similar as possible to a real-life scenario. For example, to simulate "Internet" cyber access, the RED team was provided with external access to a single switch that provided a gateway into the Blue Corporation network.

Terra was developed differently from many common "cyber" wargames, in that it was not meant to be solely for RED/BLUE competition or for BLUE team training.

It was meant to simulate a realistic attack and defense environment. In addition, Terra was developed as a cyber-physical wargame, with both cyber and physical attack vectors. Furthermore, Terra included a (secret) insider. Knowledge of the insider was only known by the RTFS, the RED team manager, and the RED team members. The BLUE team members were notified before the game started that an insider may be present, but nothing further. Even the organizers of the game, the WHITE team, did not know the identity of the insider.

The RED team could use cyberattacks, physical attacks, information or services from the insider, or a combination. The RED team would win if they stopped the centrifuges.

Each team was given currency (game-dollars or $GD) at the start of the game. As in real life, significant actions of the game players corresponded to winning or losing game-dollars. For example, the BLUE team could earn game-dollars by keeping critical services operational, and the RED team could earn game-dollars by achieving “capture the flag” (CTF) objectives or disabling critical services. If the RED team was unable to stop the centrifuges during gameplay, the team with the most currency at the end of the game would win. The rules of the game were established by the WHITE team. Penalties were defined for violation of these rules.

1.2 Intended Strategy

As mentioned, the WHITE team intended the maxim of “everything costs money, nothing is free” to be the foundation of the game. It was the objective of the WHITE team to provide the BLUE team with a “default” system security configuration and an appropriate amount of game-dollars so they could partially secure their system. As the game progressed, the BLUE team was expected to use additional earned game-dollars to purchase technical “add-ons” to strengthen their security posture.

The RED team started the game with the same amount of game-dollars as the BLUE team. As their setup, they were given the IP network range of their local area network (LAN) and the make and model of the target PLC, but no additional information (i.e., practically blind). In a real-world scenario, attackers will typically conduct extensive intelligence operations for a long period of time before attacking. Based upon the intelligence assessments of this reconnaissance activity, they would then plan their strategy and purchase technical aids (such as attack tools). However, since the Terra wargame was a 1-day attack and defense activity, it was impractical to include the reconnaissance phase into the Terra wargame. As a compromise, ARL offered an insider who could sell equivalent information and services to the RED team.

As mentioned, ARL intended for the wargame to be as realistic as possible. The wargame was scheduled over a 24-h period so as to include an “after-hours” setting when a corporate network would have fewer security defenders and could be more vulnerable to attacks.

The intention was for the WHITE team to only provide gameplay information and adjudication after the start of the wargame and not intervene in the gameplay by assisting either team.

1.3 Organizational Models

In this section, we describe the Terra game structure and model for the BLUE, RED, and WHITE teams.

1.3.1 BLUE Team

The BLUE team game model is similar to that of a Security Operations Center, which manages and monitors all network elements, computers, and technical assets of the company. Their mission is to protect the Blue Corporation decantering process from external threats and insiders. Their highest priority is to keep the centrifuges operating at 100% availability.

The BLUE team organizational structure is shown in Fig. 1. In this scenario, the BLUE team members are managed by a Security Team Manager (BLUE team lead), who is in turn managed by the Blue Corporation CEO. The CEO manages the investment of game-dollars for protecting company assets, in collaboration with the Security Team Manager.

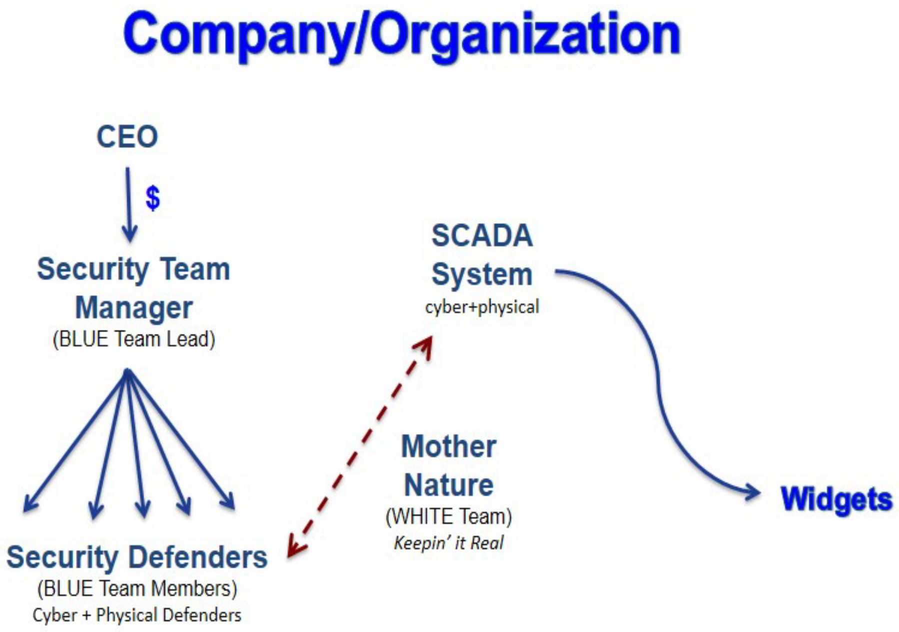

Fig. 1 BLUE team organizational structure for the Terra wargame

1.3.2 RED Team

Figure 2 illustrates the wargame model for the RED team organization (i.e., the attacking entity). The RED team members represent a team of attackers who are managed by the Attack Team Manager (RED team lead). The Attack Team Manager works with the funding source (the RTFS) to devise a strategy for stopping the Blue Corporation centrifuges. The RTFS financially supports the RED team and works closely with the RED team lead to devise attack strategies. As mentioned, a (secret) insider was available to provide information and services to the team, via consultation with the RTFS and the RED team lead.

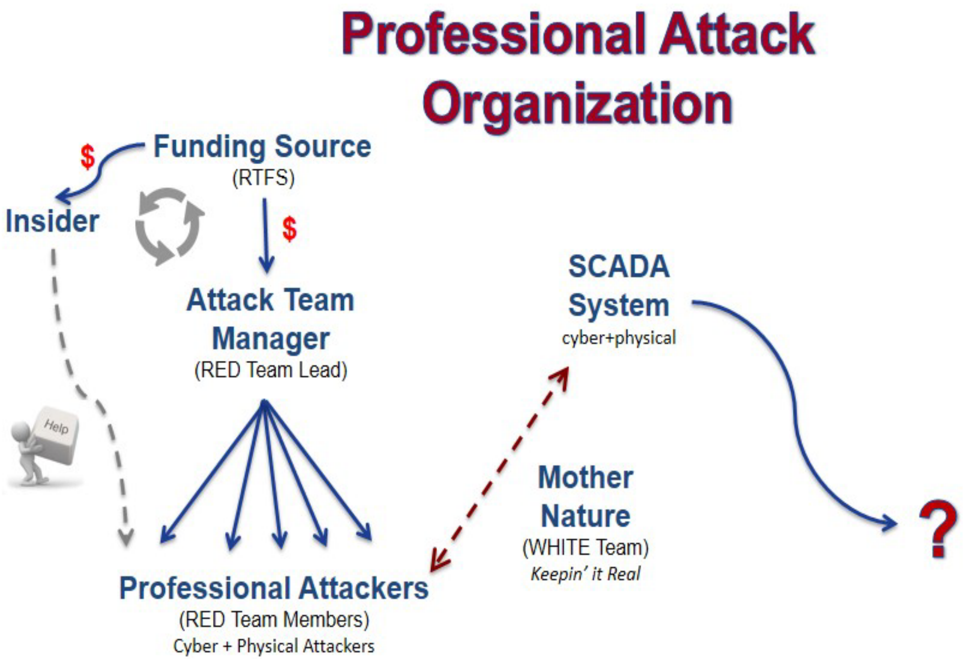

Fig. 2 RED team organizational structure for the Terra wargame

1.3.3 WHITE Team

The WHITE team functioned as the game designer and, when the game began, as the adjudicator. The main focus of the WHITE team was to design the game to simulate a realistic scenario in which events and actions that would cost money in real life would also cost money in the wargame. WHITE team functions for Terra included the following:

- Technical and administrative support for game logistics
- Design and development of gameplay strategy and rules
- Validation of gameplay design via tabletop RED/BLUE simulation activities
- Adjudication of gameplay activities
- Technical assistance to RED and BLUE team members, as needed
- Setup and tear-down of technical infrastructure
- Assessment and recording of gameplay activities

The "Prime Directives" of the WHITE team were 2-fold:

- Keep it Real.
- Keep People Happy.

Approved for public release; distribution unlimited.

In practice, there is a delicate balance between these 2 directives, and careful planning is needed to ensure that neither supersedes the other.

2. Terra Game Development and Gameplay

The Terra wargame WHITE team worked for several months to develop the game. Sample activities include recruiting the teams, designing the game infrastructure, conducting the tabletop RED/BLUE team simulation, and assigning pricing methods for each team. We discuss these activities in detail in the following sections.

2.1 Team Selection

Membership on the RED and BLUE teams was selected from a pool of volunteers from local organizations. Volunteers were required to request team membership in an email sent via the Internet to the WHITE team by the deadline of 28 October. A sample announcement that was circulated to various groups and organizations is shown in Appendix A.

Team captains were selected by the WHITE team and were notified of their individual members soon after the 28 October deadline. Game strategizing began at that point.

Due to some initial attrition of team members and requests by team captains for additional members, a second round of volunteers was recruited at a later date and each team acquired a small number of additional members on 6 December.

Members of both teams were asked not to share any information about their teams, including their team roster, to any other team. Although there was a $GD 500 penalty for violations of this rule, no evidence was brought forward to the WHITE team to indicate that this rule was violated. However, it was suspected that some collusion took place between RED and BLUE team members who worked for the same organization, or who communicated regularly using private corporate networks.

All of the WHITE team members were ARL civilian or contractor staff, and all are coauthors of this report. One of the team members (the WHITE team lead) was the primary point of contact (POC) for the Terra games and this person selected and managed the other WHITE team members who took responsibility for specific WHITE team activities.

2.2 Team Roles and Members

The BLUE and RED team rosters are shown in Tables 1 and 2. The names and organizations for Terra team players have been anonymized for this report. We use shorthand notation with curly brackets to denote a player throughout the report. For example, "{B0}" is from "Company Alpha" and played the role of Blue Corporation CEO in the game

Table 1 BLUE team roster

Player name	Player organization	Terra game role
{B0}	Company Alpha	Blue Corporation CEO (funding source)
{B1}	Company Alpha	Scribe for BLUE team activities BLUE team POC for WHITE team adjudication
{B2}	Company Bravo	BLUE Team Captain
{B3}	Company Alpha	As assigned by BLUE Team Captain
{B4}	Company Bravo	
{B5}	Company Bravo	
{B6}	Company Bravo	
{B7}	Company Alpha	

Table 2 RED team roster

Player name	Player organization	Terra game role
{R0}	Company Alpha	RTFS (15 Oct–8 Dec 2016) Insider (15 Oct–8 Dec)
{R1}	Company Alpha	RFTS (9–14 Dec) Insider (9–14 Dec) Scribe for RED team activities RED team POC for WHITE team adjudication
{R2}	Company Charlie	Team Captain
{R3}	Company Bravo	As assigned by RED Team Captain
{R4}	Company Alpha	
{R5}	Company Bravo	
{R6}	Company Alpha	
{R7}	Company Bravo	
{R8}	Company Delta	

The Blue Corporation CEO and RTFS acted as liaisons to the WHITE team starting when the teams were selected.

The insider role was initially fulfilled by {R0}. Since {R0} was not able to be present during gameplay week, {R1} took over all activities of {R0} on Friday, 9 December.

After teams were selected, the BLUE and RED team captains organized their own communication methods for strategizing. The WHITE team offered telephone bridges for regular weekly teleconferences. Some of the BLUE team members participated in the telephone bridges to ask questions to the WHITE team about the wargame. A few of the BLUE team members worked at common locations and planned in-person meetings to discuss strategy. Internet email (and perhaps private corporate email) were the primary communication modes for BLUE and RED team strategizing.

The RTFS and RED team lead began discussing usage of insider services after team selection. The intention was for the RTFS, the RED team lead, and the insider to discuss terms privately, and for the RED team lead to then communicate the insider bargain with the RED team members. The insider was available to provide technical and strategic information, and potentially divert or destroy BLUE team operations services with covert missions. As mentioned, the insider identity was never shared with the WHITE or BLUE teams until the wargame out-brief (after the wargame ended). Due to limited personnel availability during the Terra game, the person acting as the RTFS also played the role of the insider.

For convenience during gameplay, a POC was identified on each team to facilitate rapid adjudication by the WHITE team.

2.3 Blue Corporation System Setup

On 14 November 2016, the WHITE team emailed a technical document describing the game setup to the BLUE team (see Appendix B). This document included a general system diagram and some Blue Corporation network and security information. The BLUE team leveraged this document to develop their initial security configuration. The WHITE team provided an additional diagram describing network and data flow information on Monday, 12 December, after the in-brief.

While these diagrams were not supposed to be shared with RED team members, one of the RED team members was found with one of the Blue Corporation diagrams during gameplay. However, since the BLUE team did not propose this violation to be adjudicated, no penalties were imposed.

2.4 Game Strategy Development and Pricing Methods

One of the most important aspects of the Terra game design was to create a realistic environment that would have clearly defined rules and penalties and, at the same time, would offer considerable challenges to each team during the 24 h of gameplay. This proved to be more difficult than anticipated and we noted after the game ended that much more effort and time were needed in this area. In the following subsections, we describe 4 general activities of the game design: a tabletop RED/BLUE team simulation exercise, creating the game rules, pricing of team tools, and estimation of starting funds. All of these activities were conducted by the WHITE team before gameplay began.

The WHITE team made a considerable effort to design a (nearly) zero-sum wargame by moving game-dollars from one team to the other in the event of a violation or penalty. As mentioned, each team was allowed to gain additional game-dollars from the WHITE team during gameplay, and the insider acted to subtract game-dollars from the game. This feature of the game deviated from a zero-sum game design, but it was considered a necessary part of the game to motivate players.

2.4.1 Tabletop Exercise

The purpose of the tabletop RED/BLUE simulation exercise was to estimate the decisions and actions of the defenders and attackers during the gameplay, so that the initial game scenario would be reasonable and fair, and also challenging and adventurous for the game players.

Five members of the WHITE team met on 16 November for 2 h to conduct a tabletop exercise of the wargame. The following goals were defined for the activity:

- Document the details of the expected RED and BLUE team strategies.
- Estimate the material and labor costs for the BLUE team to mitigate vulnerabilities in the Blue Corporation network.

In the Terra wargame, the intended motivation of the RED and BLUE teams was to win game-dollars and/or attack/defend the centrifuges, and it was assumed that the players would make decisions based on these game goals.

The results of the tabletop simulation were used to estimate the beginning amount of game-dollars to be given to each team (see Section 2.4.4).

2.4.2 Gameplay Rules and Penalties

In this section, we describe the detailed gameplay rules and penalties presented during the Monday in-brief.

2.4.2.1 General ARL Policies

The wargame participants had to adhere to ARL policies and were given the following rules to that effect:

- You may not connect your laptops, USB devices, or other equipment to the ARL enterprise network or PCs.

- You may not tamper with any ARL PC, device, or equipment that is not part of this wargame (wargame computers were identified with labels).
- You may not connect to or try to hack the ARL wireless network.
- You may not subvert ARL policies or procedures.
- Bluetooth, wireless, camera, and microphone functions on all personal electronic devices (PEDs) must be disabled before bringing the PED into the facility.

2.4.2.2 Rules for Both the RED and BLUE Teams

The following activities were allowed in the wargame:

- Network scanning
- Active response measures such as Transmission Control Protocol (TCP) resets
- Physical tampering of wargame equipment
- Physical intrusion into the adversary's work area. If challenged, the intruder must retreat.
- Malware (after the wargame ends, teams must disclose any malware used, what was impacted, and how to remove)

Each team was permitted a debt up to $GD 10,000. If a team exceeded $GD 10,000 debt, the WHITE team adjudicator would decide whether to continue the game.

To win a cash prize (in game-dollars), the WHITE team must be presented the following as proof:

- Screen capture with a timestamp of the accomplishment
- Written notes describing the actions with the date and time

In lieu of writing notes, each player could win $GD 2,000 for 24 h of screen recording (12 fps minimum). The WHITE team provided each team with a spiral notebook as well as an USB hard drive to store video or electronic notes.

To facilitate analysis of the game activities, team members are asked to record their activities and actions, to include the date and time. However, the WHITE team did not offer game-dollar rewards for these actions and this probably caused low motivation for note-taking. In general, few players provided notes of their individual actions.

2.4.2.3 BLUE Team Rules

The following rules applied specifically to the BLUE team:

- BLUE team wins $GD 100 per hour for each critical service that is up (max $GD 600 per hour). Critical services are the following:
    - Company public web site
    - Company ecommerce web site
    - Company email web portal
    - Company email server
    - Human–machine interface (HMI)
    - Historian
- BLUE team must show a screen capture of the Hypertext Transfer Protocol (HTTP)/ HTTP Secure (HTTPS) header with a timestamp for the web sites, email web portal, HMI web screen, and Historian web screen.
    - Tools such as wget or other scripting tools can capture the headers.
- To win cash for an hour, the screen captures for the beginning and ending of the hour must be within 50–70 min.
- To earn cash for an operational email server each hour, the BLUE team must satisfy the following:
    - Send and receive emails at the start of the hour
    - Send and receive emails at the end of the hour
    - The start and end times of an hour may be 50 to 70 min apart.
- BLUE team loses $GD 25 for each 15 min of downtime for a critical service. See the following examples:
    - Down 15 min, receive $GD 75
    - Down 30 min, receive $GD 50
    - Down 45 min, receive $GD 25
- BLUE team takes $GD 100 from the RED team for completing an incident report for each cyberattack detected:
    - Incident report must contain a description (minimum of 20 words) of what happened, date/time, source and destination IP addresses,

    - what service or software was impacted, and the actions taken to remediate.
    - The game adjudicator will verify the RED team as the culprit before transferring money from the RED team to the BLUE team.
- BLUE team must keep the following public services open to any external IP address:
    - Company web site
    - Company ecommerce web site
    - Company email Simple Mail Transfer Protocol (SMTP) service
    - Company web email
    - $GD 1,000 penalty if a service is blocked to an external IP address
- BLUE team will pay $GD 500 penalty for each restore from a snapshot of a virtual machine (VM) hosting a public service (company web site, ecommerce web site, email web portal, email SMTP service).

2.4.2.4 RED Team Rules

The following rules applied to RED team actions:

- RED team takes $GD 1,000 from the BLUE team for each CTF goal. Total winnings could be $GD 5,000. The following are the goals:
    - Capture a text document of usernames and passwords from a PC.
    - Capture the network diagram.
    - Capture a PLC project file.
    - Deface a company web.
    - Create new user accounts in Active Directory.
    - Note: A file for a CTF objective will be in a folder named "RED-TEAM-OBJECTIVE".
- RED team takes $GD 200 from BLUE team for each hour a critical service is stopped.

2.4.2.5 Penalties

The WHITE team designed penalties for violations of rules. As mentioned, penalties were to be paid in game-dollars to the opposing team.

All penalties for violations transfer dollars from one team to the other team. The WHITE team did not tell the other team why they are receiving the cash until after the game:

- $GD 500 for sharing information with people not on their team
- $GD 500 for using an unapproved tool (i.e., a tool the WHITE team has not reviewed and assessed a cost)
- $GD 1,000 for late submission of the tool list
- $GD 1,000 if the BLUE team blocks access to a public service (corporate web page, ecommerce web page, SMTP service, email web portal)
- $GD 500 for not wearing team identification

In the event that a RED team member is caught in the server room by a BLUE team member, the RED team member is "arrested" (not allowed to play). Eyewitness or other physical evidence is required to adjudicate the arrest.

2.4.3 Tool Pricing

Before the game began, both the RED and BLUE teams were required to submit a list of the attack and defense tools they wanted to use during the game. These tools were priced by the WHITE team and the appropriate $GD currency was subtracted from the team bank accounts. For tools that were custom developed, the tool cost was the estimated development time using a developer wage of $GD 100/h. The RED team tools were estimated to cost about US dollars ($USD) 29K, if purchased new. A detailed list of tools used by the RED team follows in Table 3.

Table 3 RED team tools and costs

Tool	Acquisition cost ($USD)	Price source
Burp Suite Pro	$349	https://portswigger.net/buy/
Nessus Pro with the SCADA packs	$2,190	https://store.tenable.com/index.php?main_page=product_info&cPath=1&products_id=94)\
Siemens Simatic STEP 7 Professional V13	$1883.93	https://www.plc-city.com/shop/en/search?controller=search&orderby=position&orderway=desc&search_query=6ES7822-1AA03-0YA5&submit_search=
Network Miner Pro	$900	http://www.netresec.com/?page=BuyNetworkMiner
Metasploit Pro	$17,000	Price quote from Rapid 7
Sourcefire Rulesets	$5,000	The commercial rulesets are only available to customers with a Sourcefire sensor and annual maintenance. The WHITE team estimated $5,000 for the Red Team to purchase a sensor and maintenance contract
SerialTest/ComProbe/ComProbe II - RS-485/RS-232 serial sniffer	$1,395	http://shop.fte.com/RS-422485-ComProbe_p_15.html
Tcpdump/Windump	$0	Included in free Kali Linux
Wireshark	$0	
Nmap	$0	
OpenVAS with ICS Plugins	$0	
John The Ripper	$0	
Customized Python scripts	$200	The developer spent 2 h writing the scripts. The WHITE team assessed the labor rate at $100 per hour for a developer to write scripts.
Total Acquisition Cost	$28,917.93	

As shown in Table 4, the BLUE team tools did not cost any game-dollars, because they used freely available or open-source products.

Table 4 BLUE team tools and costs

Tool	Acquisition cost	Price source
Nmap	$0	Free to use from https://nmap.org/
Tcpdump	$0	Free to use from http://www.tcpdump.org/
Wireshark	$0	Free to use from https://www.wireshark.org/
Snort	$0	Free to use from https://www.snort.org/
Bro	$0	Free to use from https://www.bro.org/
Splunk Free	$0	License is free for indexing up to 500 megabytes (MBs) of data per day. See [1].
Splunk Universal Forwarder	$0	Free to use from https://www.splunk.com/en_us/download/universal-forwarder.html
DarkEther	$0	Tool built by US Government, not publically available
GRASSMARLIN	$0	Free to use from https://github.com/iadgov/GRASSMARLIN
rsyslog	$0	Free to use from http://www.rsyslog.com/
System Monitor (Sysmon)	$0	Free to use from https://technet.microsoft.com/en-us/sysinternals/sysmon
Backbox Linux with Project Redpoint Nmap scripts	$0	Free open source community project from https://backbox.org/
Dshell	$0	Free to use from https://github.com/USArmyResearchLab/Dshell
TShark	$0	Free to use from https://www.wireshark.org/download.html
Total Acquisition Cost	$0	

One of the BLUE team's tools was Splunk Free, which has a free license for indexing less than 500 MB of data per day.[1] If the volume of network collected data exceeded 500 MB per day, the WHITE team would have assessed a license fee of $GD 1,800 to the BLUE team's budget. This is the equivalent cost in $USD of an annual commercial license cost for Splunk Enterprise for 1 to less than 10 GB of data indexed per day.[2]

2.4.4 Team Starting Funds

The desire was for both teams to start gameplay with equitable bank account balances to make the game fair. Based on estimated tools to be used and the results of the tabletop exercise, the WHITE team decided the RED and BLUE teams would each start with a bank balance of $GD 11,200.

The BLUE team purchased a Cisco Adaptive Security Appliance (ASA) 5515 firewall, for a purchase price of $GD 1975, leaving them $GD 9,225 at game start.

The RED team requested to experiment with a Siemens S7-300 PLC on Tuesday, 13 December, the day before gameplay. The RED team accepted the WHITE team's price of $GD 1,500 for 1) usage of the PLC and 2) WHITE team labor to set up the PLC. The WHITE team prorated the RED team tools at $GD 1,500 since the tools would normally have been expected to be reused for other attacks by the professional attack organization. Taking into account these 2 purchases, the RED team starting balance came to $GD 8,200.

3. Gameplay

In this section, we present the gameplay week schedule, the physical layout of the wargame, each team's strategy, and the Terra final results.

3.1 Schedule

The Terra wargame events spanned 1 week (Monday–Friday), with the 24-h attack and defense event starting Wednesday morning. We show the complete schedule for the Terra gameplay week in Table 5.

Table 5 Schedule for Terra wargame (12–16 Dec 2016)

Day	Planned Terra events
Mon 12 Dec	In-brief and BLUE team preparation
Tue 13 Dec	Continue BLUE team preparation RED team tinkers with spare S7-300 PLC. WHITE team tests wargame network.
Wed 14 Dec	Wargame starts at 0900.
Thu 15 Dec	Wargame ends at 0900. WHITE team collects artifacts and prepares results.
Fri 16 Dec	WHITE team presents out-brief on Terra results.

Both teams received an in-brief and a tour of the ARL wargame facility on Monday, when the Terra wargame rules were described in full. Game preparation occurred on Monday after the in-brief and all day Tuesday. The WHITE team cleaned up the wargame environment and collected "data" on Thursday, and presented an out-brief to all interested wargame players on Friday.

3.2 Physical and Logical Game Environment

The diagram shown in Fig. 3 was provided to BLUE and RED team members during the in-brief. This describes the physical locations of each team within the ARL facility. Details of ARL room numbers have been removed for publication. Both teams had physical access to all areas during gameplay.

Due to cramped quarters in the Army Cyber-research and Analytics Laboratory (ACAL), the WHITE team agreed to move the BLUE team to a larger space closer to the SCADA equipment (see red items in Fig. 3). This compromise unfortunately positioned the BLUE team directly adjacent (and blocking entry to) the Blue Corporation SCADA equipment and made it much more difficult for the RED team to execute physical attacks.

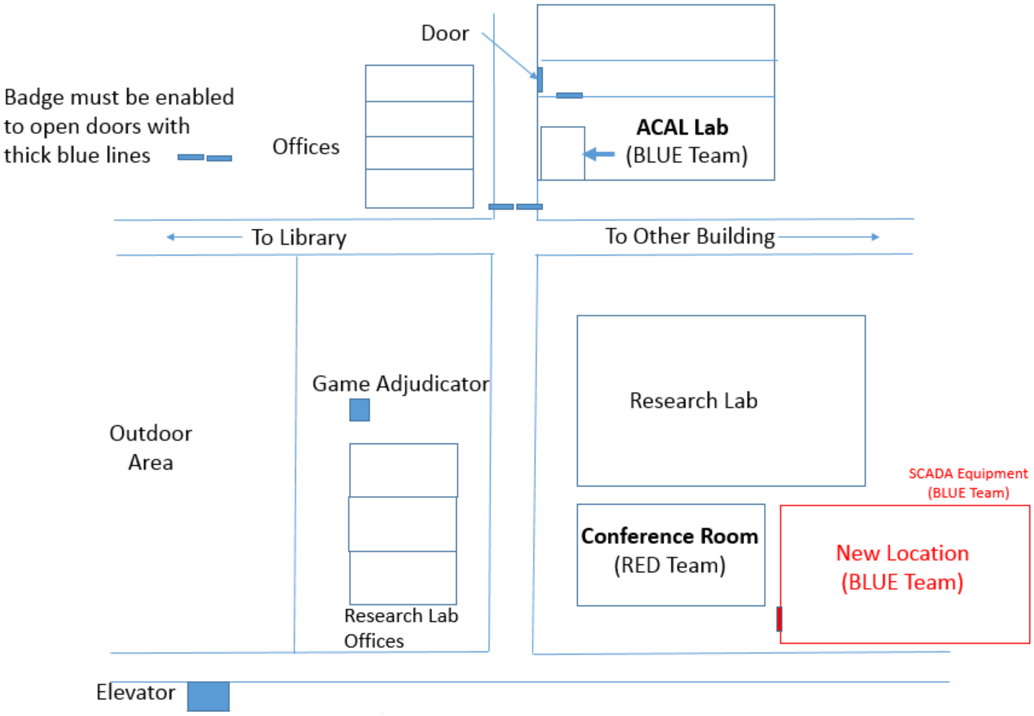

Fig. 3 Initial physical layout for Terra wargame teams. The red items in this drawing were not in the original handout; they were added for clarity (see text).

The RED team view of the Blue Corporation network is indicated in Fig. 4. As noted, they were mostly blind coming into the wargame, which made their strategy planning very time-critical.

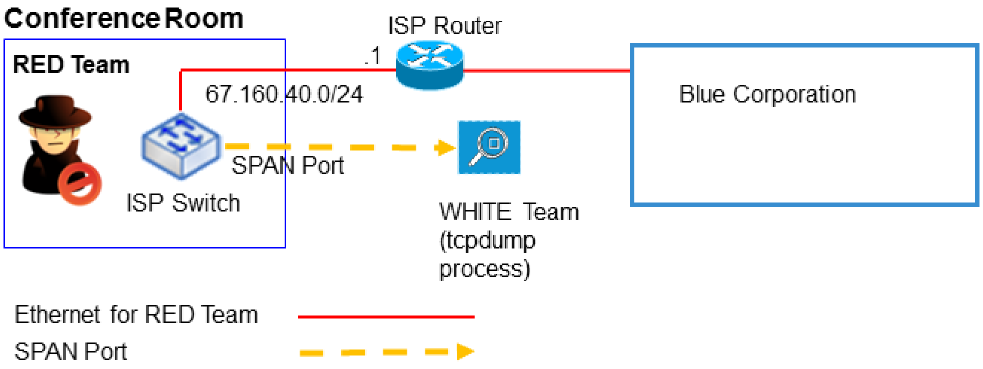

Fig. 4 RED team view of the Blue Corporation network

Approved for public release; distribution unlimited.

3.3 Strategies Used

As mentioned, the RED team had several strategies available for attack:

- Cyberattack only
- Cyber and physical attack
- Physical attack
- Usage of information provided by the insider to enhance the cyber and/or physical attack
- Usage of insider services, such as persuading a BLUE team member to degrade or destroy Blue Corporation security

The actual strategy used by the RED team was a cyber-centric strategy. Although the RED team lead was interested in using the insider, the RED team members generally did not express interest.

One strategy that could have been adopted by the RED team was to purchase small increments of information from the insider as they developed their cyber and physical attack plan. Since the insider was available before game week, this might have allowed the RED team to be more conservative with the list of tools desired, thus increasing their starting balance of game-dollars.

The BLUE team chose the following strategies:

- Use industry best practices to secure the Blue Corporation network. The best practices included using strong passwords, disconnect unused network connections, disable unused switch ports, replace Telnet with secure shell (SSH), disable unused services, disable unused email accounts, and upgrade Windows XP hosts to use Windows 7 operating system (OS).
- Segment the ICS network from the corporate network.
- Protect the ICS network with a firewall.
- Place public-facing web servers in a demilitarized zone (DMZ).
- Use Bro and Snort for intrusion detection systems.
- Install Sysmon on all Windows hosts with the Splunk universal forwarder. Sysmon would detect the presence of new processes, which could be started by RED team malware.
- Send Bro, Snort, and Sysmon data to Splunk Free to correlate events and provide situational awareness to the BLUE team.

On 12 December, the BLUE team purchased a firewall from the WHITE team to protect the ICS network and then implemented mitigations from 12 to 13 December.

During setup during gameplay week (Monday and Tuesday), both the RED and BLUE teams spent time developing their strategies. The RED team members tinkered with the Siemens PLC while the BLUE team members examined the SCADA system setup and began locking down their system.

3.4 Record of Events

The following data were collected by the WHITE team after the 24-h event. The person that provided the data is noted in parenthesis, as appropriate:

- Game-play notes from Wednesday, 14 December
- RED team POC/RTFS ({R1})
- BLUE team POC ({B1})
- WHITE team lead
- WHITE team interviews with team members {B3}, {B5}, {R1}, and {R2}.
- Packet capture files from Wednesday, 14 December
- RED team switch for the switched port analyzer (SPAN) port
- DMZ virtual switch for the SPAN port
- Corporate network switch for the SPAN port
- Network Management switch for the SPAN port
- ICS switch for the SPAN port
- Screen captures provided by the BLUE team for adjudication purposes
- Bank account ledgers
- RED team
- BLUE team
- BLUE team Splunk logs and network element configuration files ({B4})

A complete list of Terra gameplay events, reconstructed from the notes and other data listed in this section, is provided in Table C-1 in Appendix C.

3.5 Final Results: BLUE and RED Team Game-Dollar Ledgers

In Table 6, we list the BLUE team's bank balance and expenditures. The BLUE team purchased a firewall and won several game-dollar awards for providing evidence that critical services were operational.

Table 6 BLUE team transactions

Transaction	Value (Game-Dollars)	Balance (Game-Dollars)
Starting Balance		$11,200
Purchase: Cisco ASA 5515 Firewall	($1,975)	$9,225
Award: HMI Server up 0900-1000	$100	$9,325
Award: Email web server up 1000-1100	$100	$9,425
Award: Public web server up 1000-1100	$100	$9,525
Award: E-commerce web server up 1000-1100	$100	$9,625
Award: HMI server up 1100-1200	$100	Final: $9,725

The RED team's ledger is shown in Table 7. The RED team purchased tools and time and materials to tinker with a spare Siemens PLC. The RED team did not win any game-dollar awards.

Table 7 RED team transactions

Transaction	Value (Game-Dollars)	Balance (Game-Dollars)
Starting Balance		$11,200
Purchase: Commercial Tools	($1,500)	$9,700
Purchase: Tinkering with Siemens PLC	($1,500)	Final: $8,200

4. Discussion

Terra was a wargame between RED and BLUE team players who were very experienced cyber professionals. Many of them had participated in cyber wargames, but never in a cyber-physical wargame. In general, most or many of the members of the RED team were reluctant to use the insider as part of their strategy, even though the RED team lead did have an interest.

The Terra WHITE team succeeded partly in providing a realistic environment for both the attackers and the defenders (Prime Directive 1). Overall, they also achieved Prime Directive 2, which was to keep the players happy. The fact that the experience was unfamiliar and unexpected for many of the players led to some unplanned compromises (e.g., creative tool pricing and a change in the BLUE team location) in the WHITE team game strategy during gameplay. In addition, this was the first wargame for ARL, and some mistakes were made that led to further confusion among the players.

The final result of the game was that the RED team was unable to breach the Blue Corporation's defenses, they did not stop the centrifuges, and they had the least amount of game-dollars when the game ended. The RED team lost the game. However, the Terra game was a learning experience for all, and in general, everyone worked hard and expressed that they did get something out of the game, even if it was just a learning experience about team play or technical experience with SCADA equipment. The RED team could have leveraged the insider to gain entry into the network or could have paid the insider to sabotage the centrifuges and might have executed a winning strategy, but they did not choose this method. Some RED team members expressed reluctance to use the insider because they said that they felt it was cheating, perhaps because they were used to the environments of previously played cyber wargames. Some players also expressed that the rules and goals of the game were not understood fully, and the ARL WHITE team has taken the action to improve this for future cyber-physical wargames.

As mentioned, the individual BLUE and RED team players did not keep detailed activity logs, even though it was requested by the WHITE team. The activity logs were highly desired by the WHITE team to reconstruct the individual moves made by each player, since a goal of the ARL SCADA research team is to be able to model the attacker and defender decisions and compare model predictions with actual data. The WHITE team learned that assessment of game activity is a very difficult endeavor. Future ARL wargame designers will need to spend much more effort in the game design so that player actions and decisions are more naturally recorded as part of the gameplay. The Terra "data" collected during the gameplay came mostly from careful reconstructions using observations of the WHITE team and notes from the BLUE and RED team scribes.

During the out-brief on Friday of game-week, nearly all of the players in attendance provided useful feedback for improving the wargame strategy. This feedback was extremely helpful and resulted in a number of changes in ARL plans for future wargame development. The principal action is that the WHITE team must indeed identify, enumerate, and simulate the attack and defense decisions expected in the game at a much higher competence level. The tabletop exercise described in

Section 2.4.1 was intended to serve this purpose, but not enough time was spent preparing this. As a result, there were not many successful winning RED team strategies available by the time the event started at 0900 on Wednesday. By that time, the BLUE team had locked the cyber routes and had also situated themselves to make physical attack vectors difficult. Since the Terra wargame philosophy is not to assist either team once gameplay starts, it is extremely critical that the gameplay be balanced between the RED and BLUE teams. On the other hand, the WHITE team recognizes that in real life, often the attackers do fail quickly due to many circumstances, and they have to start over again with strategy planning. There needs to be a balance between realism and the creation of a "game" so that the players maintain interest during the critical time of gameplay, since the intensity of player action is concentrated in such a short time period (24 h in this case). Also, the WHITE team may offer alternatives to an insiders, such as pre-gathered intelligence for the RED team to purchase.

Certainly one of the most valuable lessons learned was that much more effort is needed to design and validate the gameplay rules and strategies, for example, using detailed playbooks and/or more extensive RED/BLUE tabletop exercises. In terms of the fraction of time spent on game preparation, this needs to take the highest priority over the setup of the SCADA equipment and other technical matters.

A number of technical aspects of a real corporate SCADA system were absent in the Terra game. For example, we did not have a steady stream of "corporate" traffic flowing in and out of "the Internet" (the RED team switch). There was no ability to search "the Internet" for clues on how the corporate network was operated (e.g., WHOIS lookups or information from a Blue Corporation web page). ARL needs to include the ability for the RED team to find this information in future cyber-physical wargames.

Despite the drawbacks, nearly all of the BLUE and RED team members were highly enthusiastic and generally appreciated the opportunity to participate in the activities, and we hope to be able to bring some of the same players back for a more adventurous experience.

5. References

Splunk Inc. About Splunk Free. San Francisco (CA): Splunk Inc. [accessed 2017 Jan 9]. https://docs.splunk.com/Documentation/Splunk/latest/Admin/MoreAboutSplunkFree.

Splunk Inc. Splunk Pricing. San Francisco (CA): Splunk Inc. [accessed 2017 Jan 9]. https://www.splunk.com/en_us/products/pricing.html#tabs/ent.

INTENTIONALLY LEFT BLANK.

Appendix A. Sample Wargame Advertisement

The following text is from a sample wargame recruiting advertisement for the US Army Research Laboratory Terra wargame. This particular example was sent by email on or about 7 October 2016.

US Army Research Laboratory Cyber-physical Wargame

What is it?

This is a cyber-physical “wargame” competition between players who defend and attack the process of a simulated SCADA system in a (simulated) corporate environment. Members will be part of various teams. For example, cyber players will be part of a red (cyber-offensive) and blue (cyber-defensive) team. Other teams will also be represented, such as a management team (e.g., system owner and operator) and a covert insider-threat team. Our physical SCADA configuration will utilize a Siemens S7-300 PLC that controls a centrifuge. The cyber network configuration will be a closed network with a simulated link to an external “Internet.” The game will be played with a highly realistic simulated corporation. For example, red team members will not be confined to cyber attacks from a pre-defined terminal – they will be free to access any part of the system that is unguarded by the blue team, including cyber connections, physical access, and indirect access via an insider.

Where is it?

This will be held at the Army Research Laboratory (ARL) Adelphi Laboratory Center (ALC) at 2800 Powder Mill Rd, Adelphi, MD 20783. The event will be held inside of an ARL building, so access to the base is required.

Who can participate?

Anyone with cyber hacking or cyber defender skills. Participants will need to be registered in JPAS and have identification for entering DoD bases, such as a CAC card.

Schedule:

01 Nov 2016: Team members are notified of their selection

10 Nov: Technical configuration document available to participants

Mon 12 Dec: Pre-game briefing for participants, describing gameplay rules

Tue 13 Dec: White team (wargame oversight) and blue team test additional defenses configured by blue team

Wed 14 Dec: GAME ACTIVITY starts approx. 0900

Thu 15 Dec: GAME ACTIVITY ends after duration of 24 hrs (approx.. 0900) White team collects artifacts from the wargame and prepares game results

Fri 16 Dec: Post-game summary briefing (optional) – discussion, awards, and lessons learned

Interested?

Please contact Edward Colbert (edward.j.colbert2.civ@mail.mil, 301-394-1674) or Dan Sullivan (daniel.t.sullivan12.ctr@mail.mil, 301-394-0248) at the US Army Research Lab before COB Oct 28, 2016

Appendix B. Read Ahead for the BLUE Team

The WHITE team emailed the following document to all BLUE team members on 14 November 2016. The document has been modified slightly to remove sensitive information such as personal names and US Army Research Laboratory room locations.

Read Ahead for BLUE Team

v1.0 – 14 Nov 2016

1. **General System Information**. Figure B-1 depicts the initial system topology. Two zones are established. The corporate zone (green network links) and industrial control system (ICS) zone (red network links) share a common (/24) network address. The management network (purple network links) enables remote access to the management ports on the network elements. The management network has its own /24 network address. The exercise network is isolated.

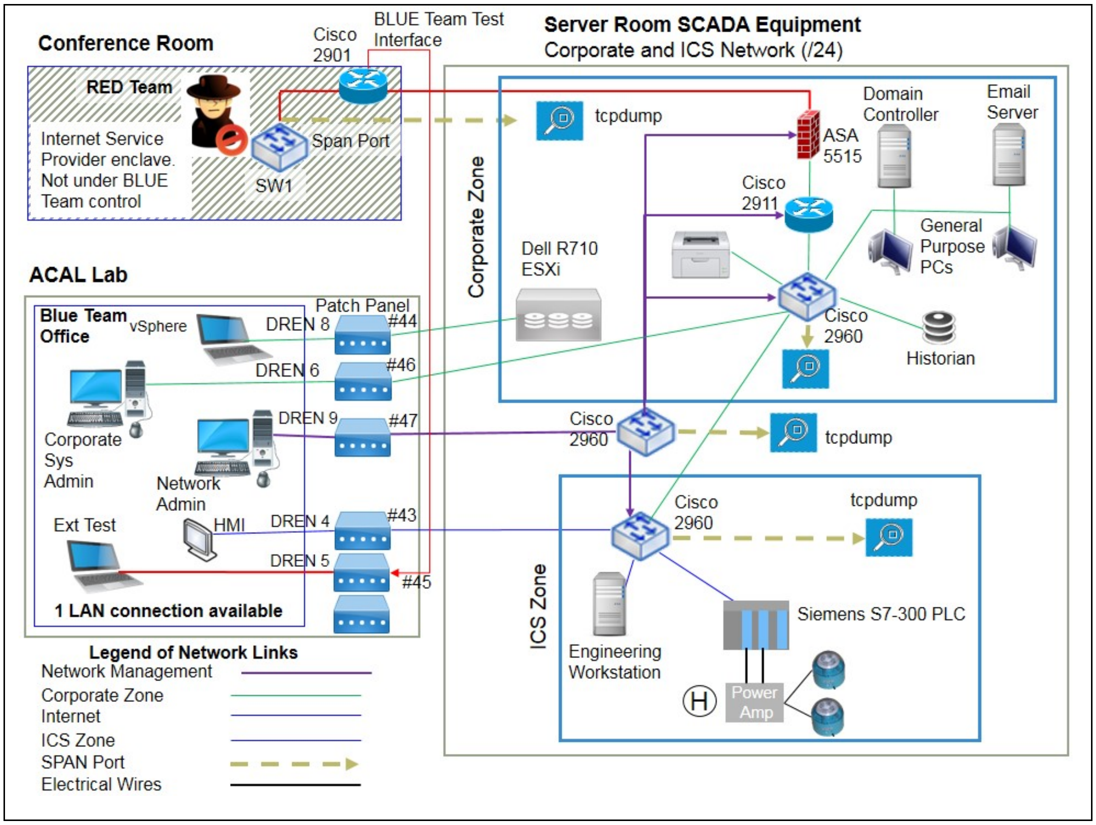

Fig. B-1 Initial corporate and ICS topology[*]

[*] SW1 and R1 are part of the Internet Service Provider enclave and are not described in this report because the BLUE team will be unable to configure or monitor them.

2. **Security Posture**. The operating systems and network elements are installed with minimal security in their default configuration.

3. **Locations.** The network elements, programmable logic controller (PLC) and virtual machines (VMs) will be in the server room. The BLUE team will have an office in the Army Cyber-research and Analytics Laboratory (ACAL) with 6 local area network (LAN) drops connecting to 3 switches in the server room.

4. **Hardware and Software List**. In Table B-1, we list the pertinent information about each server, personal computer (PC), PLC, and the network printer.

Table B-1 Corporate and ICS hosts and devices

Diagram Label	Zone	Function	Platform	Operating System	Default Applications/ Services
A	Corporate	Domain Controller	Virtual Machine (VM) hosted by Dell R710 with ESXi 5.5	Windows Server 2012 R2	Active Directory Domain Services (AD DS), Domain Name System (DNS) server, Dynamic Host Configuration Protocol (DHCP) server, Internet Information Services (IIS) 8 web server, Print Server, Remote Desktop
B	Corporate	Email Server	VM hosted by Dell R710 with ESXi 5.5	Windows Server 2012 R2	Microsoft (MS) Exchange 2010, IIS 8 web server, Remote Desktop
C, D	Corporate	General Purpose Corporate PC-1, Corporate PC-2	VM hosted by Dell R710 with ESXi 5.5	Windows 7 Enterprise Service Pack (SP) 1	MS Office 2013 with Outlook 2013, EMET 5.1, McAfee Antivirus Enterprise 8.8, Java 1.8.0_45, Adobe Reader XI, Adobe Flash Player 17, Adobe Shockwave Player 12.1, Remote Desktop
E	Corporate	Data Historian	VM hosted by Dell R710 with ESXi 5.5	Windows 7 Enterprise SP 1	Mango Automation 2.4.2, Java 1.7.0_75, Remote Desktop

Table B-1 Corporate and ICS hosts and devices (continued)

F	ICS	Engineering Workstation	VM hosted by Dell R710 with ESXi 5.5	Windows XP SP3	Siemens STEP 5.5 SP4 (to program PLC), Remote Desktop
G	ICS	PLC	Siemens CPU315-2 PN/DP	Firmware 3.1	Modbus TCP server to communicate with HMI
H	ICS	Power Amplifier	Converts power from the PLC analog output module to a high enough voltage and current to power the centrifuges		
I	ICS	Centrifuges (2)	Small centrifuges which operate on low voltages		
J	BLUE team Office	Corporate Network Printer	HP LaserJet M402dn	Firmware date code 20150731	HP Web Services
K	BLUE team Office	Windows Sys Admin PC	Dell Optiplex 780 running VirtualBox	Windows 7 Enterprise SP 1 hosted by VirtualBox	MS Office 2013 with Outlook 2013, EMET 5.1, McAfee Antivirus Enterprise 8.8, Java 1.8.0_45, Adobe Reader XI, Adobe Flash Player 17, Adobe Shockwave Player 12.1, Remote Desktop client
L	BLUE team Office	Network Admin Configuration PC	Dell Optiplex 790 running VirtualBox	Fedora 15 hosted by VirtualBox	Standard Linux applications
M	BLUE team Office	Human Machine Interface (HMI)	Dell Optiplex 745 running VirtualBox	Windows XP SP3 hosted by VirtualBox	Mango Automation 2.4.2 (web-based HMI), Java 1.7.0_75

In Table B-2, we describe the default network devices.

Table B-2 Installed network elements

Diagram Label	Network Element	Model	Operating System	Number of Non-Management Ports	Number of Available Ports
FW1	Corporate Firewall	Cisco ASA 5515	ASA 9.1 (2)	6	4
R2	Customer Premise Router	Cisco 2911	IOS 15.3(3)M3	2	4
SW2	Corporate Access Switch	Catalyst 2960-S	IOS 12.2(55)	24	9
SW3	Network Management Access Switch	Catalyst 2960-S	IOS 12.2(55)	24	18
SW4	ICS Access Switch	Catalyst 2960-S	IOS 12.2(55)	24	18

5. **Virtualization**. Items with labels A through F are guest VMs hosted on a Dell R710 server (not shown) running the ESXi 5.5 hypervisor. The Dell R710 connects via a Small Computer System Interface (SCSI) cable to a Dell MD3220 storage array. The ESXi server management interface is only connected to a laptop managed by the white team. Each guest VM is assigned a network port connected to a switch.

6. **Access to Guest VMs**. The BLUE team can use Remote Desktop to access the guest VMs.

7. **Screen Recording**. Items K, L, and M are physical desktop computers running VirtualBox 5.1.8. We will use VirtualBox's screen recording feature to capture all BLUE team actions as they use the guest VM to perform operations

8. **Modifications to Network Topology**. The BLUE team leader may select to have additional network elements, servers, honeypots, or tools installed by the white team. The WHITE team will typically be able to make the requested configuration changes for the BLUE team for a to-be-determined (TBD) game fee. The BLUE team leader will have startup money (game-dollars) to purchase initial tools and/or mitigations.

9. **Additional Security**. In Table B-3 we list additional available tools, software, and mitigations. Any additional customized defense tool or mitigation not in Table 3 will need to be discussed as early as possible with the WHITE team beforehand so a game price can be assigned and setup complexity planned. Preliminary game prices for Table B-3 items will be available by 29 Nov (we will send the game prices as soon as they are completed).

Table B-3 Menu of available equipment, tools, upgrades, and mitigations

Item
Network Elements
Cisco 1841 router (2 available)
Cisco 2950 48 port switch
Cisco ASA 5505 firewall
Cisco ASA 5515 firewall
Cisco ASA 5520 firewall
Software Installs
Wireshark
Cacti
Nagios
Snort
Sucriata
Bro
Snorby
Sguil
Squert
ELSA
Network Miner
Replace/upgrade operating system (e.g., Install Win 7, Fedora, Ubuntu, Windows Server, etc)
Install new VM or Windows PC (we have 1 extra PC and may receive a few more)
Network Services
Layer 1 (Physical)
Reconfigure physical cabling or VM network
Layer 2 (Data Link)
Use port security, i.e., sticky MAC
VLAN separation
MAC address filtering
Dynamic ARP inspection
IP source guard security
Encrypted passwords on network devices (type 5 or 7)
Layer 3 (Network)
HTTPS web authentication
VPN
Replace telnet with SSH for access to network elements
SNMPv3
Centralized Logging Server
Cisco Express Forwarding
Any firewall rule, ACLs to permit or allow
Deep packet inspection (ICMP, FTP, UDP, TCP, etc)
Intrusion Detection/ Prevention
Honeypot with a PLC (1 PLC is available to be in a honeypot)
Other Services
Lock server room
Configuration change to Windows OS or network printer (e.g., add/remove software, disable a service)
Lariat (this simulates Internet traffic)

Appendix C. Detailed List of Gameplay Events

We list a chronological record of all Terra wargame events in Table C-1. As noted in Section 3.4, this information was assembled using notes from the BLUE and RED team points of contact (POCs) (who were also acting as scribes), from WHITE team interviews with players, and from WHITE team notes. See Section 3 for additional details.

Table C-1 Summary of Terra wargame events

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
10/15 to 28		{R0}	All	Email	WHITE team sent out invitations for potential wargame volunteers. Information about potential insider is included in the notices.
Fri, 10/28	1000 and 1300	{B0}	All	Telephone	Teleconferences for all volunteers to ask questions about the wargame.
Sun, 10/30	1636	{R0}	WHITE	Email	WHITE team selected preliminary BLUE and RED team members.
10/31 to 11/9		{B0}	All	Email	WHITE team contacted prospective RED and BLUE team captains to ask if they want to lead their teams.
Fri, 11/4	1000 and 1300	{B0}	All	Telephone	Teleconference for all volunteers to ask questions. WHITE team captured their questions.
Sat-Sun, 11/5&6		{B0}	BLUE and RED	Email	WHITE team prepared written responses to the questions asked at the 4 Nov teleconferences.
Mon, 11/7	0824	{B0}	All	Email	WHITE team sent to all volunteers the questions asked on 4 Nov with their answers
Thu, 11/10	1017	{B0}	BLUE	Email	List and contact information of initial BLUE team members given to BLUE team captain.
Mon, 11/14	1420	{R0}	RED	Email	Preliminary gameplay information provided to RED team captain, including team members and information about the insider.
Mon, 11/14	1250	{B0}	WHITE/ BLUE	Email	Read-ahead document describing wargame technical and physical configuration is distributed to BLUE team.
Wed, 11/16	0900	{B0}	WHITE	Meeting	WHITE team conducted tabletop exercise of expected BLUE team strategy, estimated costs for labor and equipment mitigations, and assigned team budgets.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Thu, 11/17	1111	{B0}	BLUE	Email	BLUE team captain is emailed mitigations identified by the WHITE team, a menu of available mitigations with cost estimates, and the BLUE team budget. Suspense date is 1 Dec for the BLUE team captain to direct the WHITE team to implement mitigations.
Fri, 11/18	1000 and 1300	{B0}	BLUE	Telephone	BLUE team teleconference to ask questions and strategize.
Fri, 11/18	1739	{B0}	BLUE	Email	BLUE team captain agreed with the mitigations identified by the WHITE team and requested the WHITE team to implement all of them. He also included the software tools he would like to use and his strategy.
Mon, 11/21	0900	{B0}	WHITE	Meeting	WHITE team met to discuss game rules.
Mon, 11/21	0925	{R0}	RED	Telephone	RED team / RTFS sync-up conversation.
Thu, 12/1	0800	{R0}	RED	Telephone	RED team / RTFS / insider sync-up conversation.
Fri, 12/2	1000	{B0}	BLUE	Telephone	BLUE team teleconference to ask questions and strategize. Some members planned a follow-up meeting in person.
Fri, 12/2	1615	{B0}	BLUE	Email	BLUE team captain requested the WHITE team to install Sysmon on all hosts. The WHITE team did not install Sysmon because the request was sent after the 1 Dec suspense date.
Fri, 12/2	1725	{B0}	BLUE	Email	{B4} sent a list of tools he would like to use in the wargame.
Mon, 12/5	1400	{B0}	WHITE	Meeting	WHITE team met to review game rules.
Mon, 12/5	1545	{B0}	BLUE	Email	{B5} sent the names of the software he would like to use in the wargame.
Tue, 12/6	0811	{R0}	RED	Email	Two additional members provided to RED team ({R3} and {R8}), due to attrition.
Tue, 12/6	0819	{B0}	BLUE	Email	Two additional members provided to BLUE team ({B3} and {B6}), due to attrition.
Fri, 12/9	0830	{R0}	RED	Telephone	RED team / RTFS / insider sync-up conversation. {R1} takes over as RTFS.

Table C-1 Summary of Terra wargame events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Fri, 12/9	1000	{B0}	BLUE	Telephone	BLUE team teleconference to ask questions and strategize. Some members planned a follow-up meeting in person.
Fri, 12/9	1248	{B0}	RED	Email	RED team captain sent a list of software and tools to use in the wargame.
Fri, 12/9	1438	{R1}	RED	Email	A RED team member sent a request to use Python scripts that he developed.
Fri, 12/9	1518	{B0}	BLUE	Email	{B7} sent a list of tools he would like to use.
Sun, 12/11	1200	{R0} and {B0}	WHITE	Telephone	WHITE team finalize the in-brief slides and the cost of the BLUE and RED team tools.
Events During Gameplay Week 12-16 Dec 2016					
Mon, 12/12	During in-brief	{B0}	RED	Meeting	RED team asked if there will be traffic generators in the wargame? WHITE team replied no.
Mon, 12/12	After in-brief	{B0}	All	Meeting	After the in-brief, both teams were given a tour of the Conference Room and ACAL.
Mon, 12/12	1030 (approx)	{B0}	RED	Conference Room	The RED team inquired if they can write scripts for their cyberattacks. WHITE team replied they can but need to document the script writing in their activity logs.
Mon, 12/12	1030 (approx)	{B0}	RED	Conference Room	The RED team said they need Internet access to conduct research and download exploits. The WHITE team replied stating a PC is in their work area with Internet access. An ARL team member can log into the PC if a RED team member needs to access the Internet.
Mon, 12/12	1100 (approx)	{B0}	BLUE	Server Room/ New Location	The BLUE team captain purchased a Cisco ASA firewall from the WHITE team to place between the corporate and ICS networks.
Mon, 12/12	1130 (approx)	{B0}	BLUE	Server Room/ New Location	BLUE team was shown the server room with the PLC. The BLUE team tried to camouflage the PLC by placing cardboard boxes over the PLC and its rack shelf.
Mon, 12/12	1150 – 1300 (approx)	{B0}	BLUE	ACAL/ New Location	WHITE team directed BLUE team to relocate from the ACAL to the new location because more space is available.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Mon, 12/12	1300-1800 (approx)	{B0}	BLUE	Server Room/ New Location	BLUE team prepared 100 ft Ethernet cables to run from the server room to the BLUE team's PCs.
Mon, 12/12	1300-1800 (approx)	{B0}	BLUE	Server Room/ New Location	BLUE team installed the new firewall between the corporate switch and ICS switch.
Mon, 12/12	1300-1800 (approx)	{B0}	BLUE	Server Room/ New Location	BLUE team changed passwords and disabled unused user accounts.
Mon, 12/12	1300-1800 (approx)	{B0}	WHITE	Server Room	BLUE team upgraded the OS on the HMI and Engineering Workstation from Windows XP to Windows 7 VMs.
Mon, 12/12	1300-1800 (approx)	{B0}	WHITE	Server Room	BLUE team installed latest version of Java on the HMI and Engineering Workstation.
Mon, 12/12	1300-1800 (approx)	{B0}	BLUE	Server Room/ New Location	BLUE team disabled unused services on PCs.
Mon, 12/12	1300-1800 (approx)	{B0}	BLUE	Server Room/ New Location	The BLUE team had a choice to use Windows Remote Desktop Service or vSphere clients to access and configure the Windows VMs. The BLUE team chose to use vSphere clients because they would be using an out-of-band network to manage the Windows VMs.
Tue, 12/13	0800-2000	{B0}	BLUE	Server Room/ New Location	BLUE team relocated the Blue Corp public and e-commerce web servers and the email server into a new DMZ
Tue, 12/13	0800-2000	{B0}	BLUE	Server Room/ New Location	BLUE team assigned a new subnet for the PLC, HMI, and Historian and configured them with new IP addresses.
Tue, 12/13	0800-2000	{B0}	BLUE	Server Room/ New Location	BLUE team connected Snort and Bro to the SPAN ports of the Corporate and ICS switches. Bro was configured to send its logs to Splunk.
Tue, 12/13	0800-2000	{B0}	BLUE	Server Room/ New Location	BLUE team began installing Sysmon on all Windows hosts with the Splunk forwarder.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Tue, 12/13	0800-2000	{B0}	BLUE	Server Room/ New Location	BLUE team upgraded the Mango software to the latest version on the HMI and Historian. The new version did not work so the software was rolled back to the starting release.
Tue, 12/13	1100	{B0}	RED	Isolated Conference Room	WHITE team set up a bench power supply and spare S7-300 PLC for three RED team members to experiment with. The RED team analyzed the PLC for about 3 hours.
Tue, 12/13	1100	{B0}	RED	Isolated Conference Room	The RED team members requested Internet access for each of their laptops.
Wed, 12/14	0730 (approx)	{B0}	RED	Conference Room	WHITE team installed the RED team switch into the Conference Room and verified the public-facing web and email services of Blue Corporation were functioning.
Wed, 12/14	0830	{B0}	BLUE	Server Room	BLUE team captain resumed efforts to upgrade the Mango software to the latest version. The new version of Mango did not work properly. The BLUE team captain decided to roll back to the previous version of Mango.
Wed, 12/14	0830	{B0}	BLUE	Server Room/ New Location	BLUE team wrote firewall rules and installed Sysmon and the Splunk forwarder on the Windows hosts.
Wed, 12/14	0900	{B0}	All		Wargame activities start.
Wed, 12/14	0900	{B0}	WHITE/ RED	Conference Room	WHITE team provided 2 laptops with Kali VM to RED Team.
Wed, 12/14	0900	{B0}	WHITE/ RED	Conference Room	RED team requested ideas for software to capture laptop video to win cash.
Wed, 12/14	0915	{B0}	WHITE/ RED	Conference Room	RED team said they could not discover the Blue Corporation public facing services. The RED team requested the WHITE team provide the public IP addresses. The WHITE team provided the IP addresses and the RED team verified they could access the services.
Wed, 12/14	0930 (approx)	{B0}	All	New Location / Conference Room	WHITE team gave the RED and BLUE team captains their bank account ledgers and cash in game-dollars.
Wed, 12/14	0930 (approx)	{B0}	WHITE/ BLUE	New Location	WHITE team verified CTF goal files were present.

Approved for public release; distribution unlimited.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Wed, 12/14	0930 (approx)	{B0}	BLUE	New Location	BLUE team wrote scripts to detect if RED team attempted to access the CTF goal files.
Wed, 12/14	0930 (approx)	{B0}	WHITE/ BLUE	New Location	WHITE team reviewed rules with BLUE team for them to receive awards.
Wed, 12/14	0930 (approx)	{B0}	BLUE	New Location	BLUE team investigated why MS Outlook clients were unable to connect to MS Exchange server (now hosted in a DMZ).
Wed, 12/14	0945 (approx)	{B0}	WHITE/ RED	Conference Room	RED team requested Internet access for each player's laptop.
Wed, 12/14	0945 (approx)	{B0}	WHITE/ RED	Conference Room	{R4} claimed the CTF goal of capturing a Blue Corporation network diagram. The diagram that was shown was a working diagram used by the BLUE team to prepare. This diagram did not have a proof token number which all CTF goals had. As a result, WHITE team denied the claim.
Wed, 12/14	0945 (approx)	{B0}	WHITE/ BLUE	New Location	BLUE team awarded cash after showing proof that some critical services were up.
Wed, 12/14	1000	{B0}	BLUE	New Location	BLUE team worked to configure firewall rules to permit MS Outlook on the corporate PCs to connect to the MS Exchange server in the DMZ.
Wed, 12/14	1030 (approx)	{R1}	RED	Conference Room	{R1} obtained wireless Internet access for each RED team member via site wireless network for guest researchers.
Wed, 12/14	1030 (approx)	{R1}	RED	Conference Room	{R1} provided a CD of video screen recording software to the RED team.
Wed, 12/14	1045 (approx)	{R1}	RED	Conference Room	RED team captain and RTFS offered the option of using the insider. RED team members refused this offer.
Wed, 12/14	1133	{R1}	RED	Conference Room	{R6} captured Blue Corporation user names by accessing email and web servers.
Wed, 12/14	1133	{R1}	RED	Conference Room	{R6} completed a "SYN" scan.
Wed, 12/14	1138	{R1}	RED	Conference Room	RED team acquired first and last names of Blue Corporation user accounts.
Wed, 12/14	1150	{B1}	BLUE	New Location	BLUE team configured firewall rules.
Wed, 12/14	1150	{B1}	BLUE	New Location	BLUE team set up Snort.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Wed, 12/14	1150	{B1}	BLUE	New Location	BLUE team configured Splunk to monitor the networks.
Wed, 12/14	1150	{B1}	BLUE	New Location	BLUE team updated Splunk filters.
Wed, 12/14	1150	{B1}	BLUE	New Location	BLUE team set up a process to validate the HMI is operational every 50-70 min.
Wed, 12/14	1150	{B1}	BLUE	New Location	BLUE team wrote scripts to detect if a process (i.e., from RED team) attempted to access CTF goal files.
Wed, 12/14	1155	{B0}	WHITE/ BLUE	New Location	BLUE team awarded cash after showing proof that some critical services are up.
Wed, 12/14	1155	{B0}	BLUE	New Location	BLUE team continued configuring and testing firewall rules to permit MS Outlook on the corporate PCs to connect to the MS Exchange server in the DMZ.
Wed, 12/14	1155	{B1}	BLUE	New Location	BLUE team added a fake password file in web server directory to deceive RED team.
Wed, 12/14	1155	{B1}	BLUE	New Location	BLUE team changed file permissions on RED team CTF files to make it more difficult for the RED team to achieve the CTF goals.
Wed, 12/14	1155	{B1}	BLUE	New Location	BLUE team disabled default Windows accounts.
Wed, 12/14	1155	{B1}	BLUE	New Location	BLUE team changed default passwords.
Wed, 12/14	1235	{B0}	WHITE/ RED	Conference Room	{R5} reported the Internet Service Provider (ISP) switch configuration had changed. In particular, ports were being closed.
Wed, 12/14	1235	{B0}	WHITE	New Location	WHITE team asked BLUE team if they were configuring the ISP switch?
Wed, 12/14	1235	{B0}	BLUE	New Location	BLUE team reported they were configuring access control lists (ACLs) on the ISP router to prevent the RED team entering the Blue Corp network management switch.
Wed, 12/14	1235	{B0}	WHITE	New Location	WHITE team realized that they did not disconnect the ISP router from the Blue Corporation network before the wargame started.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Wed, 12/14	1250	{B1}	BLUE	New Location	BLUE team configured the PLC to have password protection.
Wed, 12/14	1253	{R1}	RED	Conferenc e Room	RED team completed port scans.
Wed, 12/14	1255-1320	{B0}	BLUE	New Location	The BLUE team restored the ISP router to the configuration at the start of the wargame.
Wed, 12/14	1255-1320	{B0}	WHITE/ BLUE	Server Room	BLUE team disconnected the ISP router from the BLUE team network management switch.
Wed, 12/14	1255-1320	{B0}	RED	Conferenc e Room	{R5} verified the RED team could reach the public facing web services and email server.
Wed, 12/14	1259	{B1}	BLUE	New Location	BLUE team configured Splunk to monitor network activity.
Wed, 12/14	1259	{B1}	BLUE	New Location	The BLUE team viewed RED team packets targeting the public web server using the tcpdump tool.
Wed, 12/14	1300 (approx)	{R1}	RED	Conferenc e Room	{R5} discovered ports 22 and 23 from the Cisco network elements were open.
Wed, 12/14	1300 (approx)	{R1}	RED	Conferenc e Room	{R3} used Telnet to access the Cisco network elements and identified IP addresses present on the network.
Wed, 12/14	1306	{R1}	RED	Conferenc e Room	RED team identified some of the target network topology using Telnet.
Wed, 12/14	1309	{R1}	RED	Conferenc e Room	{R3} identified IP ranges available for pinging.
Wed, 12/14	1309	{R1}	RED	Conferenc e Room	{R5} discovered a router connection.
Wed, 12/14	1315 (approx)	{R1}	RED	Conferenc e Room	RED team captain and RTFS again offer the possibility of leveraging an insider. RED team members decline this idea.
Wed, 12/14	1333-1337	{R1}	RED	Conferenc e Room	RED team captured the ISP switch address resolution protocol (ARP) table.
Wed, 12/14	1333-1337	{R1}	RED	Conferenc e Room	{R8} identified the IP and MAC addresses of 3 switches.
Wed, 12/14	1400	{B0}	RED	Hallway by Research Lab	The RED team is making little progress so the RED team captain departed.
Wed, 12/14	1400	{B1}	BLUE	New Location	After installing Sysmon on the HMI, the BLUE team discovered the Mango user accounts were (somehow) changed. The BLUE team restored the HMI to a snapshot prior to the installation of Sysmon.

Table C-1 Summary of Terra Wargame Events (continued)

Date	Time	Information Source	Team(s) Involved	Media/ Location	Description of Event(s)
Wed, 12/14	1400	{B1}	BLUE	New Location	BLUE team updated the HMI user accounts with strong passwords.
Wed, 12/14	1419	{B1}	BLUE	New Location	BLUE team configured the corporate firewall to only log packets which traverse the firewall.
Wed, 12/14	1419	{B1}	BLUE	New Location	BLUE team fixed a problem in sending the firewall logs to Splunk.
Wed, 12/14	1434	{R1}	RED	Conference Room	{R8} obtained access to a Blue Corporation virtual local area network (VLAN).
Wed, 12/14	1440 (approx)	{B0}	RED	Conference Room	{R3} and {R7} departed because the RED team was making little progress.
Wed, 12/14	1445	{B0}	All	RED and BLUE Team areas	WHITE team conducted a morale check.
Wed, 12/14	1455 (approx)	{B0}	WHITE	Meeting	WHITE team met and suggested offering a rule change to the RED and BLUE teams. The idea was to break the wargame into 2 rounds.
Wed, 12/14	1530 (approx)	{B0}	RED	Conference Room	{R5} departed. Only {R6} and {R8} remained on RED team.
Wed, 12/14	1545 (approx)	{B0}	All	RED and BLUE Team areas	WHITE team offered the rule change to separate the wargame into 2 rounds. Remaining RED team members ({R6} and {R8}) as well as BLUE team captain agreed to end Round 1 and start Round 2.
Wed, 12/14	1551	{B0}	All	Email	WHITE team sent an email to all participants with the rule change to have 2 rounds in the wargame.
Wed, 12/14	1625	{B0}	All	Email	After discussing the scope of wargame Round 2 with the RED and BLUE teams, the WHITE team decided to end the wargame. WHITE team sent an email to all participants informing them that the wargame had completed.
Wed, 12/14	1625-1800	{B0}	All	Server Room	RED and BLUE team members investigated the wargame network for their own learning.
Wed, 12/14	1800	{B0}	All	New Location	Last game participant departed.
Thu, 12/15	0900-1600	{R0} and {B0}	WHITE	Meetings	WHITE team prepares out-brief slides.
Fri, 12/16	0900-1030	{R0} and {B0}	All	CISD Conference Room and Telephone	Out-brief presentation and lessons-learned discussion.

List of Symbols, Abbreviations, and Acronyms

ACAL	Army Cyber-research and Analytics Laboratory
ACL	Access Control List
AD DS	Active Directory Domain Services
ARP	Address Resolution Protocol
ARL	US Army Research Laboratory
ASA	Adaptive Security Appliance
CAC	common access card
CEO	chief executive officer
CISD	Computational and Information Sciences Directorate
CIV	civilian
CTF	capture the flag
CPS	Cyber-Physical System
CTR	contractor
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarized zone
DNS	Domain Name System
DoD	Department of Defense
FTP	File Transfer Protocol
$GD	game-dollars
HMI	human–machine interface
HP	Hewlett Packard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services
IP	Internet Protocol
ICS	industrial control system

ICMP	Internet Control Message Protocol
IOS	Internetwork Operating System
ISP	Internet Service Provider
LAN	local area network
MAC	Media Access Control
MS	Microsoft
NSD	Network Science Division
OS	operating system
PC	personal computer
PED	personal electronic device
PLC	programmable logic controller
POC	point of contact
RTFS	Red Team Funding Source
SCADA	supervisory control and data acquisition
SCSI	Small Computer System Interface
SMTP	Simple Mail Transfer Protocol
SNMPv3	Simple Network Management Protocol version 3
SPAN	switched port analyzer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	universal serial bus
VLAN	virtual local area network
VM	virtual machine

1 DEFENSE TECH INFO CTR
(PDF) DTIC OCA

2 US ARMY RSRCH LAB
(PDF) RDRL IMAL HRA MAIL & RECORDS MGMT
RDRL CIO L TECHL LIB

1 GOVT PRNTG OFC
(PDF) A MALHOTRA

13 US ARMY RSRCH LAB
(PDF) RDRL HRB D N BUCHLER
RDRL CIN A KOTT
RDRL CIN T
A SWAMI
M REINSFELDER
RDRL CIN D
J CLARKE
E COLBERT
N LESLIE
R LEWIS
RDRL CIN S
C ARNOLD
J PATRICK
R RITCHEY
J SCHAUM
D SULLIVAN

INTENTIONALLY LEFT BLANK.