REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
10-01-2023	Final Report	10-Mar-2014 - 9-Mar-2015

4. TITLE AND SUBTITLE
Final Report: Cyber Warfare: Building the Scientific Foundation

5a. CONTRACT NUMBER
W911NF-14-1-0116

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Sushil Jajodia

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
George Mason University
4400 University Drive, MSN 4C6

Fairfax, VA 22030 -4422

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
65000-NC-CF.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS
Adaptive cyber defense, moving target defense, control theory, game theory

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Sushil Jajodia
UU	UU	UU	UU		19b. TELEPHONE NUMBER 703-993-1653

RPPR Final Report
as of 13-Jan-2023

Agency Code: 21XD

Proposal Number: 65000NCCF **Agreement Number: W911NF-14-1-0116**
INVESTIGATOR(S):

Name: Sushil Jajodia
Email: jajodia@gmu.edu
Phone Number: 7039931653
Principal: Y

Organization: **George Mason University**
Address: 4400 University Drive, MSN 4C6, Fairfax, VA 220304422
Country: USA
DUNS Number: 077817450 EIN: 540836354

Report Date: 09-Jun-2015 Date Received: 10-Jan-2023
Final Report for Period Beginning 10-Mar-2014 and Ending 09-Mar-2015
Title: Cyber Warfare: Building the Scientific Foundation
Begin Performance Period: 10-Mar-2014 **End Performance Period:** 09-Mar-2016
Report Term: 0-Other

Submitted By: Sushil Jajodia Email: jajodia@gmu.edu
Phone: (703) 993-1653

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 0 **STEM Participants:**

Major Goals: We organized two invitational workshops at George Mason University on Cyber Warfare. The goals of the workshops were to establish the state of the art in this area and to set the course for future research. A multidisciplinary group of leading researchers from cyber security and cognitive system met to elaborate on the fundamental challenges facing the research community and identify promising solutions paths.

Accomplishments: The results of the workshop were captured in the following edited books:

1. Sushil Jajodia, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, eds., Cyber Deception: Building the Scientific Foundation, Springer, ISBN 978-3-319-32697-9, Springer, Switzerland, 2016, 314 pages. DOI: 10.1007/978-3-319-32699-3

2. Sushil Jajodia, Paulo Shakarian, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, eds., Cyber Warfare: Building the Scientific Foundation, ISBN 978-3-319-1408-4, Springer, Berlin, 2015, 340 pages.

Table of contents of both volumes and workshop agendas are given in the attached report.

Training Opportunities: Nothing to Report

Results Dissemination: Please see the attached report.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Please see the attached report.

PARTICIPANTS:

Participant Type: PD/PI
Participant: Sushil Jajodia
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:

RPPR Final Report
as of 13-Jan-2023

National Academy Member: N

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Sushil Jajodia
Signature Date: 1/10/23 12:51PM

Final Report
Cyber Warfare: Building the Scientific Foundation
Research Agreement No. W911NF-14-1-0116

Submitted by

Sushil Jajodia
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
jajodia@gmu.edu

We organized two invitational workshops at George Mason University on Cyber Warfare. The goals of the workshops were to establish the state of the art in this area and to set the course for future research. A multidisciplinary group of leading researchers from cyber security and cognitive system met to elaborate on the fundamental challenges facing the research community and identify promising solutions paths.

The results of the workshop were captured in the following edited books:

1. Sushil Jajodia, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, eds., Cyber Deception: Building the Scientific Foundation, Springer, ISBN 978-3-319-32697-9, Springer, Switzerland, 2016, 314 pages. DOI: 10.1007/978-3-319-32699-3

2. Sushil Jajodia, Paulo Shakarian, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, eds., Cyber Warfare: Building the Scientific Foundation, ISBN 978-3-319-1408-4, Springer, Berlin, 2015, 340 pages.

Table of contents of both volumes and workshop agendas are given below.

Advances in Information Security 56

Sushil Jajodia
Paulo Shakarian
V.S. Subrahmanian
Vipin Swarup
Cliff Wang *Editors*

Cyber Warfare

Building the Scientific Foundation

Springer

Contents

1 Cyber War Games: Strategic Jostling Among Traditional Adversaries 1
Sanjay Goel and Yuan Hong

2 Alternatives to Cyber Warfare: Deterrence and Assurance 15
Robert J. Elder, Alexander H. Levis and Bahram Yousefi

3 Identifying and Exploiting the Cyber High Ground for Botnets 37
Patrick Sweeney and George Cybenko

4 Attribution, Temptation, and Expectation: A Formal Framework for Defense-by-Deception in Cyberwarfare 57
Ehab Al-Shaer and Mohammad Ashiqur Rahman

5 Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security 81
Christopher Kiekintveld, Viliam Lisý and Radek Píbil

6 Cyber Counterdeception: How to Detect Denial & Deception (D&D) 103
Kristin E. Heckman and Frank J. Stech

7 Automated Adversary Profiling 141
Samuel N. Hamilton

8 Cyber Attribution: An Argumentation-Based Approach 151
Paulo Shakarian, Gerardo I. Simari, Geoffrey Moores and Simon Parsons

9 The Human Factor in Cybersecurity: Robust & Intelligent Defense 173
Julie L. Marble, W. F. Lawless, Ranjeev Mittu, Joseph Coyne, Myriam Abramson and Ciara Sibley

10 CyberWar Game: A Paradigm for Understanding New Challenges of Cyber War 207
Noam Ben-Asher and Cleotilde Gonzalez

11 Active Discovery of Hidden Profiles in Social Networks Using Malware 221
Rami Puzis and Yuval Elovici

12 A Survey of Community Detection Algorithms Based On Analysis-Intent 237
Napoleon C. Paxton, Stephen Russell, Ira S. Moskowitz and Paul Hyden

13 Understanding the Vulnerability Lifecycle for Risk Assessment and Defense Against Sophisticated Cyber Attacks 265
Tudor Dumitraş

14 Graph Mining for Cyber Security 287
B. Aditya Prakash

15 Programming Language Theoretic Security in the Real World: A Mirage or the Future? 307
Andrew Ruef and Chris Rohlf

Contributors

Myriam Abramson Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Ehab Al-Shaer University of North Carolina at Charlotte, Charlotte, USA

Noam Ben-Asher Department of Social and Decision Sciences, Dynamic Decision Making Laboratory, Carnegie Mellon University, Pittsburgh, PA, USA

Joseph Coyne Information Technology Division, Naval Research Laboratory, Washington, DC, USA

George Cybenko Thayer School of Engneering at Dartmouth College, Hanover, NH, USA

Tudor Dumitraş Electrical and Computer Engineering Department, University of Maryland, College Park, MD, USA

Robert J. Elder System Architectures Laboratory, George Mason University, Fairfax, VA, USA

Yuval Elovici Telekom Innovation Laboratories and Department of Information Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel

Sanjay Goel University at Albany, State University of New York, New York, USA

Cleotilde Gonzalez Department of Social and Decision Sciences, Dynamic Decision Making Laboratory, Carnegie Mellon University, Pittsburgh, PA, USA

Samuel N. Hamilton Siege Technologies, Manchester, USA

Kristin E. Heckman The MITRE Corporation, McLean, VA, USA

Yuan Hong University at Albany, State University of New York, New York, USA

Paul Hyden Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Christopher Kiekintveld Computer Science Department, University of Texas at El Paso, El Paso, USA

W. F. Lawless Paine College, GA, Augusta, USA

Alexander H. Levis System Architectures Laboratory, George Mason University, Fairfax, VA, USA

Viliam Lisý Agent Technology Center, Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Prague, Czech Republic

Julie L. Marble Advanced Physics Laboratory Senior Human Factors Scientist Asymetric Operations Sector, Johns Hopkins University, Laurel, MD, USA

Ranjeev Mittu Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Geoffrey Moores Department of Electrical Engineering and Computer Science, U.S. Military Academy, West Point, NY, USA

Ira S. Moskowitz Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Radek Píbil Agent Technology Center, Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Prague, Czech Republic

Simon Parsons Department of Computer Science, University of Liverpool, Liverpool, UK

Napoleon C. Paxton Information Technology Division, Naval Research Laboratory, Washington, DC, USA

B. Aditya Prakash Department of Computer Science, Virginia Tech., Blacksburg, VA, USA

Rami Puzis Telekom Innovation Laboratories and Department of Information Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel

Mohammad Ashiqur Rahman University of North Carolina at Charlotte, Charlotte, USA

Chris Rohlf Yahoo Inc., New York, USA

Andrew Ruef Trail of Bits, New York, USA

Stephen Russell Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Paulo Shakarian Arizona Sate University, Tempe, AZ, USA

Ciara Sibley Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Gerardo I. Simari Department of Computer Science and Engineering, Universidad Nacional del Sur, Bahìa Blanca, Argentina

Frank J. Stech The MITRE Corporation, McLean, VA, USA

Patrick Sweeney Thayer School of Engneering at Dartmouth College, Hanover, NH, USA

Bahram Yousefi System Architectures Laboratory, George Mason University, Fairfax, VA, USA

Sushil Jajodia · V.S. Subrahmanian
Vipin Swarup · Cliff Wang *Editors*

Cyber Deception

Building the Scientific Foundation

Springer

Contents

Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense 1
Frank J. Stech, Kristin E. Heckman, and Blake E. Strom

Cyber Security Deception 25
Mohammed H. Almeshekah and Eugene H. Spafford

Quantifying Covertness in Deceptive Cyber Operations 53
George Cybenko, Gabriel Stocco, and Patrick Sweeney

Design Considerations for Building Cyber Deception Systems 71
Greg Briskin, Dan Fayette, Nick Evancich, Vahid Rajabian-Schwart, Anthony Macera, and Jason Li

A Proactive and Deceptive Perspective for Role Detection and Concealment in Wireless Networks 99
Zhuo Lu, Cliff Wang, and Mingkui Wei

Effective Cyber Deception 117
A.J. Underbrink

Cyber-Deception and Attribution in Capture-the-Flag Exercises 151
Eric Nunes, Nimish Kulkarni, Paulo Shakarian, Andrew Ruef, and Jay Little

Deceiving Attackers by Creating a Virtual Attack Surface 169
Massimiliano Albanese, Ermanno Battista, and Sushil Jajodia

Embedded Honeypotting 203
Frederico Araujo and Kevin W. Hamlen

Agile Virtual Infrastructure for Cyber Deception Against Stealthy DDoS Attacks 235
Ehab Al-Shaer and Syed Fida Gillani

Exploring Malicious Hacker Forums 261
Jana Shakarian, Andrew T. Gunn, and Paulo Shakarian

Anonymity in an Electronic Society: A Survey 285
Mauro Conti, Fabio De Gaspari, and Luigi Vincenzo Mancini

Center for Secure Information Systems

George Mason University, MSN 5B5
4400 University Drive
Fairfax, VA 22030-4444
(703) 993-3767

Fax: (703) 993-4776
http://csis.gmu.edu/

ARO Invitational Workshop on Cyber Warfare
George Mason University
March 13-14, 2014

March 13, 2014

Guest Wireless Account:
Username: armyresearch
Password: Initi4tive

8:00-8:30 **Continental Breakfast**

8:30-10:00 **Sushil Jajodia, Cliff Wang**
Opening Remarks

Vipin Swarup
TBD

Yuval Elovici
Protecting National Infrastructures and Businesses from DDoS Attacks Launched via BotNets

10:00-10:30 **Break**

10:30-12:00 **Andrew Ruef, Chris Rohlf**
Programming language theoretic security in the real world: a mirage or the future?

Kristin Heckman, Frank J. Stech
Cyber Wargame Exercises: How to Incorporate Denial & Deception (D&D)

Sam Hamilton
Automated Cyber Adversary Profiling

12:00-1:00 **Lunch**

1:00-2:30 **Michael Ovelgonne**
Fatal Attraction? On the Relationship between Human Behavior and Susceptibility to Cyber Attacks

V. S. Subrahmanian
Deception, Deterrence, and Disclosure: Smart Ways to Protect Assets?

LtGen Robert J. Elder, USAF (ret), Alexander H. Levis
Alternatives to Cyber Warfare: Deterrence and Assurance

2:30-3:00 **Break**

3:00-5:00 **Coty Gonzalez**
CyberGame: A Paradigm for Understanding New Behavioral Challenges for Cyber War

Cliff Wang
Wrap Up

6:00 **Dinner at Boxwood, Mason Inn**

http://csis.gmu.edu/repository/aro-cyber-warfare-workshop/
Username: aro-cw
Password: Cyb3rW4r!

March 14, 2013

8:00-8:30	**Continental Breakfast**
8:30-10:00	**Aditya Prakash** Dynamical Processes on Networks
	George Cybenko The Roles of Game Theory in Cyberwarfare
	Chris Kiekinteveld Game-theoretic Foundations for the Strategic Use of Honeypots in Network Security
10:00-10:30	**Break**
10:30-12:00	**Raphael Marty** Visual Analytics
	Tudor Dumitras Security and (In)Security: A Big Data Approach
	Sanjay Goel Cyber Warfare: Confidence Building Measures
12:00-1:00	**Lunch**
1:00-2:30	**Ehab Al-Shaer** Cyber Polymorphism: Defense by Mystification in Cyber Warfare
	Paulo Shakarian, Geoff Moores Power Grid Defense Against Malicious Cascading Failure and An Argumentation-Based Framework to Address the Attribution Problem in Cyber-Warfare
	Myriam Abramson Attribution from Web browsing behavior
2:30-3:00	**Break**
3:00-5:00	**Edoardo Serra** Pareto-Optimal Adversarial Defense of Enterprise Systems
	Vipin Swarup Wrap UP

Wireless Account Information: Username: armyresearch, Password: Initi4tive

To use this account connect the device to the "Mason" SSID. The user should be taken to the UAC where "Guest Access" should be clicked on. If this page does not appear automatically, open a web browser and navigate to uacwireless.gmu.edu, and click "Guest Access" Once authenticated, the device can connect to the internet.

Center for Secure Information Systems

George Mason University, MSN 5B5
4400 University Drive
Fairfax, VA 22030-4444
(703) 993-3767

Fax: (703) 993-4776
http://csis.gmu.edu/

ARO Invitational Workshop on Cyber Deception
George Mason University
Research Hall, Room 163
July 28-29, 2015

Tuesday, July 28. 2015

8:00-8:30 **Continental Breakfast**

8:30-10:00 **Sushil Jajodia, Cliff Wang**
Opening Remarks

Kristin Heckman, Frank J. Stech
Conceptual Design of a Cyber D&D Defender System

Ari Juels
A Bodyguard of Lies: The Use of Honey Objects in Information Security

10:00-10:30 **Break**

10:30-12:00 **V. S. Subrahmanian**
TBD

George Cybenko
Logical Cyber Deception

12:00-1:00 **Lunch**

1:00-2:30 **Al Underbrink**
Effective Cyber Deception

Paul Syverson
The Evolution of Anonymous Communication Adversary Models

2:30-3:00 **Break**

3:00-5:00 **Eric Nunes**
Cyber-Deception and Attribution in Capture-the-Flag Exercises

William Lawless
Cyber-(in)Security

Cliff Wang
Wrap Up

Wednesday, July 29. 2015

8:00-8:30	**Continental Breakfast**
8:30-10:00	**Debarun Kar** SHARP: Modeling Adaptive Boundedly Rational Adversaries in Repeated Stackelberg Security Games
	Julie Marble TBD
10:00-10:30	**Break**
10:30-12:00	**Panel** Jason Li, Moderator
12:00-1:00	**Lunch**
1:00-2:30	**Ehab Al-Shaer** TBD
	Myriam Abramson Guess Who is Online? Deceptive Identities in Cyberspace
2:30-3:00	**Break**
3:00-5:00	**Haining Wang** Human or Bot? A Behavioral-based Classification Approach, Challenges and Limitations
	Massimiliano Albanese Deceiving Attackers through In-Depth Attack Surface Manipulation
	Vipin Swarup Wrap UP

Wireless Account Information:

Wireless Network: 'Mason', Username: arocyberdeception, Password: 65z3~t4HC

To use this account connect the device to the "Mason" SSID. The user should be taken to the UAC where "Guest Access" should be clicked on. If this page does not appear automatically, open a web browser and navigate to uacwireless.gmu.edu, and click "Guest Access". Once authenticated, the device can connect to the internet.