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

Cyber Deception

Building the Scientific Foundation

Springer

Cyber Deception

Sushil Jajodia • V.S. Subrahmanian
Vipin Swarup • Cliff Wang
Editors

Cyber Deception

Building the Scientific Foundation

Springer

Editors
Sushil Jajodia
Center for Secure Information Systems
George Mason University
Fairfax, VA, USA

V.S. Subrahmanian
Department of Computer Science
University of Maryland
College Park, MD, USA

Vipin Swarup
The MITRE Corporation
McLean, VA, USA

Cliff Wang
Computing & Information Science Division
Information Sciences Directorate
Triangle Park, NC, USA

ISBN 978-3-319-32697-9 ISBN 978-3-319-32699-3 (eBook)
DOI 10.1007/978-3-319-32699-3

Library of Congress Control Number: 2016941329

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

This volume is designed to take a step toward establishing scientific foundations for cyber deception. Here we present a collection of the latest basic research results toward establishing such a foundation from several top researchers around the world. This volume includes papers that rigorously analyze many important aspects of cyber deception including the incorporation of effective cyber denial and deception for cyber defense, cyber deception tools and techniques, identification and detection of attacker cyber deception, quantification of deceptive cyber operations, deception strategies in wireless networks, positioning of honeypots, human factors, anonymity, and the attribution problem. Further, we have made an effort to not only sample different aspects of cyber deception, but also highlight a wide variety of scientific techniques that can be used to study these problems.

It is our sincere hope that this volume inspires researchers to build upon the knowledge we present to further establish scientific foundations for cyber deception and ultimately bring about a more secure and reliable Internet.

Fairfax, VA, USA — Sushil Jajodia
College Park, MD, USA — V.S. Subrahmanian
McLean, VA, USA — Vipin Swarup
Triangle Park, NC, USA — Cliff Wang

Acknowledgments

We are extremely grateful to the numerous contributors to this book. In particular, it is a pleasure to acknowledge the authors for their contributions. Special thanks go to Susan Lagerstrom-Fife, senior publishing editor at Springer for her support of this project. We also wish to thank the Army Research Office for their financial support under the grant numbers W911NF-14-1-0116, W911NF-15-1-0576, and W911NF-13-1-0421.

Contents

Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense

Frank J. Stech, Kristin E. Heckman, and Blake E. Strom

Abstract This chapter outlines a concept for integrating cyber denial and deception (cyber-D&D) tools, tactics, techniques, and procedures (TTTPs) into an adversary modeling system to support active cyber defenses (ACD) for critical enterprise networks. We describe a vision for cyber-D&D and outline a general concept of operation for the use of D&D TTTPs in ACD. We define the key elements necessary for integrating cyber-D&D into an adversary modeling system. One such recently developed system, the Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™) Adversary Model is being enhanced by adding cyber-D&D TTTPs that defenders might use to detect and mitigate attacker tactics, techniques, and procedures (TTPs). We describe general D&D types and tactics, and relate these to a relatively new concept, the cyber-deception chain. We describe how defenders might build and tailor a cyber-deception chain to mitigate an attacker's actions within the cyber attack lifecycle. While we stress that this chapter describes a concept and not an operational system, we are currently engineering components of this concept for ACD and enabling defenders to apply such a system.

Traditional approaches to cyber defense increasingly have been found to be inadequate to defend critical cyber enterprises. Massive exploitations of enterprises,

The original version of this chapter was revised. An erratum to this chapter can be found at DOI 10.1007/978-3-319-32699-3_13

Authors: Frank J. Stech, Kristin E. Heckman, and Blake E. Strom, the MITRE Corporation (stech@mitre.org, kheckman@mitre.org, and bstrom@mitre.org). Some material in this chapter appeared in Kristin E. Heckman, Frank J. Stech, Ben S. Schmoker, Roshan K. Thomas (2015) "Denial and Deception in Cyber Defense," *Computer*, vol. 48, no. 4, pp. 36–44, Apr. 2015. http://doi.ieeecomputersociety.org/10.1109/MC.2015.104

F.J. Stech (✉) • K.E. Heckman • B.E. Strom
MITRE Corporation, Mclean, VA, USA
e-mail: stech@mitre.org; kheckman@mitre.org; bstrom@mitre.org

S. Jajodia et al. (eds.), *Cyber Deception*, DOI 10.1007/978-3-319-32699-3_1

commercial (e.g., Target[1]) and government (e.g., OMB[2]), demonstrate that the cyber defenses typically deployed over the last decade (e.g., boundary controllers and filters such as firewalls and guards, malware scanners, and intrusion detection and prevention technologies) can be and have been bypassed by sophisticated attackers, especially the advanced persistent threats (APTs[3]). Sophisticated adversaries, using software exploits, social engineering or other means of gaining access, infiltrate these defended enterprises, establish a persistent presence, install malware and backdoors, and exfiltrate vital data such as credit card records, intellectual property and personnel security information. We must assume, then, that an adversary will breach border defenses and establish footholds within the defender's network. We must also assume that a sophisticated adversary will learn from and attempt to evade technology-based defenses, so we need new ways to engage the adversary on the defender's turf, and to influence the adversary's moves to the defender's advantage. One such means of influence is deception, and we argue a key component in the new paradigm of active cyber defense[4] is cyber denial and deception (cyber-D&D).

[1]Jim Walter (2014) "Analyzing the Target Point-of-Sale Malware," McAfee Labs, Jan 16, 2014. https://blogs.mcafee.com/mcafee-labs/analyzing-the-target-point-of-sale-malware/ and Fahmida Y. Rashid (2014) "How Cybercriminals Attacked Target: Analysis," *Security Week*, January 20, 2014. http://www.securityweek.com/how-cybercriminals-attacked-target-analysis

[2]Jim Sciutto (2015) OPM government data breach impacted 21.5 million," *CNN*, July 10, 2015. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/ Jason Devaney (2015) "Report: Feds Hit by Record-High 70,000 Cyberattacks in 2014," *NewsMax*, 04 Mar 2015. http://www.newsmax.com/Newsfront/cyberattacks-Homeland-Security-Tom-Carper-OMB/2015/03/04/id/628279/

[3]Advanced persistent threats (APTs) have been defined as "a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack." https://en.wikipedia.org/wiki/Advanced_persistent_threat A useful simple introduction and overview is Symantec, "Advanced Persistent Threats: A Symantec Perspective—Preparing the Right Defense for the New Threat Landscape," no date. http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf A detailed description of an APT is Mandiant (2013) *APT1: Exposing One of China's Cyber Espionage Units,* www.mandiant.com, 18 February 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[4]The U.S. Department of Defense (DOD) defined *active cyber defense* (ACD) in 2011: "As malicious cyber activity continues to grow, DoD has employed active cyber defense to prevent intrusions and defeat adversary activities on DoD networks and systems. Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities . . . . using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks." Department of Defense (2011) *Strategy for Operating in Cyberspace*, July 2011, p. 7.

The goal of D&D is to influence the adversary to behave in a way that gives the defender (i.e., the deceiver) an advantage, creating a causal relationship between the psychological state created by the influence on the adversary and the adversary's behavior. Denial TTTPs[5] actively conceal facts and fictions and create perceptual ambiguity to prevent the adversary from accurately perceiving information and stimuli (Table 1, right column). Deception TTTPs (Table 1, middle column) reveal facts and fictions to provide misleading information and stimuli to the adversary to actively create and reinforce the adversary's perceptions, cognitions, and beliefs in the defender's deception cover story.

Both denial and deception methods affect the adversary's situational awareness systems (e.g., for orientation and observation) and operational systems (e.g., for decision and action), that is, D&D influences the adversary's "OODA loop."[6] D&D aims to either: (1) generate a mistaken certainty about what is and is not real, making the adversary erroneously confident and ready to act, or (2) create sufficient uncertainty about what is real such that the adversary wastes time and/or resources

Cyber researcher Dorothy Denning differentiated active and passive cyber defense: "*Active Cyber Defense* is direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets. *Passive Cyber Defense* is all measures, other than active cyber defense, taken to minimize the effectiveness of cyber threats against friendly forces and assets. Whereas active defenses are direct actions taken against specific threats, passive defenses focus more on making cyber assets more resilient to attack." Dorothy E. Denning (2014) "Framework and Principles for Active Cyber Defense," *Computers & Security*, 40 (2014) 108–113. http://www.sciencedirect.com/science/article/pii/S0167404813001661/pdfft?md5=68fecd71b93cc108c015cac1ddb0d430&pid=1-s2.0-S0167404813001661-main.pdf

In both the DOD's and Denning's definitions, actions are defensive. Thus ACD is NOT the same as hacking back, offensive cyber operations, or preemption. However, ACD options are active and can involve actions outside of one's own network or enterprise, for example, collecting information on attackers and sharing the information with other defenders.

[5]"Tactics, techniques, and procedures (TTPs)" is a common military expression and acronym for a standardized method or process to accomplish a function or task. We added 'tools' because cyber adversaries use a variety of different tools in their tactics, techniques, and procedures. On the analysis of TTPs, see Richard Topolski, Bruce C. Leibrecht, Timothy Porter, Chris Green, and R. Bruce Haverty, Brian T. Crabb (2010) *Soldiers' Toolbox for Developing Tactics, Techniques, and Procedures (TTP)*, U.S. Army Research Institute for the Behavioral and Social Sciences Research Report 1919, February 2010.http://www.dtic.mil/dtic/tr/fulltext/u2/a517635.pdf

[6]Jeffrey Rule quotes its creator, John R. Boyd, describing the OODA loop: "orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window. ...the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection." Jeffrey N. Rule (2013) "A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought," Carlisle PA: U.S. Army War College. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA590672 Rule and other exponents of the OODA loop concept see the utility of D&D to isolate the adversary inside their own OODA loop and thus separate the adversary from reality. Osinga sees Boyd's OODA theory as affirming the use of deception against the adversary's OODA loop: "Employ a variety of measures that interweave menace, uncertainty and mistrust with tangles of ambiguity, deception and novelty as the basis to sever an adversary's moral ties and disorient or twist his mental images and thus mask, distort and magnify our presence and activities." Frans P. B. Osinga (2007) *Science, Strategy and War: The strategic theory of John Boyd*, Oxford UK: Routledge, p. 173.

Table 1 D&D methods matrix

Deception objects	Deception: Mislead (M)-type methods	Denial: Ambiguity (A)-type methods
	Revealing	Concealing
Facts	Reveal facts: Nonessential elements of friendly information Reveal true information to the target Reveal true physical entitles, events, or processes to the target	Conceal facts (dissimulation): Essential elements of friendly information Conceal true information from the target Conceal true physical entitles, events, or processes from the target
Fiction	Reveal fiction (simulation): Essential elements of deception information Reveal false information to the target Reveal false physical entitles, events, or processes to the target	Conceal fiction: Nondisclosable deception information Conceal false information from the target Conceal false physical entitles, events, or processes from the target

Kristin E. Heckman, Frank J. Stech, Ben S. Schmoker, Roshan K. Thomas (2015) "Denial and Deception in Cyber Defense", *Computer*, vol. 48, no. 4, pp. 36–44, Apr. 2015. http://doi.ieeecomputersociety.org/10.1109/MC.2015.104 and Kristin E. Heckman and Frank J. Stech (2015) "Cyber Counterdeception: How to Detect Denial & Deception (D&D)," in Sushil Jajodia, Paulo Shakarian, V.S. Subrahmanian, Vipin Swarup, & Cliff Wang eds. (2015) *Cyber Warfare; Building the Scientific Foundation*. Switzerland: Springer

via poor decisions or attempts to increase their certainty. We describe in this chapter how defenders can integrate cyber-D&D into a system of adversary modeling for ACD.

1 Vision for Cyber-D&D in Active Cyber Defense

Inclusion of Cyber-Denial & Deception (D&D) as Standard Operating Procedure (SOP) As adversaries' attack techniques evolve, defenders' cyber systems must also evolve to provide the best active and continuous defense. We envision cyber-D&D as a key part of the standard operating procedures (SOPs) of cyber defensive and security operations, along with cyber threat intelligence[7] and cyber

[7]"Cyber threat intelligence" is still an evolving concept. See, for example, Cyber Intelligence Task Force (2013) *Operational Levels of Cyber Intelligence,* Intelligence and National Security Alliance, September 2013. http://www.insaonline.org/i/d/a/Resources/Cyber_

operations security (OPSEC).[8] Engineering cyber systems to better detect adversarial tactics and to actively apply D&D against APTs will force adversaries to move more slowly, expend more resources, and take greater risks. In doing so, defenders may possibly avoid, or at least better fight through, cyber attacks.

Assist Defender Use of Cyber-D&D Tools, Tactics, Techniques, and Procedures (TTTPs) in Conjunction with Other Defensive Mitigation TTPs Cyber-D&D is a relatively new concept and cyber defenders have relatively little experience in engineering defensive cyber-D&D operations. The cyber-D&D concept envisions specific aids to provide cyber defenders with information on when and how to use cyber-D&D TTTPs against specific attack TTPs.

Table 2 shows the two-dimensional D&D framework (from Table 1) adapted to cyber-D&D operations. The cyber-D&D defender uses denial to prevent the detection of the *essential elements of friendly information* (EEFI) by hiding what's real, and uses deception to induce misperception by using the *essential elements of deception information* (EEDI) to show what's false. The deceiver also has to hide the false information—that is, the *nondisclosable deception information* (NDDI)—to protect the D&D plan, and additionally show the real information—the *nonessential elements of friendly information* (NEFI)—to enhance the D&D cover story. Deception is a very dynamic process, and deception planners will benefit from the interplay of techniques from more than one quadrant in Table 2 for conducting a defensive deception operation.

Defend Against APT Threats During the Cyber Attack Lifecycle (Both Pre- and Post-Exploit) Ultimately, we envision cyber-D&D TTTPs being engineered to counter APT threats before, during, and after APT exploitation of the defended cyber enterprise vulnerabilities, that is, throughout the lifecycle of the cyber attack, or

Intelligence.aspx; Cyber Intelligence Task Force (2014) *Operational Cyber Intelligence,* Intelligence and National Security Alliance, October 2014. http://www.insaonline.org/i/d/a/Resources/OCI_wp.aspx; Cyber Intelligence Task Force (2014) *Strategic Cyber Intelligence,* March 2014. http://www.insaonline.org/CMDownload.aspx?ContentKey=71a12684-6c6a-4b05-8df8-a5d864ac8c17&ContentItemKey=197cb61d-267c-4f23-9d6b-2e182bf7892e; David Chismon and Martyn Ruks (2015) *Threat Intelligence: Collecting, Analysing, Evaluating.* mwrinfosecurity.com, CPNI.gov.uk, cert.gov.uk. https://www.mwrinfosecurity.com/system/assets/909/original/Threat_Intelligence_Whitepaper.pdf

[8]The concept of "cyber operations security (OPSEC)" has had little systematic development or disciplined application in cyber security. One analyst wrote, "Social media, the internet, and the increased connectivity of modern life have transformed cyber space into an OPSEC nightmare." Devin C. Streeter (2013) "The Effect of Human Error on Modern Security Breaches," *Strategic Informer: Student Publication of the Strategic Intelligence Society:* Vol. 1: Iss. 3, Article 2. http://digitalcommons.liberty.edu/si/vol1/iss3/2 See also Mark Fabro, Vincent Maio (2007) *Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments, Version 1.0 Draft*, Idaho Falls, Idaho: Idaho National Laboratory, INL Critical Infrastructure Protection Center, February 2007. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/OpSec_Recommended_Practice.pdf

Table 2 D&D methods matrix with cyber-D&D techniques

Deception objects	Deception: M-type methods	Denial: A-type methods
	Revealing	Concealing
Facts	Reveal facts: Nonessential elements of friendly information Publish true network information Allow disclosure of real files Reveal technical deception capabilities Reveal misleading, compromising details Selectively remediate intrusion	Conceal facts (dissimulation): Essential elements of friendly information Deny access to system resource Hide software using stealth methods Reroute network traffic Silently intercept network traffic
Fiction	Reveal fiction (simulation): Essential elements of deception information Misrepresent intent of software Modify network traffic Expose fictional systems Allow disclosure of fictional information	Conceal fiction: Nondisclosable deception information Hide simulated information on honey pots Keep deceptive security operations a secret Allow partial enumeration of fictional files

what Lockheed Martin termed "the cyber kill chain."[9] Our concept applies similarly to the "left-of-exploit" APT TTPs. In this chapter, however, we focus on APT post-exploit TTPs, or "right-of-exploit."

An Integrated Approach that Facilitates Communication and Coordination Between Analysts, Operators, and D&D Planners Deception operations require careful planning, preparation, and execution; communications among cyber operations, cyber threat intelligence, and cyber OPSEC functions; close coordination of ongoing denial and deception activities and other defensive and mitigation operations; feedback from cyber threat intelligence to deception operations on the success or failure of deception activities; and close monitoring of the APT adversary's actions and

[9]E.M. Hutchins, M.J. Cloppert, and R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Cyber Kill Chains," presented at the 6th Ann. Int'l Conf. Information Warfare and Security, 2011; www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LWhite-Paper-Intel-Driven-Defense.pdf

reactions to maintain OPSEC for the defensive cyber deception operations.[10] Our concept for cyber-D&D envisions a shared vocabulary, comprehensive framework, and a systems approach to cyber-D&D operations to facilitate communication and coordination between cyber analysts, cyber defensive operators, and cyber-D&D operators.

2 Key Elements of Integrating Cyber-D&D into Adversary Modeling

The cyber-D&D defensive concept described in this chapter envisions several key elements that must be integrated to communicate and coordinate deception with other defensive operations to influence sophisticated adversaries to the benefit of the enterprise defenders.

Cyber Threat Intelligence The cyber-D&D defensive system depends on threat intelligence on the attacker's TTPs. Defenders must be able to obtain, process, and use both public and private threat information; collect observable systems and network data; correlate sensor data to indicators of possible attacker TTPs; specify the characteristics of the attacker TTPs; monitor and track the frequencies of attacker use of various TTPs; and specify known and possible attack patterns of TTPs used by APTs.[11]

Systems and Network Sensors Enterprise networks require host, server and network sensors, as well as associated storage and processing infrastructure, to observe and characterize system behavior and attacker TTPs. They also require sensors to monitor cyber-D&D influence attempts and the effectiveness of defensive mitigations in influencing attacker behaviors. Sensors enable defenders to determine if mitigations and deceptions are working or not, when to reinforce such efforts, or when to switch to back-up plans for defenses.

Intrusion Detection and Adversary Behavior Analysis Defenders will require an analytic platform for analysis of data collected from systems and network sensors for the purpose of intrusion detection and situational awareness. The platform should allow for correlation of data to detect adversary presence and scope of intrusion. When sufficient data is unavailable, it should also allow defenders to

[10] Bodner et al. argue "Working in unison is the only way we can reverse the enemy's deception," and offer an overview on applying integrated cyber-D&D to defense operations and implementing and validating cyber-D&D operations against the adversary's OODA loop; Sean Bodmer, Max Kilger, Gregory Carpenter, and Jade Jones (2012) *Reverse Deception: Organized Cyber Threat Counter-Exploitation,* New York: McGraw-Hill, p. 354.

[11] See, for example, David Chismon and Martyn Ruks (2015) Threat Intelligence: Collecting, Analysing, Evaluating. mwrinfosecurity.com, CPNI.gov.uk, cert.gov.uk. https://www.mwrinfosecurity.com/system/assets/909/original/Threat_Intelligence_Whitepaper.pdf

estimate, with some confidence level, that an attacker may be within the network and enable further investigation to increase confidence. Ideally, this analytic platform should not be located in or directly accessible from the enterprise network, which may allow for the attacker to gain awareness of intrusion detection and cyber-D&D defensive capabilities.

Defender Mitigations As defenders characterize attacker TTPs, they need specific mitigations and cyber-D&D TTTPs to use against the attacker TTPs that defenders detect are being used against their enterprise. Defender mitigations and specific cyber-D&D TTTPs should be crafted for specific attacker TTPs.

RED—BLUE Experimentation To some extent, effectiveness of attacker detection, TTP mitigations, and cyber-D&D TTTPs can be estimated and measured technically. That is, some attacker TTPs can be completely defeated or deceived by technical means. However, mitigating, denying, or deceiving some attacker TTPs depends upon successfully influencing the attacker. To measure the success of mitigation recommendations and cyber-D&D TTTPs, experiments and exercises (i.e., RED teams emulating attacker behavior pitted against BLUE teams using the analytic platform and employing cyber-D&D) may be necessary to gain confidence that the mitigations and cyber-D&D methods will influence the adversary as needed.

3 Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)

The recently developed MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) model[12] provides a taxonomy and framework describing APT actions and behavior in an enterprise network during the post-exploit phases of the cyber attack lifecycle. The model incorporates technical descriptions of TTPs, details specific sensor data observables and indicators for each TTP, describes detection analytics for the TTPs, and specifies potential mitigations. ATT&CK describes techniques that can be used against Microsoft Windows-based enterprise network environments, but the concept and methodology for deconstructing TTPs with an adversarial mindset can be extended into other technologies and operating systems.

While there is significant research on initial exploitation and use of perimeter-focused cyber defenses, there is a gap in public knowledge of adversary process after initial compromise and access to an enterprise network. ATT&CK incorporates information on adversary TTPs gathered from various sources, including MITRE research, public threat intelligence, penetration testing, vulnerability research, and from RED versus BLUE team exercises and experiments. ATT&CK collects knowledge characterizing the post-exploit activities of cyber adversaries. ATT&CK

[12] See https://attack.mitre.org/wiki/Main_Page for details on the ATT&CK model and framework.

Table 3 MITRE ATT&CK matrix™—overview of tactics and techniques described in the ATT&CK model

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Shortcut Modification		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		Bypass UAC		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		DLL Injection		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		Indicator blocking on host		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Exploitation of Vulnerability	Indicator removal from tools		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit		Indicator removal from host			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts		Masquerading			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		NTFS Extended Attributes			Windows admin shares			
Mod. Exist'g Service		Obfuscated Payload						
Registry Run Keys		Rootkit						
Serv. Reg. Perm. Weakness		Rundll32						
Windows Mgmt Instr. Event Subsc.		Scripting						
Winlogon Helper DLL		Software Packing						

MITRE

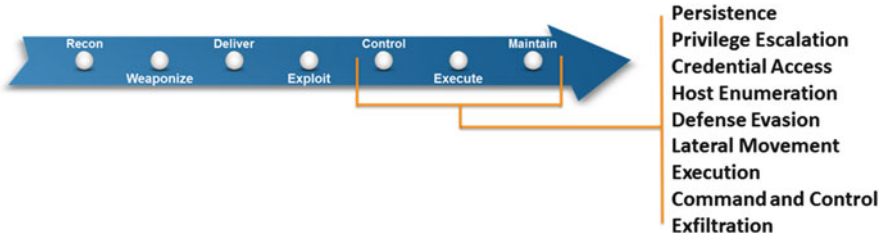

Fig. 1 ATT&CK™ adversary model. *Source*: https://attack.mitre.org/wiki/File:9_tactics.png

includes the TTPs adversaries use to make decisions, expand access, and execute their objectives. ATT&CK describes an adversary's steps at a high enough level to be applied widely across different platforms, while maintaining enough details to be technically applicable to cyber defenses and research.

The nine tactic categories for ATT&CK (Table 3, top row), ranging from Persistence to Exfiltration, were derived from the later stages (Control, Maintain, and Execute) of the seven stage cyber attack lifecycle (Fig. 1).

Focusing on these post-exploit tactic categories provides a deeper level of granularity in describing what can occur during an intrusion, after an adversary has acquired access to the enterprise network. Each of the nine tactic categories (e.g., Persistence) lists specific techniques an adversary could use to perform that tactic

(e.g., Legitimate Credentials). Note that several techniques may serve more than one post-exploit tactic. For example, the technique of using "Legitimate Credentials" can serve three tactic categories: Persistence, Privilege Escalation, and Defense Evasion.

We are currently developing and adding cyber-D&D TTTPs to the ATT&CK Matrix cells. These cyber-D&D TTTPs will complement or substitute for the defensive mitigations in the matrix. To understand the efficacy of cyber-D&D TTTPs for defense, we are currently exploring experimental validation. We have an experimental design with control and test conditions which balances scientific rigor with ecological validity. In this design, participants will be using a number of steps from the ATT&CK Matrix to attack a network, which will be defended by a cyber-D&D tool in one of the test conditions, and in the other test condition, the network will be "defended" by participants' belief that the network uses cyber-D&D defenses. The cyber-D&D tool captures command line commands, silently fails to execute a set of specified commands, but reports execution success.

Much like using ATT&CK to identify gaps in detection coverage of adversary behavior, applying empirical adversary threat intelligence to the ATT&CK model helps focus cyber-D&D on the commonly used techniques across current threat activity. This forms the basis of knowledge necessary to construct cyber-D&D methods against techniques most likely to be used by threats to a particular network or organization.

4 D&D Types and Tactics

Just as the D&D methods matrix includes both facts and fictions, and concealing (i.e., ambiguity-producing denial methods) as well as revealing (i.e., misleading-type deception methods), each of the four cells in the D&D methods matrix (Tables 1 and 2) can contain a variety of D&D tactics, as shown in Fig. 2.[13]

In turn, these D&D tactics can be engineered into cyber-D&D TTTPs. For example, Fig. 3 shows a number of attacker (top) and defender (bottom) D&D TTPs mapped to the D&D methods matrix. Conversely, the D&D methods matrix and associated D&D tactics are being used to develop defensive cyber-D&D TTTPs for the specific post-exploit adversary TTPs shown in the ATT&CK matrix.

In other words, defenders using cyber-D&D need to have cyber-D&D TTTPs available and ready to employ when attacker TTPs are detected (e.g., through the ATT&CK model techniques). As adversaries develop new attack TTPs, and adjust and adapt old ones to counter cyber defenses, the D&D matrix can help

[13]Definitions of the D&D tactics shown in Fig. 2 are provided in Kristin E. Heckman, Frank J. Stech, Roshan K. Thomas, Ben Schmoker, and Alexander W. Tsow *Cyber Denial, Deception& Counterdeception: A Framework for Supporting Active Cyber Defense.* Switzerland: Springer, ch. 2.

defenders adapt old, or develop new, cyber-D&D TTTPs. To be fully effective, cyber-D&D defensive operations can be planned, prepared, and executed using the cyber deception chain.

5 Cyber-Deception Chain

The deception chain is a high-level meta-model for cyber-D&D operations management from a lifecycle perspective (Fig. 4). Analogous to Lockheed Martin's "cyber kill chain" model,[14] the deception chain is adapted from Barton Whaley's ten-step process for planning, preparing, and executing deception operations.[15] The deception chain facilitates the integration of three systems—cyber-D&D, cyber threat intelligence, and cyber operations security (OPSEC)—into the enterprise's larger active defense system to plan, prepare, and execute deception operations. Deception operations are conducted by a triad of equal partners working those three systems interactively: cyber-D&D planners, cyber threat intelligence analysts, and cyber-OPSEC specialists. This triad (planners, analysts, and specialists) is essential for a threat-based active cyber defense. Just as computer network defense (CND) is not any one tool but a system that deploys new technologies and procedures as they

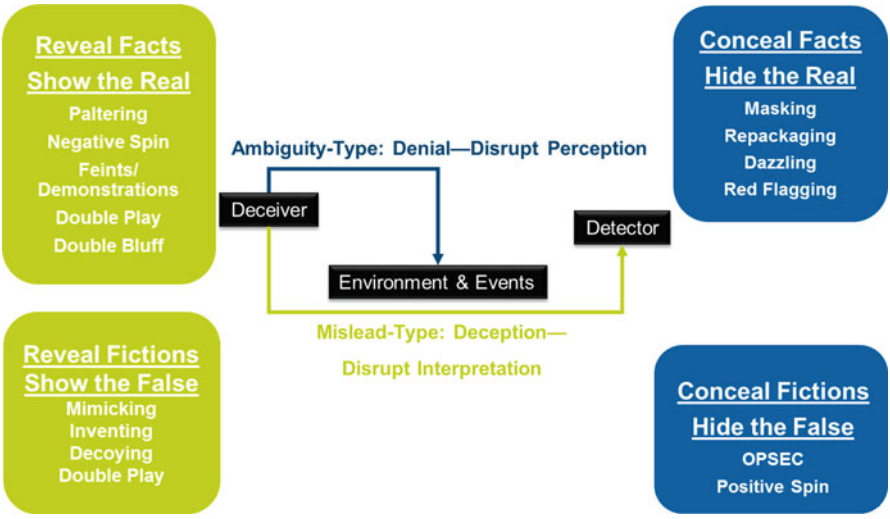

Fig. 2 Types of D&D tactics

[14]E.M. Hutchins, M.J. Cloppert, and R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Cyber Kill Chains," Op cit.

[15]Barton Whaley, "Toward a General Theory of Deception," J. Gooch and A. Perlmuter, eds., *Military Deception and Strategic Surprise*, Routledge, 2007, pp. 188–190.

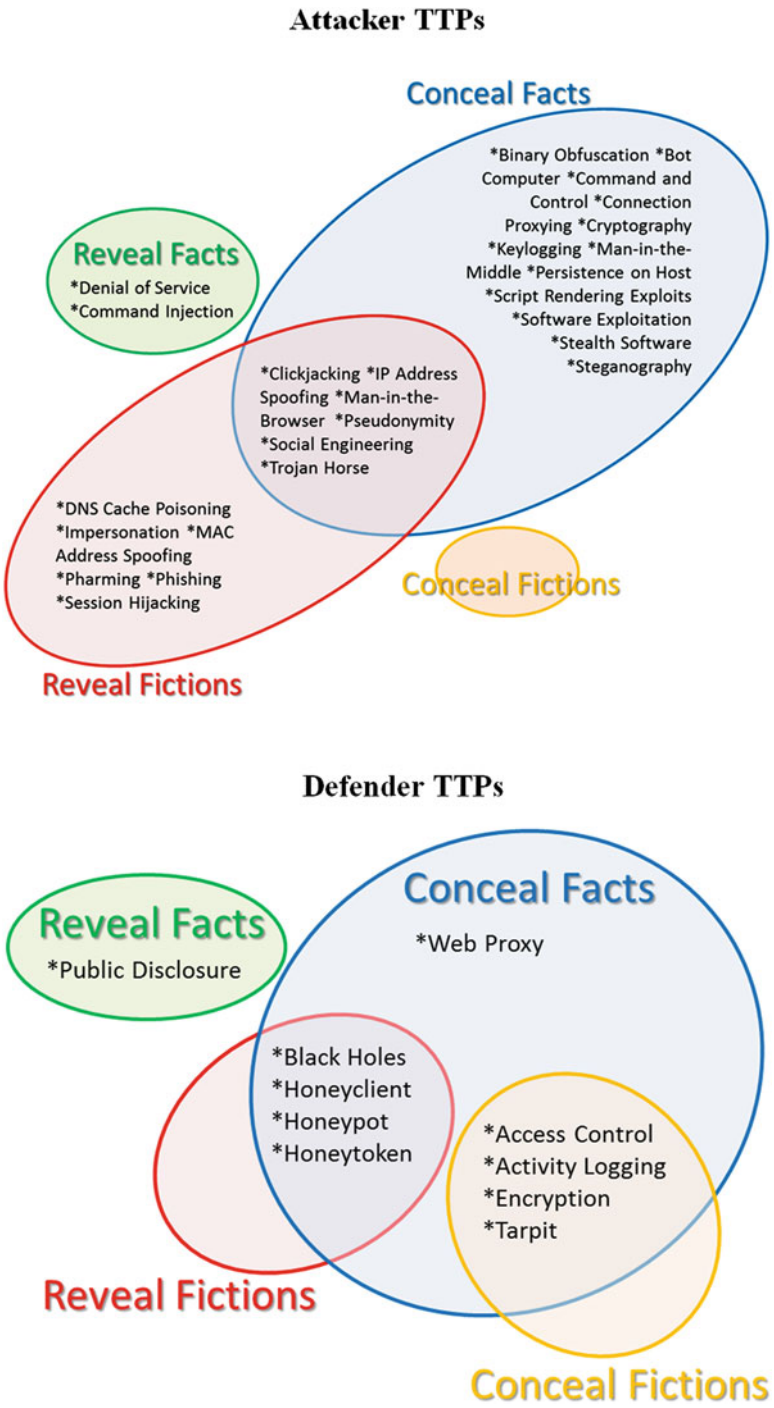

Fig. 3 Cyber D&D TTPs

become available, cyber-D&D must be thought of as an active defensive operational campaign, employing evolving tools, tactics, techniques, and procedures (TTTPs). We believe the deception chain is a flexible framework for embedding advanced TTTPs into operational campaigns while focusing on an organization's mission objectives. There are eight phases in the deception chain (Fig. 4).

Purpose This initial phase helps enterprise managers define the strategic, operational, or tactical goal for the deception operations—in other words, the purpose of the deception—and the criteria that would indicate the deception's success. Since deception operations fundamentally aim to influence the adversary's behavior, the purpose of cyber-deception operations should be defined in terms of the desired influence on the behaviors of the adversary. That is, the deception operation's goal is to influence the adversary to take action or inaction to the benefit of the defender.

Collect Intelligence In the next phase of the cyber-deception chain, D&D planners define how the adversary is expected to behave in response to the deception operation. Defining expected behaviors is done in part through the planners' partnership with cyber threat intelligence, to determine what the adversary will observe, how the adversary might interpret those observations, how the adversary might react (or not) to those observations, and how defenders will monitor the adversary's behavior. This threat intelligence will help planners during the last two phases (monitor and reinforce) to determine whether the deception is succeeding. Cyber threat intelligence can inform D&D planners on what the adversary already knows, believes, and potentially their expectations.

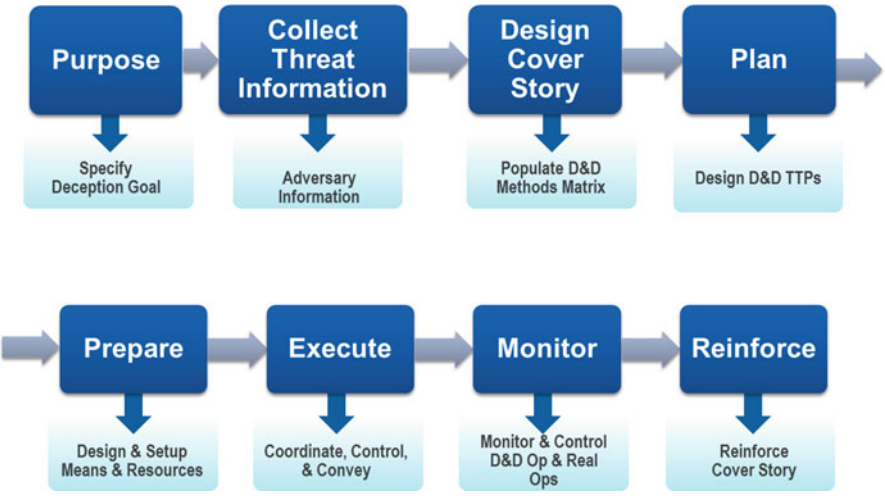

Fig. 4 The cyber-deception chain

One internal source of cyber intelligence is intrusion campaign analysis.[16] Broadly speaking, an intrusion campaign is a framework for grouping related intrusion events and artifacts into knowledge about particular threats to an organization. Analytic methodologies such as the Diamond Model of Intrusion Analysis are also useful in grouping activities in a consistent way.[17] Threat-sharing partnerships are another source of cyber threat intelligence and might involve government, private industry, or non-profit organizations. Information may be shared through various means. Two examples of efforts created for scalable and secure sharing of threat information are the Structured Threat Information eXpression (STIX; http://stix.mitre.org) and Trusted Automated eXchange of Indicator Information (TAXII; http://taxii.mitre.org) systems, sponsored by the Office of Cybersecurity and Communications at the US Department of Homeland Security. STIX and TAXII provide structured formats for defenders to share threat indicators in a manner that reflects the trust relationships inherent in such transfers. STIX is a community-driven language used to represent structured cyber threat information. It contains a structured format for the cyber-deception chain. TAXII enables the sharing of information across organization and product boundaries to detect and mitigate cyber threats. A threat seen by one partner today might be the threat facing another partner in the near future. All of these sources of cyber threat intelligence can aid D&D planners in assessing an adversary's cyber attack capability maturity, which in turn supports the development of an appropriately customized cyber-D&D operation.

Design Cover Story The *cover story* is what the cyber-D&D planner wants the adversary to perceive and believe. The D&D planner will consider the critical components of the D&D operation, assess the adversary's observation and analysis capabilities, and develop a convincing story that "explains" the operation's components observable to the adversary, but misleads the adversary as to the meaning and significance of those observations. The D&D planner will decide what information must be hidden (the EEFI and the NDDI, Table 2) and what information must be created and revealed (the EEDI and the NEFI, Table 2). The D&D methods matrix in Tables 1 and 2 aid planners by capturing the true and false information that must be revealed or concealed to make the deception operation effective. The planners and cybersecurity operators must decide what information "belongs" in the four cells of the matrix and get buy-in from enterprise managers for the deception goals and cover story.

Plan In this phase, cyber-D&D planners analyze the characteristics of the real events and activities that must be hidden to support the deception cover story, identify the corresponding signatures that would be observed by the adversary, and plan to use denial tactics (such as masking, repackaging, dazzling, or red

[16]MITRE, Threat- Based Defense: A New Cyber Defense Playbook, 2012; www.mitre.org/sites/default/files/pdf/cyber_defense_playbook.pdf

[17]Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "Diamond Model of Intrusion Analysis," Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2013.

flagging, Fig. 2) to hide the signatures from the adversary. Planners also analyze the characteristics of the notional events and activities that must be portrayed and observed to support the cover story, identify corresponding signatures the adversary would observe, and plan to use deception tactics (such as mimic, invent, decoy, or double play or double bluff,[18] Fig. 3) to mislead the adversary. In short, D&D planners turn the matrix cell information into operational activities that reveal or conceal the key information conveying the cover story. These steps must be coordinated with cyber OPSEC activities so that the D&D steps are as realistic and natural as possible, and the deception should allow the adversary to observe real operational events that support the cover story.

Prepare In this phase, D&D planners design the desired perceptual and cognitive effects on the adversary of the deception operation and explore the available means and resources to create these effects. This entails coordination with OPSEC specialists on the timing for developing the notional and real equipment, staffing, training, and other preparations to support the deception cover story.

Execute As the deception preparations and real operational preparations are synchronized and supported, the D&D planners and OPSEC specialists must coordinate and control all relevant ongoing operations so they can consistently, credibly, and effectively support and execute the deception cover story, without hindering or compromising the real operations.

[18]The tactics "mimic, invent, decoy" are all commonly used terms describing actions to mislead. The tactic "double play," or "double bluff," requires some explanation. A double play or a double bluff is a ruse to mislead an adversary (the deception "target") in which "true plans are revealed to a target that has been conditioned to expect deception with the expectation that the target will reject the truth as another deception," Michael Bennett and Edward Waltz (2007) *Counterdeception: Principles and Applications for National Security.* Boston: Artech House, p. 37. A poker player might bluff repeatedly (i.e., bet heavily on an obviously weak hand) to create a bluffing pattern, and then sustain the bluff-like betting pattern when dealt an extremely strong hand to mislead the other players into staying in the betting to call what they believe is a weak hand. The double play formed the basis of a famous Cold War espionage novel, John le Carré's, *The Spy Who Came in from the Cold*. An intelligence service causes a defector to reveal to an adversary the real identity of a double agent mole spying on the adversary. The defector is then completely discredited as a plant to deceive the adversary, causing the adversary to doubt the truth, that the mole could actually be a spy. The Soviet Union *may* have used a version of the double play to manipulate perceptions of a defector (Yuriy Nosenko), i.e., "too good to be true," to mislead the CIA to doubt the bona fides of Nosenko and other Soviet defectors (e.g., Anatoliy Golitsyn). See Richards J. Heuer, Jr. (1987) "Nosenko: Five Paths to Judgment," *Studies in Intelligence*, vol. 31, no. 3 (Fall 1987), pp. 71–101. Declassified, originally classified "Secret." http://intellit.muskingum.edu/alpha_folder/H_folder/Heuer_on_NosenkoV1.pdf However, "blowing" an actual mole with a double play is atypical of what CIA counterintelligence agent, Tennent Bagley, called "Hiding a Mole, KGB-Style." He quotes KGB colonel Victor Cherkashin as admitting the KGB dangled "Alexander Zhomov, an SCD [Second Chief Directorate] officer," in an "elaborate double-agent operation in Moscow in the late 1980s to protect [not expose] Ames [the KGB's mole in the CIA]." Tennent H. Bagley (2007) *Spy Wars: Moles, Mysteries, and Deadly Games*. New Haven: Yale University Press, p. 226. http://cdn.preterhuman.net/texts/government_information/intelligence_and_espionage/Spy.Wars.pdf

Monitor D&D planners work with cyber threat intelligence analysts and OPSEC specialists to monitor and control the deception and real operations. This entails monitoring both friendly and adversary operational preparations, carefully watching the observation channels and sources selected to convey the deception to the adversary, and monitoring the adversary's reaction to the "performance," that is, the cover story execution. These targeted channels must remain open to the adversary, convey the planned deception, and be observed by the adversary to convey the cover story. Most importantly, cyber-D&D operators must monitor the adversary to determine if deception operations are having the desired effect on adversary behavior.

Reinforce If cyber intelligence on the adversary indicates that the deception operation does not seem to be "selling" the cover story to the adversary and creating the desired effects on the attacker's behavior, the D&D planners may need to reinforce the cover story through additional deceptions, or to convey the deception operation to the adversary through other channels or sources. The planners may have to revisit the first phase of the deception chain, execute a back-up deception, or plan another operation.

6 The Deception Chain and the Cyber Kill Chain

Adversaries follow a common pattern of behavior to compromise valuable information in a target network. Adversaries generally employ a cyberattack strategy, divided into the six phases of the cyber kill chain or attack lifecycle. Like the cyber kill chain, the deception chain is not always linear. Progression through the phases can be recursive or disjoint. One run of the kill chain models a single intrusion, but a campaign spanning multiple engagements builds on previous results and omits phases as necessary (Fig. 5). Similarly, D&D planners and cyber defense operators will selectively run through the deception chain to achieve their goals. The deception chain is also applicable at each phase of the cyber kill chain, and deception operational goals may be associated with each kill chain phase, as suggested by the following hypothetical D&D tactics:

Recon: If defenders are aware of adversarial reconnaissance efforts, provide the adversary with a set of personae and a Web footprint for defensive targeting efforts in the delivery phase. Note that deception operations can be used to influence adversary actions in future kill chain phases.

Weaponize: Making the adversary (wrongly) feel certain about an organization's vulnerabilities, defense posture, or capabilities could enable the organization to recognize or defend against the adversary's weaponized payload. If the recon phase was successful, the adversary will attempt to deliver the weaponized payload to one or more of the false personae.

Exploit: Recognizing exploitation attempts, defenders may redirect the adversary to a honeypot environment, which appears to be part of a network that contains

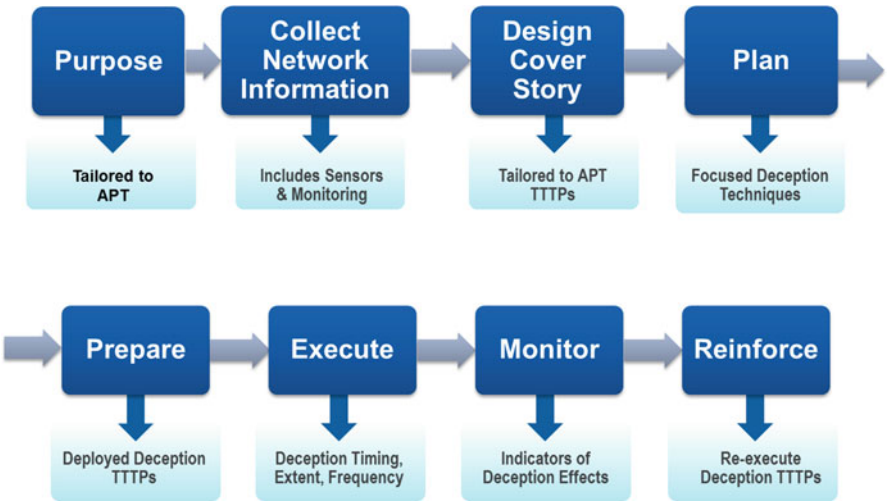

Fig. 5 Building a cyber-deception chain defense

valuable information but is actually isolated and monitored by defenders. The goal is to conceal all honeypot "tells" or indicators to delay the adversary.

Control: When the adversary has "hands on keyboard" access, provide the adversary with a high interaction honeypot with a rich variety of information, designed with the D&D planners, to help identify the adversary's motives, intentions, and capability maturity.

Execute: Slow the adversary down by simulating system interrupts to collect cyber intelligence.

Maintain: Keep up the appearance of realism in a high-interaction honeypot by adding or retiring false personae, as well as maintaining existing personae and their "pocket litter," such as files, email, password change history, login history, and browser history.

These examples also show that there may be a need for more than one deception operation during a single intrusion.

The example below shows a cyber-deception chain built to deflect the attacker TTP of using Legitimate Credentials. The ATT&CK Matrix defines this TTP as:

> Adversaries may steal the credentials of a specific user or service account using Credential Access techniques. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network and may even be used for persistent access to remote systems. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. The adversary may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.[19]

[19] https://attack.mitre.org/wiki/Legitimate_Credentials

The overlap of credentials and permissions across a network is of concern because the adversary may be able to use Legitimate Credentials to pivot across accounts and bypass any access controls. The Legitimate Credentials TTP serves the attack tactic categories of Persistence, Privilege Escalation, and Defense Evasion.

6.1 Purpose: Legitimate Versus Compromised Credentials

The defensive cyber-D&D operators begin to plan the cyber-deception chain by establishing a *Deception Goal:*

> To influence the adversary to utilize compromised credentials and enable them to further their operations via known false accounts whose usage can be tracked and whose pocket litter can be prepared to further enable the adversary to operate in a means controlled by the defense.

The defensive cyber-D&D operators specify *Effectiveness and Influence Measures* to monitor and measure the effectiveness of their deception operations:

> Detection delay; operational delay; adversary confusion; self-doubt; extra actions; exposed malware; wasted time; dwell time; and dwell ratio.

6.2 Collect Information: Legitimate Credentials: Tactics and Technical Description

Development of the cyber-deception chain continues by *Collecting Network Information* such as sensor data to detect the specific attacker technique, as shown in Table 4.

6.3 Design Cover Story: D&D Methods Matrix

The cyber-D&D defenders then design the deception operation *Cover Story* using the denial and deception (D&D) methods matrix (Tables 1 and 2) to specify the facts and fictions that must be revealed or concealed (Table 5) and the deception operations needed.

6.4 Plan: Legitimate Credentials: Detection and Mitigation

The building of the cyber-deception chain continues with the *Planning* of cyber-D&D TTTPs based on an understanding of enterprise network attacker detection

Table 4 Legitimate Credentials attacker technique and detection methods

Attacker technique: Legitimate Credentials	Detection
Permissions required: user, administrator Effective permissions: user, administrator Data sources: authentication logs, process monitoring Defense bypassed: antivirus, firewall, host intrusion prevention systems, network intrusion detection system, process whitelisting, system access controls	Suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information; e.g. a user has an active login session but has not entered the building or does not have VPN access

https://attack.mitre.org/wiki/Legitimate_Credentials

capabilities, and the set of mitigations defined for the Legitimate Credentials ATT&CK TTP (Table 6).

Planning concludes with the identification of a set of parallel defensive cyber-D&D TTTPs that can complement or substitute for the defender mitigations against the attacker TTP Legitimate Credentials (Table 7).

The defensive cyber-D&D operators then *Prepare*, *Execute*, *Monitor*, and *Reinforce* the cyber-deception chain defenses, coordinating with the ongoing enterprise operations, cyber threat intelligence, and cyber OPSEC.

7 Summary

Paradigms for cyber defense are evolving, from static and passive perimeter defenses to concepts for outward-looking active defenses that study, engage, and influence the cyber adversary. This evolution opens the door at tactical, operational, and strategic levels for cyber-D&D to enhance defenses for cyber enterprises,

Table 5 Designing the cover story using the D&D methods matrix

	Reveal-deception	Hide-denial
Facts	• Deception bait accounts with less guarded credentials • Drop clues: "Baited deception accounts are being used to trap attackers" • Some deception bait accounts are harder to access than other deception accounts	• Deception bait accounts facilitate lateral movement to honey traps and other defender controlled systems • Make all deception accounts easier to access than real accounts • Attacker is under observation (and possibly control)
Fictions	• Defender actions: "All legitimate credential account accesses are treated equally"	• Defender actions: Hacked real accounts receive extra deception defenses to make them appear to be bait accounts

Table 6 Preparing deployed deception TTTPs

Detection	Mitigation
Suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information; e.g. a user has an active login session but has entered the building or does not have VPN access	1. Take measures to detect or prevent credential dumping or installation of keyloggers. 2. Limit credential overlap across systems to prevent access if passwords and hashes are obtained. 3. Ensure local administrator accounts have complex, unique passwords across all systems on the network. 4. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled as this is often equivalent to having a local administrator account with the same password on all systems.

such as outlined in the concepts described in this chapter. Cyber-D&D is an emerging interdisciplinary approach to cybersecurity, combining human research, experiments, and exercises into cyber-D&D operations with the engineering and testing of appropriate cyber-D&D TTTPs.

Table 7 Planning deception TTTPs to be deployed

Attacker technique: Legitimate Credentials	
ATT&CK mitigations	Parallel D&D techniques
1. Take measures to detect or prevent credential dumping or installation of keyloggers.	Set up deception accounts with less guarded credentials as bait for attackers. Detect and monitor credential dumping and installation of keyloggers to determine if attackers find deception bait accounts.
2. Limit credential overlap across systems to prevent access if passwords and hashes are obtained.	Set up deception bait accounts with less guarded credentials, with credentials overlap across systems to facilitate attacker access if passwords and hashes are obtained for bait accounts.
3. Ensure local administrator accounts have complex, unique passwords across all systems on the network.	Make some deception bait accounts harder to access than other deception accounts, but make all deception accounts easier to access than real accounts. Link bait accounts to honey traps, etc.
4. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled as this is often equivalent to having a local administrator account with the same password on all systems.	Put deception bait accounts in the local administrator groups across systems with looser controls. Prepare deception materials to support cover story, in the event real accounts are compromised, that deception accounts are being used.

There is currently no coherent intellectual "center of gravity" for developing an integrated concept for cyber-D&D systems for active cyber defenses such as the concept we have described. Such a center of gravity would conduct and coordinate innovative research, standards development, cyber-D&D systems engineering, shared repositories, and training curriculum creation for cyber-D&D. Integration is lacking for developing policies and programs in cyber-D&D, and for coordinating the development and use of cyber-D&D defenses. The concept of a defensive cyber-D&D center of gravity would involve three action areas:

- Standards, methodologies, and shared repositories;
- Research and operational coordination; and
- Active defense cyber-D&D enterprise organization.

The first area focuses on best practices and standards for defensive cyber-D&D:

- Cataloging ongoing offensive and defensive cyber-D&D techniques;
- Mapping ongoing cyber threats to appropriate D&D techniques to support cyber threat intelligence on adversaries and intrusion campaign analysis;
- Conducting outcome analysis of operational cyber-D&D defensive techniques, impacts, and effectiveness; and
- Enabling the sharing of standards and methodologies through repositories of tools and practices to counter cyber threats with defensive D&D.

The second area focuses on facilitating four types of information exchange:

- Strategic, to formulate cyber-D&D policy, programs, and sponsorship for participants and stakeholders;
- Research management, to formulate a strategic cyber-D&D research roadmap with cyber researchers and operational community participation;
- Research, to share technical cyber-D&D research; and
- Transformation, to formulate an operational roadmap that incorporates cyber-D&D research results into cyber defense operations.

Government-sponsored research needs to lead the effort and commercial technology needs to make substantial investments.

Success in the third area requires an organization to serve as a trusted intermediary to broker cyber-D&D operational sharing, collaboration, and networking to manage cyber-D&D defenses in the threat landscape, while safeguarding such techniques from compromise to cyber adversaries.

This organization would also organize sharing of cyber-D&D information exchange at highly detailed technical levels via technical exchange meetings, shared repositories, and standards. The organization would support the identification of near-term and long-term research needs and threat-based defense gaps, and help government, industry, and academia to meet those needs with cyber-D&D defenses. Finally, the defensive cyber-D&D center of gravity organization would foster the development of cyber-D&D training and educational curricula.