

Preface

The field of cyber security has evolved over the last three decades and today is at a critical juncture. Computer network defense (CND) has reached the limits of what traditional perimeter defenses such as boundary controllers and firewalls, as well as intrusion detection systems, can do to increase an organization's overall security posture. Sophisticated, well-organized attackers collectively known as the advanced persistent threat (APT) continue to bypass these traditional defense mechanisms by exploiting zero-day vulnerabilities. Trying to block access by intruders in many cases is futile: it is more realistic to assume that the defense perimeter is porous and that stealthy adversaries may have established a semi-persistent presence in the defender's network. Both researchers and practitioners acknowledge, at least tacitly, that they need more advanced and active defense security techniques. Such techniques would not merely monitor, detect, and block intrusions, but would actively engage adversaries and study their tactics, techniques, and procedures (TTPs) and craft customized responses and mitigation strategies.

Throughout history, denial, deception, and counterdeception have proven effective force multipliers when used in conflict. As the challenges to U.S. national security increasingly move into the cyber domain, the field of cyber security needs an analogous force multiplier to defend effectively against computer network attacks, intrusions, and pervasive electronic espionage. What role can cyber denial and deception (cyber-D&D) play in such a paradigm? That is the subject of this book.

A significant opportunity exists for advancing CND by adapting and applying classical D&D theory and techniques to CND operations. Such adaptation and application entail connecting classical D&D theory and techniques to cyber defense in order to develop a framework that facilitates greater use of D&D in routine CND operations. As adversaries' attack techniques evolve, defenders' cyber systems must also evolve to provide the best continuous defense. This will usher in a new paradigm, consisting of a highly customized network defense based on understanding the specifics of adversary attacks. By knowing how to engineer cyber systems to better detect and counter the deception aspects of advanced cyber threats, and how to apply D&D against the APT and other threats, cyber defenders will force

adversaries to move more slowly, expend more resources, and take greater risks, while themselves possibly avoiding or at least better fighting through cyber degradation.

A review of the cyber security research literature indicates that the use of denial, deception, and counterdeception in the cyber domain is in its infancy when compared to D&D use in the physical world and kinetic warfare.¹ Training in government and academic settings rarely integrates classical deception theory with cyber security. As a result, many computer network defenders have limited familiarity with D&D theory or approaches, let alone how to apply them. This, coupled with disjoint terminology, theory, and lack of a cohesive framework, may have contributed to fewer empirical and operational applications of D&D in cyber security.

Given this, we wished to introduce a wide audience to the role that cyber-D&D can play as part of a larger and more comprehensive active CND scheme. However, this book is not intended as a technical manual for crafting cyber-D&D techniques. Viewing cyber-D&D primarily as a technical initiative or problem would lead to low adoption and failure to counter cyber threats. Instead, concepts for cyber-D&D must be conceived, championed, managed, and matured within the larger organizational, business, and cyber defense context. This book represents our attempt to lay out a blueprint for these broader considerations.

Mc Lean, VA, USA

Kristin E. Heckman
Frank J. Stech
Roshan K. Thomas
Ben Schmoker
Alexander W. Tsow

¹ Frank Stech, Kristin E. Heckman, Phil Hilliard, and Janice R. Ballo. "Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space," *PsychNology Journal*, v. 9, no. 2, pp. 79–122, 2011.

Cyber Denial, Deception and Counter Deception

A Framework for Supporting Active Cyber Defense

Heckman, K.E.; Stech, F.J.; Thomas, R.K.; Schmoker, B.;

Tsow, A.W.

2015, XV, 251 p. 30 illus., 28 illus. in color., Hardcover

ISBN: 978-3-319-25131-8