MICAH ZENKO

RED TEAM

HOW TO SUCCEED BY THINKING LIKE THE ENEMY

RED
TEAM

RED TEAM

HOW TO SUCCEED BY THINKING LIKE THE ENEMY

MICAH ZENKO

A COUNCIL ON FOREIGN RELATIONS BOOK

BASIC BOOKS
A Member of the Perseus Books Group
New York

Published by Basic Books, A Member of the Perseus Books Group

A Council on Foreign Relations Book

Designed by Pauline Brown

Library of Congress Cataloging-in-Publication Data

Zenko, Micah.
Red team : how to succeed by thinking like the enemy / Micah Zenko.
pages cm
Includes bibliographical references and index.
ISBN 978-0-465-07395-5 (ebook) 1. Success in business. 2. Risk management. 3. Private security services. 4. Competition. I. Title.
HF5386.Z46 2015
658.4'01—dc23

20150152

10 9 8 7 6 5 4 3 2 1

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, thin tank, and publisher dedicated to being a resource for its members, government officials, business executive journalists, educators and students, civic and religious leaders, and other interested citizens in order to he them better understand the world and the foreign policy choices facing the United States and oth countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with speci programs to promote interest and develop expertise in the next generation of foreign policy leade convening meetings at its headquarters in New York and in Washington, DC, and other cities where senio government officials, members of Congress, global leaders, and prominent thinkers come together wi CFR members to discuss and debate major international issues; supporting a Studies Program that foste independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtabl that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, t preeminent journal on international affairs and US foreign policy; sponsoring Independent Task Forces tha produce reports with both findings and policy prescriptions on the most important foreign policy topics; an providing up-to-date information and analysis about world events and American foreign policy on website, www.cfr.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has n affiliation with the US government. All views expressed in its publications and on its website are th sole responsibility of the author or authors.

CONTENTS

INTRODUCTION

Within the Roman Catholic Church, the formal title was the *Promotor Fidei*, or Promoter of the Fait More commonly, the position became known within the Church and the laity as the *Advocatus Diaboli*, Devil's Advocate. Today, the term applies to anyone who is a skeptic, or takes an unpopular or contrar position for the sake of argument alone. A professor who provokes discussion by countering studen assumptions, a trial attorney attempting to predict opposing counsel's arguments, or simply a crank—a might be branded devil's advocates according to the more flexible understanding of the term. Within th Catholic Church, however, the role of the Devil's Advocate emerged as a clearly defined position with specific responsibility: to challenge the purported virtues and miracles of nominees for sainthood.

During its first thousand years, the Church's saint-making process had been relatively haphazard an decentralized.[1] Local Christian communities could assign sainthood based on *vox populi*, or popul sentiment, and they avidly awarded the title to those who had died as a martyr, to some who had great professed their faith, or even to those who had done little more than live a particularly pious life. The resu was an explosion of locally proclaimed saints.

In an effort to add rigor to the process in the fifth century, bishops began to require written *vitae*- documentation of the life, virtues, and miracles of candidates—in order for someone to be considered f sainthood. However, those *vitae* were largely based on local gossip and hearsay, with little examination an verification of testimonies. As late as the ninth century, the canonization process, as one scholar described i was "still essentially, as it had been in the second century, the spontaneous act of the local community. Vatican officials perceived that allowing sainthood to be determined by the whims of *vox populi* w becoming a threat to the central authority of the Church.

By the thirteenth century, popes sought to exert greater direct control over the canonization process in a effort to consolidate power within the Vatican and protect the sanctity and legitimacy of sainthood. In 123 Pope Gregory IX—best known for establishing the Inquisition to confront alleged heretics—decreed th the papacy had "absolute jurisdiction" over all aspects of the canonization process. Under subseque reforms, the framework, standards, and procedures of determining sainthood were formalized an centralized within the Sacred Congregation of Rites, the Vatican's committee of cardinals that oversaw an vetted all papal canonizations. In the process, the Devil's Advocate was born.

The Church authorities introduced the position of the *Advocatus Diaboli* to serve as an independe investigator and designated dissenter. It would be his job to provide point-by-point objections to all eviden presented on behalf of the candidate, and to detail all the unfavorable evidence in a written summar Throughout a canonization process that could last decades, corroborating details and objections alike we presented to the sacred Congregation, and ultimately to the pope, before final approval could be granted Thus, Pope Gregory IX made clear to everyone the need for the position of Devil's Advocate, knowledgeable insider who was empowered to step outside of the Church and objectively assess ea candidate for sainthood.

For centuries, these reforms kept the process in check. In 1781, Scottish physician and author Jo

Moore published an account of an abbreviated canonization debate that he witnessed as a tourist in t
Vatican:

> The business is carried on in the manner of a lawsuit. The Devil is supposed to have an interest in preventing men from being made Saints. That all justice may be done, and that Satan may have his due, an advocate is employed to plead against the pretensions of the Saint Expectant, and the person thus employed is denominated by the people, the Devil's Advocate. He calls in question the miracles said to have been wrought by the Saint and his bones, and raises as many objections to the proofs brought of the purity of his life and conversation as he can. It is the business of the Advocate on the other side, to obviate and refute these cavils.[4]

Over time, the Devil's Advocate was transformed from a formal ecclesiastical position into commonplace figure of speech used to describe an argumentative person, and soon enough, the Vatican most senior official decided that the position had outlived its usefulness. In 1983, in an effort to streamli the canonization process, Pope John Paul II issued an Apostolic Constitution reducing the number miracles required from four to two, and eliminating the office of the Devil's Advocate. The reforms wer intended to foster a more cooperative spirit by making the process simpler, faster, and far less adversaria Subsequently, Pope John Paul II produced more beatifications (1,338) and canonizations (482) in som twenty years than all of his 263 predecessors combined over almost two thousand years.[5] With few requirements and the removal of an independent and dissenting voice, the Vatican was transformed in what was dubbed the "saint factory."[6] In becoming far more commonplace, saints were increasingly le venerated, and, in the words of one critic, "inflation produced a devaluation."[7] By eradicating this centurie old institutional check on saint-making, the integrity associated with the process and outcome was negated well. Yet, even though the Vatican eventually abandoned the position, the enduring value of its thirteenth century innovation should not be forgotten.

The office of the Devil's Advocate was the first established and routine use of "red teaming." However red teaming was not formally referred to as such by the US military until the Cold War, and it was on standardized in the 2000s. As it is known today, red teaming is a structured process that seeks to bett understand the interests, intentions, and capabilities of an institution—or a potential competitor—throug simulations, vulnerability probes, and alternative analyses. Though red teaming has subsequently bee adopted in a wide range of fields and tailored to various needs, it remains woefully underexplored an severely underutilized by corporate boardrooms, military commands, cyber-security firms, and countle other institutions that find themselves facing threats, complex decisions, and strategic surprises. B employing a red team, institutions can get a fresh and alternative perspective on how they do things. It ca help them reveal and test unstated assumptions, identify blind spots, and potentially improve the performance.

Al Kibar: "Gotta Be Secret, Gotta Be Sure"

Red teaming is not only about using a devil's advocate to scrutinize and challenge day-to-day operations. Fo institutions facing a significant decision, red teaming may also be a one-time effort. We can see how

properly administrated red team can help ensure that a crucial decision is the right one by studying t
following example found in recent national security decision making.

In April 2007, Israeli national security officials surprised their American counterparts by informing the about a large building under construction at Al Kibar in a valley in the eastern desert of Syria. In one-on-o briefings, the Israeli officials provided dozens of internal and external color photographs dating back before 2003. The evidence strongly suggested that the building was a nuclear reactor, remarkably similar t the gas-cooled, graphite-moderated reactor in Yongbyon, North Korea. Israeli Prime Minister Ehud Olme then delivered his request to President George W. Bush: "George, I'm asking you to bomb the compound.

Senior Bush administration officials were deeply troubled. North Korea had conducted its first nucle weapons test the previous October using plutonium produced in the Yongbyon reactor. The Israeli briefing reinforced the US intelligence community (IC) assessments of "sustained nuclear cooperation" betwee North Korea and Syria. Though the IC had been monitoring the construction of a facility that they ha described as "enigmatic" since 2005, the new Israeli photographs cast the compound in Al Kibar under harsh new light. Immediately, a Central Intelligence Agency (CIA)-led task force reevaluated all of th available intelligence related to Al Kibar and North Korea's nuclear cooperation with Syria. Given th flawed intelligence assessment that resulted in the incorrect conclusion in 2002 about Iraq possessin weapons of mass destruction (WMD), nobody wanted to be wrong again. As Bush told his intelligen chiefs: "Gotta be secret, and gotta be sure."[9]

The CIA task force reaffirmed the Israeli officials' claims, but Bush administration officials too extraordinary measures to increase their confidence level. To ensure that they could be nearly certain in the assessment of Al Kibar, they employed devil's advocate techniques markedly similar to those invented by th Vatican centuries earlier. National Security Advisor Stephen Hadley told IC officials to assemble some their best analysts to review the data to see if the facility could be anything other than a reactor.[10] The CI director, General Michael Hayden, was similarly concerned given that "we had a poor record of assessing th WMD programs of countries bordering the Euphrates River." He noted, "You increase your certainty b widening the circle, but we still had to keep the circle small to keep it a secret." To do this, the IC employe two red teams that were totally independent from the task force and had not yet been "read in" on th intelligence regarding Al Kibar.[11]

Bush's intelligence chiefs so thoroughly bought into the concept of red teaming that they issued the tw groups opposing goals: one would be commissioned to prove "yes" and the other to prove "no." The "yes red team assessment came from a private sector analyst who held a top-secret security clearance and was w known for his proficiency in monitoring nuclear weapons programs. The analyst was not told where th facility was located, but was provided with the Israeli and American internal and overhead imagery of it. Th obvious efforts to camouflage the reactor vessel and the spent fuel pools within a building that had nearly a identical footprint to that of the Yongbyon reactor, and the trenches and pipes leading to a nearby wat source (the Euphrates) were among several telltale giveaways. Within a few days, the analyst informed the I officials, "That's a North Korean reactor."[12]

Hayden's "no" red team was composed of senior analysts from the CIA's Weapons Intelligence Nonproliferation, and Arms Control Center (WINPAC). This team received the same access to all th available data and intelligence as its counterpart, but was explicitly instructed to reach a hypothesis that t

facility in Syria *was not* a nuclear reactor. "Prove to me that it is something else," the CIA director to them. Over the course of the following week, the WINPAC group considered whether Al Kibar cou contain a chemical weapons production or storage site, or something related to missile or rocket program Anything was plausible—they even investigated the possibility that it might be some sort of secretive no weapons-related vanity project of Syrian President Bashar al-Assad. They also explored whether al-Assad ha directed that a mock-up of a reactor be built, simply because he *wanted* it to be bombed for some reaso Another senior CIA official recalled that they had particular difficulty finding an alternative explanation fo the internal photographs of the facility, which not only closely resembled Yongbyon but also even containe what appeared to be North Korean workers.[13] "The alternative hypothesis that they came up with, for whic the most evidence unquestionably and markedly lined up behind, was that it was a fake nuclear reactor Hayden recalled.[14]

At the weekly Tuesday afternoon meeting in Hadley's office, a handful of senior officials met to discus what to do about the purported Syrian reactor. The results of the red-teaming exercises gave officials a hig degree of confidence that they had their facts straight. They took comfort in the additional levels of scrutin that had been applied to the initial intelligence estimates. "It gave us more confidence about the instinct an conclusion of the intelligence community regarding whether it was a reactor. Every other alternati explanation was not plausible," according to Hadley.[15] Secretary of Defense Robert Gates, who attended a of these meetings, also recalled, "Everybody agreed that we could not find an alternative to this being nuclear reactor."[16]

However, even though the Al Kibar compound was all but confirmed to be a nuclear reactor, this did no mean that the United States should accede to Prime Minister Olmert's request to destroy it. While Hayde could comfortably declare, "That's a reactor. I have high confidence," the red teams had notably found n evidence of a facility required to separate spent reactor fuel into bomb-grade plutonium or of weaponizatio work, which further led him to state, "On [the question whether] it is part of a nuclear weapons program, have low confidence."[17] Bush subsequently told Olmert that the United States would not participate in military attack: "I cannot justify an attack on a sovereign nation unless my intelligence agencies stand up an say it's a weapons program."[18]

The two independent intelligence assessments provided Bush administration officials with far greate confidence about what was being constructed in the Syrian desert. They informed Bush's decision-makin calculus, even though his primary concern remained the risks to US interests in the Middle East if I authorized another preemptive attack on a Muslim country. With bombing now off the table, the CI developed options to covertly sabotage the reactor before it went critical; however, CIA Deputy Directo Stephen Kappes told the White House that sabotage had a low likelihood of success.[19] Therefore, Bush cho to pursue diplomatic channels by going public with the intelligence to the United Nations Security Coun and International Atomic Energy Agency, in order to pressure Syria to verifiably dismantle the reacto Before this could happen, four Israeli fighter jets destroyed the suspected reactor at Al Kibar on Septemb 6, 2007, without any resistance from Syria's air defenses or overt support from the United States.

In this case, the findings of the two devil's advocates, based on their independent analysis of availab intelligence, greatly enhanced the credibility of the intelligence estimates regarding the existence of a nucle reactor, and enabled Bush to make up his mind on the basis of more complete and vetted informatio

Ultimately, the president decided to refrain from launching strikes. This was a classic example of re teaming in action—having outsiders test the validity of the intelligence and consider the possibility alternate hypotheses.

Why Organizations Fail, But Can't Know It

This is a book about how to improve the performance of an institution by enabling it to see the world in new and different way. Institutions—whether they are military units, government agencies, or sma businesses—operate according to some combination of long-range strategies, near-term plans, day-to-d operations, and to-do lists. Decision-makers and their employees do not simply show up at their jobs ea morning anew and decide then and there how to work and what to work on. The existing guidanc practices, and culture of an institution are essential to its functioning effectively. Yet, the dilemma for an institution operating in a competitive environment characterized by incomplete information and rap change is how to determine when its standard processes and strategies are resulting in a suboptimal outcom or, more seriously, leading to a potential catastrophe. Even worse, if the methods an institution uses t process corrective information are themselves flawed, they can become the ultimate cause of failure.

This inherent problem leads to the central theme of this book: you cannot grade your own homewor Think back to a high school class where you struggled every day to grasp the subject. Now, imagine that th teacher empowered you to grade your own homework. At first this would seem like a great boon—guaranteed 100 percent every time! No matter how poorly you actually performed, you could decide yo own grade for each assignment. In correcting those assignments you would develop a range rationalizations as to why you really deserved an A, in spite of inferior results: "this wasn't covered in class "the teacher did a lousy job," "I was really tired," or maybe "just this one last time." Now, imagine you shock when, after a semester of self-grading, the teacher hands out the final exam and announces that th time she will be the one holding the red pen. This would expose all the things that you should have learne or maybe thought you understood, but never really did. Grading your own homework might feel good the short term, but it completely clouds one's self-awareness, and can eventually lead to a failing grade.

The warning that "you cannot grade your own homework" has relevance far beyond the classroom Consider the mistaken self-evaluation strategy that was employed by the CIA in its post-9/11 detention an interrogation program. Internal assessments of its operations' necessity and effectiveness—including the u of "enhanced interrogation techniques" (i.e., torture) against suspected terrorists—were conducted by th same CIA personnel that had been assigned to develop and manage the program, and also by outsi contractors who had obvious financial interests in continuing or expanding it. In June 2013, an internal CI review found that its personnel regularly made "assessments on an ad hoc basis" to determine if "variou enhanced techniques were effective based upon their own 'before and after' observations" of changes in detainee's demeanor. [20] Unsurprisingly, the CIA personnel and outside contractors judged with confidenc that the program they worked in was both highly effective and needed.

Despite requests by National Security Advisor Condoleezza Rice and the Senate Select Committee o Intelligence in the mid-2000s to commission what was the equivalent of a red team alternative analysis these programs, none was ever ordered by senior CIA officials. As the Agency acknowledged: "The so

external analysis of the CIA interrogation program relied on two reviewers; one admitted to lacking t requisite expertise to review the program, and the other noted that he did not have the requisite informatio to accurately assess the program."[21] An informed and empowered red team, comprised of knowledgeab experts holding the requisite security clearances, would have offered a more realistic evaluation of the use torture and provided recommendations for how to revise or terminate the detention and interrogatio program.

An astonishing number of senior leaders are systemically incapable of identifying their organization's mo glaring and dangerous shortcomings. This is not a function of stupidity, but rather stems from two routin pressures that constrain everybody's thinking and behavior. The first is comprised of cognitive biases, such a mirror imaging, anchoring, and confirmation bias. These unconscious motivations on decision-makin under uncertain conditions make it inherently difficult to evaluate one's own judgments and actions. A David Dunning, a professor of psychology at Cornell University, has shown in countless environment people who are highly incompetent in terms of their skills or knowledge are also terrible judges of their ow performance. For example, people who perform the worst on pop quizzes also have the widest varian between how they thought they performed and the actual score that they earned.[22]

The second related pressure stems from organizational biases—whereby employees become captured b the institutional culture that they experience daily and adopt the personal preferences of their bosses an workplaces more generally. Over a century ago, the brilliant economist and sociologist Thorstein Veble illustrated how our minds become shaped and narrowed by our daily occupations:

> What men can do easily is what they do habitually, and this decides what they can think and know easily. They feel at home in the range of ideas which is familiar through their everyday line of action. A habitual line of action constitutes a habitual line of thought, and gives the point of view from which facts and events are apprehended and reduced to a body of knowledge. What is consistent with the habitual course of action is consistent with the habitual line of thought, and gives the definitive ground of knowledge as well as the conventional standard of complacency or approval in any community.[23]

Though we would now refer to this derisively as "going native" or "clientism"—whereby people becom incapable of perceiving a subject critically after years of continuous study—any honest employee or staff should recognize this all-pervasive phenomenon that results in organizational biases. This is particular prominent in jobs that require deep immersion in narrow fields of technical or classified knowledge, an those that are characterized by rigid hierarchical authority—the military is a clear example. Taken togethe these common human and organizational pressures generally prevent institutions from hearing bad new without which corrective steps will not be taken to address existing or emerging problems.

When discussing their own leadership and management styles, bosses usually acknowledge the need encourage, appreciate, and thoughtfully listen to dissenting views from their employees. No reputable bo would proclaim, "I make it a point to discourage my staff from speaking up, and I maintain a culture th prevents dissenting viewpoints from ever getting aired." If anything, most bosses even say that they are pr dissent. This sentiment can be found throughout the *New York Times*'s "Corner Office" series o conversations with corporate, university, and nonprofit leaders, published weekly in the newspaper's busine section. In these interviews, the featured leader is asked about their management techniques, and regular

claims to continually foster internal protest from more junior staffers. As Bob Pittman, chief executive
Clear Channel Communications, remarked in one of these conversations: "I want us to listen to the
dissenters because they may intend to tell you why we can't do something, but if you listen hard, wh
they're really telling you is what you must do to get something done."[24] To hear American leaders describ
their organizations, it seems they are run more like cooperative anarchist collectives than hierarchic
institutions.

The trouble is that Pittman's approach wrongly assumes that the people who work for these leaders hav
the skills to identify emerging problems (highly unlikely), that they will tell their bosses about the
problems (potentially career damaging), and that they will face no negative consequences for bringing su
issues to their leaders' attention (rare, since it disrupts the conventional wisdom). Think about what yo
perceive as obvious and readily apparent shortcomings in your own job. Would you risk your reputation
career by raising them with your boss, even if asked to do so? Now, assume that there are unseen disasters
the horizon. How likely is it that you could identify and then warn your boss about them given su
constraints? Harvard Business School professor Amy Edmondson researches why employees in a range
settings believe it is unsafe to admit to and report on failures that they observe in their workplaces. "We ha
a deep, hardwiring that we have inherited that leads us to be worried about impression-making
hierarchies," she says, adding that "no one ever got fired for silence."[25] Just as institutions cannot be counte
upon to grade their own homework, they also do not reliably self-generate dissenting viewpoints that a
presented to senior leaders.

One prominent, recent example of this phenomenon can be seen in the independent investigation in
General Motors's (GM's) decision to wait a decade before recalling its Chevrolet Cobalt compact car tha
had a faulty ignition switch. This defect caused the ignition to inadvertently shut the engine off while drivin
—likely due to a heavy keychain or a shift in its weight—subsequently cutting off power to the pow
steering and brakes, airbags, and antilock brakes. The results included at least 119 deaths and 243 majo
injuries, costs to the company of up to $600 million in victim compensation, and the firings of fifte
members of senior management.[26]

Employees interviewed as part of the investigation "provided examples where culture, atmosphere, an
the response of supervisors may have discouraged individuals from raising safety concerns."[27] GM employe
received formal training in how to describe safety issues in written documents so that their warnings wou
appear less vivid and alarmist. Thus, the suggested replacement for "safety" was "has potential safet
implications," and "defect" became "does not perform to design." In an apparent attempt at humo
employees were also told not to use phrases like "Kevorkianesque," "tomblike," and "rolling sarcophagus
The reason for insisting upon the watered-down language was to deny ammunition to any plaintiff's lega
team that might sue GM over safety issues. However, it also served to undersell the seriousness of the safe
and security problems that the company's employees witnessed. The investigation concluded: "Whethe
general 'cultural' issues are to blame is difficult to ascertain, but the story of the Cobalt is one in which GM
personnel failed to raise significant issues to key decision-makers."[28] It's not that the GM employees wh
refrained from speaking up were unaware of the extent of the ignition switch problems, nor were they ev
people. Rather, they were simply behaving as they believed they should, based upon the tone and form
guidance established by higher management. Instead of employing red teaming to identify and rectify th

problems at the heart of their organization, GM made the problem worse by attempting to avoid the issu by diminishing and outright ignoring them. The result was a near catastrophe for GM, and was tru catastrophic for the victims and their families.

How Red Teams Function

In recent years, red teaming has grown increasingly important as a means of forestalling disasters like th suffered by GM. More and more institutions are using the three core red-teaming techniques of simulation vulnerability probes, and alternative analyses. These tactics are employed by red teams that vary widely composition and activities: from in-house contrarians (like the Vatican's defunct Devil's Advocate), t externally hired "tiger teams" that attempt to break into secure buildings or computer networks, an management consultants tasked with scrubbing a company's strategy. Red teams can also be temporary, suc as when a company's staff uses "liberating structures"—brainstorming techniques used to generat innovation and break conventional thought processes—to stimulate divergent thinking that would not ha occurred otherwise.

Ultimately, whether comprised of outside consultants or everyday employees, red teams help institutio in competitive environments visualize themselves outside of daily routines, evaluate plans, identi institutional and strategic vulnerabilities and weaknesses, and potentially improve performance via thr techniques: simulations, vulnerability probes, and alternative analyses.

Simulations

Prior to scheduled events or anticipated scenarios, institutions develop, test, and refine their strategies b modeling how they could play out in the foreseen situation. The simulations capture each of the actor motivations and capabilities, and the likely interactions between them. In this scenario, red teams can cons of consultants that model litigation outcomes to help law firms decide how they should settle cases; footba scout teams that emulate the next opponent the starting team will face to show their tendencies in various i game situations; or business war-gamers who independently consider future outcomes that can then infor strategic decision-making. The US military also routinely models what are believed to be the emergi international security trends to help develop the concepts and force structure for future defense plannin Two examples are the annual North Atlantic Treaty Organization (NATO) Unified Vision war-gam exercises that test collaboration and information sharing in simulated combat settings, and the US Army Unified Quest program that aims to determine how the Army will fight in future operating environment The military also conducts war games for possible large-scale interventions and discrete military operation For example, the May 2011 US Navy SEAL raid in Pakistan that killed Osama bin Laden was "red teame to death," according to Secretary of Defense Leon Panetta.[29] The SEAL team ran through real-li simulations to test every "what if?" contingency that might arise. Even when one of the SEALs' tw transportation helicopters crash-landed in bin Laden's compound, the mission went off without a hitc because they had planned and trained for that exact contingency.

Vulnerability probes

Computer networks, facilities, and people require protection from their potential adversaries. Red teams ca assume the role of "surrogate adversaries" to test the reliability of a targeted institution's defensive system and procedures to identify any weaknesses. Vulnerability probes should be independent and unannounce based on an updated evaluation of likely adversaries' capabilities and motivations, and conducted in manner realistic as to how they would attempt to breach or damage the targeted institution or system. The can be external hires, such as "white-hat" (or ethical) hackers contracted by firms to assume the role "black-hat" (or malicious) hackers and attempt to compromise that firm's computer systems—the finding of which are then shared with the firm. Or they can be Government Accountability Office undercov investigators who examine the defenses of government agencies, such as those that smuggled radioacti material across the southern and northern US borders in 2006, bomb components into ninete unidentified airports in 2007, and bomb components into ten federal buildings—out of ten attempts— 2009. There are also internal probes by undercover counterintelligence agents within firms or governme agencies that uncover insider threats by bribing or coercing employees to gauge their honesty an dependability.

Alternative analyses

Traditional analyses characterize the current environment within which an institution exists, analyze specif topics, and generate forecasts. These analyses are conducted to support senior leaders who face critic decisions, and to help institutions refine their everyday plans and operations. However, analysts can be he back by normal cognitive biases, or by the patterns of thinking commonly accepted within the organizations. These biases often include mirror imaging, in which analysts instinctively assume that the adversary would think in the same way that the analyst would under similar circumstances; anchoring, wh analysts rely too heavily on initial information or impressions that make significant shifts in their judgme unlikely; or confirmation bias, in which analysts favor those findings that support their personal theories beliefs. The objective of alternative analysis is to hedge against these natural human and organization constraints by using liberating structures or structured analytic techniques, or by employing a whol different team not already immersed in an issue to challenge assumptions or present alternative hypothes and outcomes.[30]

Alternative analysis by its nature involves different people, processes, or products than those involved traditional analysis. Over time, individuals conducting traditional analysis can become heavily influenced b the institutional culture they experience and the personal preferences of their bosses. As a result, ev longtime analysts are susceptible to adopting the assumptions and biases of the institutions and subjects th are supposed to be objectively studying. When properly developed and applied, the approaches an frameworks used in alternative analysis limit cognitive biases and allow for unconventional thinking.

One prominent, publicly available example is the small CIA Red Cell. Separate from mainli authoritative analytical units within the Agency, the Red Cell conducts alternative assessments of I products, or alerts policymakers to unexpected or unorthodox issues.[31] A 2010 Red Cell memo that ra completely counter to conventional thinking on the sources of terrorism was aptly titled, "What Foreigners See the United States as an 'Exporter of Terrorism'?" This type of bracing, counterintuitiv approach can compel policymakers to challenge assumptions that they had previously been unaware of, an

conceive of an issue from a fresh perspective.

How Red Teams Succeed or Fail

Though red teams are unique, like any other management tool their impact can range from priceless t worthless. This predominantly depends on the willingness and receptiveness of an institution's leaders. Whe red teaming is faithfully conducted, correctly interpreted, and judiciously acted upon, it can reve important shortcomings in an institution's methods or strategies. Yet it is just as possible for red teams to b flawed in design or execution, or, as some practitioners say, "prostituted."

Corporations often convene managers to purportedly conduct a red team analysis before launching a ne product or entering an unexplored market. In essence, such exercises can be intended to provide intern validation for the decisions already made by senior management. The Nuclear Regulatory Commissio (NRC), which regulates commercial nuclear power plants, is tasked with conducting force-on-for performance testing—in which inspectors simulate a plausible, fictional adversary and conduct a surpri commando-style attack to probe the facility's defensive vulnerabilities. After the 9/11 terrorist attacks, th NRC was found to be conducting fraudulent testing of simulated terrorist attacks, which included giving u to-twelve months advance notice of a mock attack so that the nuclear facility could increase the number its security guards in preparation. US generals and admirals have increasingly adopted their own person Commander's Initiatives Groups (CIG), which are groups of staffers who are supposed to provide critic thinking of strategies unfettered from the daily activities required of a military commander's staff. I practice, many of the CIGs become "captured" by the daily demands of the office, and find themselv writing speeches, preparing congressional testimony, and presenting memos that they know their bosses wa to hear.

Finally, red teams can be scrupulous in their execution and simply find themselves ignored by decisio makers. In 2010, the US Department of Health and Human Services (HHS) hired McKinsey & Compa to serve as "an independent team charged with 'pressure testing' existing trajectory of federal marketplace of the Patient Protection and Affordable Care Act, or ObamaCare.[32] The McKinsey red team reviewe HHS's strategy and privately warned the White House six months before the October 2013 ObamaCa rollout of likely glitches in the HealthCare.gov website and that "insufficient time and scope of end-to-en testing" had been devoted during preparation for the launch. McKinsey also briefed members of t HealthCare.gov development team—though apparently not its key leaders—about many of t management and technical glitches that would eventually plague the federal healthcare website. Thoug McKinsey had diligently uncovered shortcomings that HHS had not found on its own, the red team findings and warnings were disregarded. Ultimately, the ObamaCare rollout was a needless political disast for the White House and President Barack Obama's approval ratings.[33]

The inherent tension for red teams is how to operate successfully within an institution—obtaining th information and access needed, and having their results listened to—while maintaining the requisi independence to honestly question and rigorously challenge that same institution. This requires the red tea to be intimately aware of the personalities and culture that surround it, without becoming constrained by t commonly accepted range of perspectives. The best red teams exist somewhere in an undefined sweet spo

between institutional capture and institutional irrelevance. Global health expert Gregory Pirio compared t most proficient red teamers to the *ronin* samurai in feudal Japan who, because they had no master, we "free to tell the shogun that he was an idiot." As Pirio further explained, slipping into twenty-first centu consultant-speak, "Since the ronin were de-institutionalized, they didn't know how to shape their messag to meet the mimetic environments."[34] What distinguishes the lone *ronin* speaking truth to a ruler from t red teams assessed throughout this book is that the latter has a more formal routine and relationship with institution and its decision-makers. However, both embody one of the most important aspects of an effecti red team—functioning either at the very edges of, or outside of, the institution it is analyzing.

Into the World of Red Teaming

Red teaming is an inherently social phenomenon that can only be understood by speaking to its practitione and observing how they apply their techniques in the real world. In an effort to convey the best practices a essence of red teaming, this book tells the stories of red teamers at work, often in their own words. The anecdotes have been compiled through interviews with more than two hundred prominent red teamers a their colleagues in a wide variety of fields—from twenty-something-year-old white-hat hackers to senior vi presidents, from former CIA directors to retired four-star generals. A few of them cannot be identified b name because they are not authorized by their employers, or are simply secretive by nature, but all we willing to share their thoughts and experiences because of their belief in the need to expand the practice red teaming. Beyond conversations, it was essential to witness red teaming in action: the "A-ha! momen generated by a consultant forcing corporate staffers to assume the role of competing firms, or the zombi like trance of a hacker intently scanning source code for vulnerabilities. Finally, this exploration would hav been incomplete without taking courses at the Fuld Gilad Herring Academy of Competitive Intelligenc where business war-gaming is taught, and the University of Foreign Military and Cultural Studies (UFMC (i.e., Red Team University), where red team techniques are taught to military officers (and me, the ra civilian) in a refurbished former military prison at Fort Leavenworth, Kansas. Since its transformation 2004, detailed in chapter 2, UFMCS has become the preeminent hub for the study and instruction of r teaming.

This book focuses on the kind of red teaming that occurs in the context of a relatively competitiv environment. This includes potential military conflicts between two or more enemies; marketplace settin where firms contend for market share or returns on investment with direct competitors; legal and regulato regimes that firms "game" to reduce costs and burdens; threatening environments where individual facilities, and critical infrastructure face a heightened risk of attack from potential adversaries; environments of uncertainty where individuals, firms, or intelligence agencies require alternative analyses limit or mitigate the consequences of strategic surprises. In short, this book deals with competiti environments in which there are obvious gains from success, and costs for poor performance.

The seventeen case studies described and analyzed were selected with the objective of presenting reade with the greatest variety of red teaming. For government secrecy, proprietary, or reputational reasons, mo institutions that employ red teams strive to keep them well hidden, sometimes even misrepresenting the structure and impact for outside audiences. Based upon several years of digging, sifting, and interviews, t

mini-cases presented in chapters 2 through 6 emerged as those that were the most rich in information an granular detail, being bolstered with insider accounts that are essential to understanding how red teams a actually formed and operate. The cases also have different compositions, methods of operation, an outcomes—some fail, some succeed, while others have inconclusive or yet-to-be-determined results. Son are diagnostic in nature, while others are intended to elicit new and unconventional thinking. Finally, the include both historical and contemporary examples that demonstrate several commonly recurring barriers improved institutional performance, and how the six specific red team best practices detailed in chapter evolved.

Though red teams exist in multiple challenging environments, no single work has yet assessed an evaluated how they are utilized across various fields, nor has one identified best practices that are similar applicable across those fields. One reason for the lack of comparative analytical research on red teaming that the US government and military rarely provide money to federally funded research organizations—suc as the RAND Corporation—to draw upon nonmilitary fields. Conversely, the private sector does no publish its own red-teaming processes or results, since this is closely held proprietary information that often guarded by nondisclosure agreements with clients. Meanwhile, news accounts of "red teams"—ofte mentioned in quotes—usually lack the proper context and perspective needed to understand how they a used beyond the single issue covered in an article. This book fills the knowledge gap by providing a typolog of techniques, a survey of its uses by way of practitioners and their experiences, and practical guidance th any institution's leader needs to know about how to utilize red teams. Most of the examples are drawn fro the military and national security worlds—communities that have few insights into one another's re teaming efforts—but they have profound applications for the private sector as well.

This exploration into red teaming begins with chapter 1's presentation of the six red-teaming be practices leaders could use to mitigate the cognitive and organizational biases that harm performanc Identified through interviews with more than two hundred red teamers and their colleagues, the six be practices are: 1) The boss must buy in. Without providing "top cover" support and approval for dissentin views, red teams will be under-resourced, marginalized, or wholly ignored. 2) Outside and objective, wh inside and aware. Effective red teams have to be designed with the correct structure relative to the target institution they assess, scope of the activities they pursue, and sensitivity with which they operate and prese their findings and recommendations. 3) Fearless skeptics with finesse. Red teamers are weird—get over They tend to be loners, mavericks, and arrogant, which is exactly why they think and act differently—th most vital skill of a red teamer. 4) Have a big bag of tricks. Red teams must not become predictable. If th use the same methods over and over, they become victims of institutional capture, and their findings becom predictable and are then ignored. Red teaming changes everyone. Even those merely exposed to the resu will rethink the issue under examination, and, more generally, think differently in their day-to-day routine 5) Be willing to hear bad news and act on it. If institutions will not learn, then red-teaming results will n matter. Institutions unwilling to absorb and integrate red team findings should not bother going through th process. 6) Red team just enough, but no more. Red teaming can be a stressful and demoralizing activity done too often, which in turn can be irreparably disruptive to an institution's strategies and plans. Howeve if red teaming is done too infrequently, the institution soon becomes hidebound and complacent.

Chapter 2 covers the most prominent recent red-teaming units and events that have been developed an

employed by the US military, concluding with a look at how red teaming has spread abroad. These includ the Red Team University initiative at Fort Leavenworth where more than 2,700 officers and governmen employees have received formal training in red team approaches and methodologies since 2005; a 20 example in which two Red Team University instructors were called upon to facilitate a moderated discussio and an analysis of an important military concept document to identify assumptions, possible failures, a alternatives; the halting and still incomplete attempts to develop and integrate formal red team units with US Marine Corps command staffs since it was made a top priority by former Marine Corps Commanda General James Amos; and the notorious summer 2002 Millennium Challenge concept-development exerci in which Pentagon leaders' hopes for a rapid transformation in how the military would fight future wa were dashed by a devious retired three-star Marine lieutenant general. This is the first evaluation Millennium Challenge based upon the military's own declassified after-action report and interviews with a of the key officials involved. This chapter will also describe the more limited uses of red teams outside of th United States, including in the Israel Defense Forces, the United Kingdom's Ministry of Defence, an NATO's Allied Command Transformation.

Chapter 3 examines how the spies and analysts of the US intelligence community (IC) have applied re teaming techniques in recent years. The featured events and units include the 1976 Team B competitiv intelligence analysis by non-IC experts of the CIA's National Intelligence Estimate of Soviet Union strateg nuclear weapons capabilities and intentions; the August 1998 absence of an independent alternative analy of the CIA's estimate that the Al Shifa pharmaceutical factory in Khartoum, Sudan, was producing VX ner gas and was tied to Osama bin Laden; the first-ever inside look at the CIA's Red Cell, which was created th day after the September 11, 2001, terrorist attacks to serve as an alternative-analysis unit semi-independe of all other mainline analytical offices; and the three 2011 red team probability estimates conducted to asse whether bin Laden was living in a compound in Abbottabad, Pakistan.

Chapter 4 looks into the activities of several US government homeland security agencies, which condu vulnerability probes and simulations of defenses and critical infrastructure to test and (ostensibly) impro security systems. Features include the tragic story of the pre-9/11 Federal Aviation Administration (FAA) re team, which found systematic failures in commercial airline security but was ignored by FAA officials Washington who did little to address the shortcomings or mandate the airline industry to do so; the mi 2000s red team simulation of the threat to New York City airports posed by terrorists armed with Ma Portable Air Defense Systems (MANPADS); another unprecedented look inside the New York Polic Department's (NYPD's) tabletop exercises, authorized and led by the NYPD commissioner, which revie and evaluate New York City's preparations for responding to catastrophic terrorism scenarios; and, finally the Information Design Assurance Red Team (IDART), a small unit based within the Sandia Nation Laboratories in Albuquerque, New Mexico, which has served as the elite US government adversarial hacki unit, breaking into software, computer networks, and defended facilities in order to improve their securi since 1996.

Chapter 5 investigates the application of red teaming in the ultimate competitive environment—t private sector. Featured is the role of outside consultants who run business war games for corporations order to simulate and evaluate the wisdom of a strategic decision; an immersion into the rapidly expandi field of "white-hat" hackers who conduct lawful and commissioned penetration tests of their client

computer networks and software programs; a successful and shocking white-hat hack that demonstrates ho a small group was able to obtain root access on a Verizon femtocell (i.e., a miniature cell-phone tower th looks like a wireless router) in order to steal all of the voice and data from any phone that unknowing associate itself with the femtocell; and, finally, a firsthand account of the relative ease with which one ca obtain unauthorized access into supposedly secure buildings, and an exploration of red team physic penetration testers who easily, and often amusingly, break into supposedly secure buildings over and over.

Chapter 6 presents some of red teaming's realistic outcomes, misimpressions, and misuses that decisio makers should be conscious of when considering the use of red teams. This includes cases highlighte previously, and additional examples of how and why it is too often underappreciated, underutilized, misapplied. The five worst practices revealed include: 1) Flawed ad hoc approaches, by which leade appoint one person to provide a dissenting view to unrealistically prevent groupthink; 2) Mistaking t findings of a red team for policy, usually placing them in the wrong context or oversubscribing to the findings; 3) Empowering red teams to direct the decision-making process; 4) Freelance red teaming that fa to consider the institution's structure, processes, and culture; and 5) Distrust of the red team practitioners b leaders and managers who are unable or unwilling to listen to their findings. This chapter will also look the tendency of government or business officials to misuse a red team's findings. It concludes with a series o recommendations for government red teams and a brief look at the future of the process.

While not yet a commonly used phrase, red teaming is a concept that people intuitively and readily gra once presented with real-world examples. By the time you finish reading this book, you will have bee exposed to both a new and largely unknown process, and a fascinating cast of characters who do it for living. In addition, leaders and managers should become unpleasantly conscious of how unaware they a about the shortcomings and vulnerabilities of the companies or organizations they run. Moreover, the should also understand why red teaming matters and how it can best be utilized to improve their institution

Just as the Vatican abolished the Devil's Advocate role in its saint-making process, leaders could choose t silence challenging voices. If nothing else, this book will convince you that such an approach is unlikely triumph in the long run. As enticing as the prospect of unruffled consensus in the workplace may be, whe leaders dissuade dissent and divergent thinking, they create an environment that may allow disasters materialize. Red teaming is the method for making it more likely that those disasters will be foreseen an thereby prevented.

ONE

BEST PRACTICES IN RED TEAMING

> When you hear "best practices," run for your lives. The *Titanic* was built with best practices. It was faithfully operated in accordance with best practices.
>
> — Retired US Army Colonel Gregory Fontenot, Director of the University of Foreign Military and Cultural Studies (Red Team University), 2011[1]

As Gregory Fontenot's above observation makes clear, the very concept of "best practices" is one that tru red teamers might find alien to their profession. By definition, red teaming exists outside of institution strategy, standard operating procedures, and structure. By nature its practitioners are contrarian thinker deeply skeptical of any outsider who would impose a rigid classification on what they do. Over the course the more than two hundred interviews conducted for this book with those who red team for a living, as side job, or as just a component of their work, some visibly winced just hearing the term "best practices and resisted the notion that their tradecraft could be distilled or summarized into a how-to manual. Indee there is no single blueprint that applies to all settings. One might conclude that the overarching best practi is to be flexible in the approaches or techniques applied. As subsequent chapters will demonstrate, there a often severe costs and consequences for institutions in competitive environments that do not employ ar best practices by disregarding a red team's findings and recommendations, as well as powerful benefits fo those that listen.

Best practices are never a one-size-fits-all set of instructions, but rather are a set of pragmatic principles guide and inform a red team and the organization that it targets—or, the "targeted institution." If the adhere to best practices, red teamers are much more likely to mitigate the cognitive and organizational bias that routinely hamper institutional performance. The alternative to relying upon such informed guidelines to arbitrarily "red team" based upon intuition and whatever information one stumbles across. There are cle perils to red teaming in such a haphazard manner. As retired US Marine colonel and current red tea instructor and facilitator Mark Monroe asks: "Would you go into surgery with somebody who had n medical training or experience?"

Research demonstrates that the following six principles—drawn from the red teamers' firsthan experiences detailed in upcoming chapters—are, in fact, the real best practices because they have bee repeatedly effective. While delving into the four fields that are assessed in the chapters to come, the reade should keep the following six principles in mind.

1. The Boss Must Buy In

Despite the widespread perception that performance is improved when hierarchy is flattened, almost a institutions still have a small team in charge, or, more likely, a singular boss at the top of an organization chart. Hierarchy and a clear chain of command can be essential to resolving collective-action problems ar

establishing responsibility and accountability for decision-making. An effective boss will instill and reinfor the ethics, values, and expected behaviors for the staffs and employees throughout an institution. And t boss's buy-in is absolutely crucial to getting things done.

Unsurprisingly, the best practice that was most often raised by red teamers and those exposed to the results was the need for a boss to be willing to endorse and support the red team and its results. Whether t boss is a military commander, a government agency official, a chief information officer, or a senior vic president, someone in charge must value red teaming, and, just as importantly, signal their support to all the employees for whom the findings are relevant. This "top cover," in military parlance, is highly critical. comes in many forms and with differing intensities, but everyone is well aware of its presence or absence. Paul Van Riper, the retired Marine lieutenant general and widely acknowledged red-teaming guru, declare "Unless the commanders themselves want it, support it, resource it, institutionalize it, and respond to it, won't matter."[2]

This buy-in must manifest itself in several ways.

First, bosses must recognize that there is a vulnerability within their organization that red teaming ca help uncover and address. Organizations tend to be poor judges of their own performance, and are oft blind to shortcomings and pitfalls. Indeed, in many instances, a readily apparent failure or disaster must ha already occurred—resulting in meaningful human, financial, or reputational costs—before a boss w willingly listen to appeals for red teaming. For example, it was not until after the bombing of Pan Am Flig 103 over Lockerbie, Scotland, in which 270 people died, that the administrator of the Federal Aviatio Administration (FAA) institutionalized a small red team to conduct realistic threat and vulnerabili assessments. (Even after these assessments, the FAA clearly disregarded what the exercises had revealed. demonstrated in chapter 4, the troubling security lapses that this red team consistently reported even we unheeded prior to the terrorist attacks of 9/11.)

Alternatively, when senior managers are about to make a consequential decision for which they will b held directly accountable, they might seek out a simulation or alternative analysis to provide cover in case failure. Ben Gilad, who has run simplified but rigorous business war games for Fortune 500 companies f more than thirty years, has learned that presidents or vice presidents actively seek him out when they a about to roll out a new product or enter a new market. Gilad notes that these bosses "might go out (be fire or up (get promoted), but they know that it is a major decision," and commissioning him to run a war gam serves as both a "pressure test" evaluation of that decision and a potential "cover your ass" warranty.[3]

The need for buy-in not only applies to the highest node on the hierarchy. Bosses need to be aware of th likelihood that when this requirement to red team is just perfunctorily imposed on a manager by a mo senior leader, the junior person will be less likely to value it, utilize it willingly, or listen to and implemen the findings. As detailed in chapter 2, beginning in 2010, Marine Corps Commandant General James Am ordered that all Marine Expeditionary Forces (MEF) and deploying Marine Expeditionary Brigades (ME incorporate a red-teaming element within their command staffs. According to military personnel an civilians who served on MEF and MEB red teams, they were often underutilized or ignored by th commanding general, or, more frequently, by their senior staffs during their initial years. The Marin commanders had not been properly instructed in how to employ their red teams, and were not made ful aware of the potential added value. In the private sector, a corporate board could similarly mandate that th

chief executive officer or senior vice president subject a company's business strategy to a simulation that conducted by an outside consultant. A senior vice president from a multinational energy corporation, wh was directed to commission such a simulation, noted that his unit decided to "sleepwalk our way through th thing," and produced a pro forma after-action report that they could simply tout as evidence to the board having done it.[4] It is clear from these examples that, for red teaming to be of the greatest value, not only th most senior leaders, but also leaders throughout the targeted institution's hierarchy, should lend the effor their support.

Second, bosses must be willing to commit the resources, personnel, and time to support either an in-hou or outside red team hired to scrutinize their institution. Red teaming is rarely an activity essential to a organization's core mission. As a result, it can face funding barriers, and all too often gets cut when its need not immediately apparent. For example, a typical penetration test of a medium-sized company's comput networks costs between $1,500 and $10,000 per day, while an elaborate business war game costs $500,00 or more. For employees who participate in or facilitate the red team, the amount of lost work hours can b substantial. This can lead senior managers to treat the red team as a "dumping ground" for margin employees, or those whom they are not sure what to do with—many Army and Marine Corps red teame have reported experiencing this phenomenon. Even when the boss recognizes the need for red teamin several acknowledged that it is "nice to have, but not a must have." When they hold this opinion and expre it publicly, it can dramatically reduce the viability of a red team's effectiveness.

Third, the boss must allow the red teamers to be completely truthful about their findings. They cannot b punished for pointing out that the strategies or processes that the boss personally developed and authorize are deeply flawed, or that the conventional wisdom among the targeted institution's employees is misleadin or riddled with inherent contradictions. If the boss punishes or conspicuously ignores people for speakin up, nobody will speak up again.

In many real-world instances, bosses have adopted a number of techniques to publicly embrace an empower their red teams, ensuring that a red team's dissenting and contradictory viewpoints will be heard They can attend the red team event to demonstrate their support, just as New York Police Departmen (NYPD) Commissioner Ray Kelly and his successor William Bratton made it a point to participate in eve single tabletop exercise, described in chapter 4, that was conducted with senior commanders during h tenure. Red teams can also be rewarded for their work—for example, the CIA Red Cell has received th National Intelligence Meritorious Unit Citation on multiple occasions—or a proficient red teamer ca conspicuously be promoted to a more senior position. Former Iraq and Afghanistan commander Gener David Petraeus found that in order to encourage dissenting viewpoints within a command, "you have t create a culture that preserves and protects the iconoclasts."[5]

Fourth, of course, it is up to the boss to decide whether the red team's findings are assimilated or ignored This judgment is based on whether the boss believes the targeted institution can live with the risks c challenges presented by the red team, or should commit the resources—in terms of money, personnel, an opportunity costs—to undertake the necessary changes. Ideally, the same boss who commissions the re team should also have the authority to authorize the implementation of its findings, or to strongl recommend that a more senior boss endorses them. Without first securing the bosses' buy-in, and havin that buy-in signaled to all relevant employees, the next five best practices will likely be ignored or irrelevant