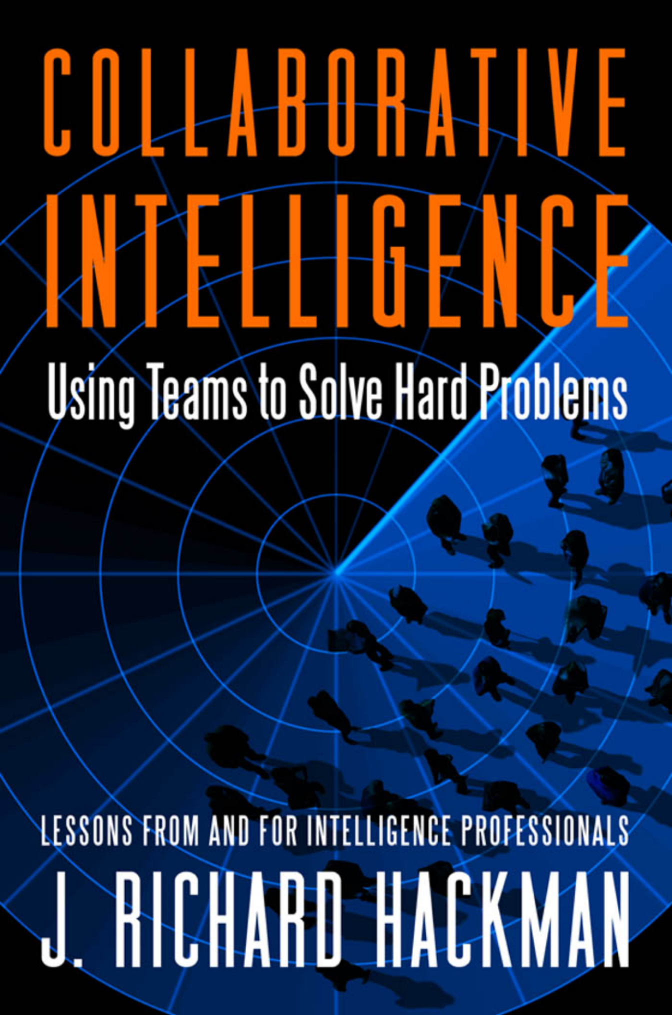

COLLABORATIVE INTELLIGENCE

Using Teams to Solve Hard Problems

LESSONS FROM AND FOR INTELLIGENCE PROFESSIONALS

J. RICHARD HACKMAN

An Excerpt From

Collaborative Intelligence: Using Teams to Solve Hard Problems

by J Richard Hackman
Published by Berrett-Koehler Publishers

COLLABORATIVE INTELLIGENCE

Using Teams to Solve Hard Problems

J. RICHARD HACKMAN

BK®

Berrett–Koehler Publishers, Inc.
San Francisco
a BK Business book

CONTENTS

INTRODUCTION

The Challenge and Potential of Teams

Intelligence professionals commonly are viewed as solo operators. Here is an analyst, alone in a cubicle at Langley, calling up images and reports on a secure computer, consulting historical materials on the cubicle shelf, thinking deeply about the implications of ambiguous but worrisome recent developments. There is an undercover officer making seemingly casual social contacts overseas to identify locals who might have access to useful information—and then inducing the most promising of them to share what they know or can find out. And down there is a clandestine service trainee, straining to acquire the knowledge and skills of the trade, worried about washing out, unsure about having what it takes for a successful career in intelligence.

Engaging images such as these are the stuff of spy novels and movies. They sometimes even are accurate. But that's not how it generally happens. Although there are indeed many heroic individuals in the intelligence community, most intelligence work actually involves extensive and intensive collaboration with others—with colleagues in the intelligence community to be sure, but also with outsiders such as people from other government agencies, academic researchers, and employees of private-sector organizations.

The analyst activates a network of contacts both inside and outside government for ideas about what those worrisome developments might portend. The clandestine officer works with a team to cultivate and exploit sources of information. Even in training—which is still more individually focused than real intelligence work—instructors are discovering the pedagogical power of team exercises in which trainees may learn as much from teammates as from their teachers. So we have across the intelligence community fusion teams, training teams, special activities teams, networked collaborations, management teams, scientific teams, and more. Moreover, as electronic technologies for communication and coordination become more powerful and pervasive, teamwork-at-a-distance is becoming more the rule than the exception. Teams are everywhere in the community, and they make a difference.

Teams have great potential for solving hard problems in challenging contexts. They obviously bring more knowledge, skill, and experience to the work than any single individual could. They provide flexibility in how members are deployed. They offer members nonstop opportunities for real-time learning. And they have at least the potential of integrating members' diverse contributions into a creative product that is just what is needed. Yet, as an extensive body of research has documented, teams also can go badly wrong, spinning their wheels and not even finishing their work or, perhaps, falling into a syndrome known as "groupthink," which results in a true fiasco. A team is akin to an audio amplifier: whatever comes in, be it Mozart or ear-grating static, comes out louder.[1]

What Helps and What Gets in the Way

The intelligence community has more than its share of unique features, some of which facilitate collaboration and teamwork, and others that get in the way. For starters, the people who work in U.S. intelligence organizations are, as a group, extraordinarily talented. In 2008, for example, the CIA received over 120,000 online job applications, and offered positions to only the very best candidates.[2] But it's not just the raw talent of intelligence analysts, operations officers, and technologists that is impressive, it is also their deep personal commitment to public service. I've been involved with the community for over a decade now, both as a researcher and in an advisory capacity, and it is not an exaggeration to say that I am in awe of the dedication of most of the intelligence professionals I have encountered. Again and again I have spoken with people who could make much more money and have much more time for personal pursuits in the private sector—but who stay where they are because of their commitment to what they are doing. They know that their work contributes directly to the security of the nation and to the well-being of their fellow citizens. Indeed, a community-wide employee climate survey published in 2007 showed that almost 90 percent of the respondents affirm the importance of their work and, moreover, their satisfaction with their coworkers.[3]

Intelligence community leaders do not have much reason to worry, therefore, about the dedication or smarts of the people who do intelligence work. Arranging things so the work can be accomplished efficiently and well, however, is another story. Virtually all organizations in the intelligence community are large bureaucracies, and one does not need a doctorate in sociology to know that bureaucratic policies and practices sometimes frustrate even the most capable and best-intentioned employees. Worse, the intelligence community is not just a large bureaucracy, it is a whole *set* of them, linked together in sometimes-hard-to-fathom ways. When you have an intelligence budget that exceeds $80 billion, more than 850,000 professionals holding top secret clearances, and a workforce that is distributed across nearly 50 government organizations and 2,000 private companies, management is, to say the least, a significant challenge.[4] So it is perhaps not surprising that only about 40 percent of the respondents to the climate survey reported that their leaders engender motivation and commitment in the workplace, or that good work is recognized and reinforced. Even fewer respondents felt that appropriate steps are taken to deal with poor performers.

Secrecy also poses significant problems in getting intelligence work done. Although absolutely essential for some intelligence activities, the need for secrecy has spawned a labyrinth of compartments and such a pervasive disposition to classify materials that it sometimes can be nearly impossible for intelligence professionals to obtain the information they need for their work. And there is the difficulty of navigating between being too responsive to what policymakers want to hear (and thereby becoming politicized) and being insufficiently responsive to their needs (and thereby becoming irrelevant).[5]

And then there is the *external* context of intelligence work. On one side are our adversaries, including non-state entities whose technological and scientific sophistication presents analytic and operational challenges beyond anything that the community has had to deal with before. On the other side, *our* side, is the U.S. political establishment, some members of which seem always to have their "intelligence failure" rubber stamp at the ready.

Perhaps most worrisome of all is the sheer volume of the work to be done. The number of potential adversaries has proliferated (one analyst told me how much he missed the "good old days" when one could focus mainly on the Soviet Union). Simultaneously, new collection technologies and methods, along with the flood of open source information now available, have increased by orders of magnitude the amount of data flowing into community organizations. Trying to keep track of it all can be overwhelming.

Searching for Solutions

There is no obviously best way to structure and manage intelligence work. The people are great and the work is important, to be sure, but the frustrations in getting the work done correctly and on time are escalating. In the years since 9/11, many commentators have had their say about how to "fix" intelligence, and every new revelation of some slip-up or oversight generates more diagnoses of what went wrong and what it would take to keep it from happening again. The prescriptions are a varied lot: Change the culture of the intelligence community. Simplify the organizational structure. Give intelligence professionals access to better information technologies. Require more sharing of information across agencies. Make social networking more accessible. Improve the recruitment and training of intelligence professionals. Institute a community-wide leadership development program. And more.

This book offers an alternative approach. Its premise is that the frontline work performed by intelligence professionals—how that work is designed, how it is staffed, and how it is led—may be a good point of departure for improvement efforts. A report on analytic pathologies from the CIA's Center for the Study of Intelligence reaches a similar conclusion: "Analytic failures stem from dysfunctional behaviors and practices *within* the individual agencies and are not likely to be remedied either by structural changes in the organization of the community as a whole or by increased authorities for centralized community managers."[6]

Moreover, since intelligence work increasingly requires coordination and collaboration among people who have a diversity of knowledge, skill, and experience, it often is necessary to create teams whose members come from a variety of intelligence disciplines and, in many cases, from different intelligence organizations. Carmen Medina, a veteran intelligence analyst and former director of the CIA's Center for the Study of Intelligence, has written that what is most needed these days to generate the insights that policymakers demand are interdisciplinary teams that cross traditional institutional boundaries.[7] Consistent with Medina's view, the response of the National Counterterrorism Center to the failed attempt to bring down an airliner on Christmas Day in 2009 was to form "pursuit teams" composed of professionals from across the intelligence and law enforcement communities to prioritize and pursue terrorism threats.

Perhaps the most compelling reason for giving close attention to intelligence teams is that it is *feasible* to improve how they operate and how well they perform. It can be extraordinarily daunting to fundamentally change either whole institutions (cultural inertia is awe inspiring) or individual persons (trying to alter how a person thinks, feels, or acts without taking account of his or her group memberships is an exercise in futility). Because teams are located right at the nexus of the individual and the organization, they are accessible to those who seek to improve how intelligence work is performed. For all these reasons, teams appear to be a good place to start to make things better.

The Challenge

The challenge is to identify what it takes for teams to exploit their considerable potential while avoiding the dysfunctions that await the unwary. Although it assuredly is true that leaders cannot *make* a team be great, we do now know what conditions they can put in place to increase the likelihood (although not to guarantee) that a team will be effective—that it will generate a first-rate product while simultaneously becoming stronger as a performing unit and fostering the learning and professional development of its individual members.

To do that, however, we must get beyond conventional thinking about how teams work. Our natural impulse is to search for the specific causes of the effects in which we are interested—to search for the "active ingredient" that makes a team effective. But there is no single cause of team performance. Instead, as this book will show, it takes a *set* of conditions, operating together, to help a team move onto a track of ever-increasing competence as a performing unit.

There are six enabling conditions, each of which has its own chapter in Part II of this book. Although these conditions are explicitly based on social science research and theory, they are presented here as imperatives for action, as concrete things that those who create, lead, or serve on teams can do to help their teams succeed.[8] The job of those who create or lead teams, then, is not to exhort members to work together well, not to personally manage members' collaborative work in real time, and certainly not to run their teams through a series of "team building" exercises intended to foster trust and harmony. The leader's job, instead, is to get the enabling conditions in place, to launch the team well, and only then to help members take the greatest possible advantage of their favorable performance circumstances. Indeed, my best estimate is that 60 percent of the variation in team effectiveness depends on the degree to which the six enabling conditions are in place, 30 percent on the quality of a team's launch, and just 10 percent on the leader's hands-on, real-time coaching (see the "60-30-10 rule" in Chapter 10).

The optimistic message of the book is that intelligence teams, for all the challenges and uncertainties they face, can perform much better than they usually do. Moreover, if community leaders find ways to improve collaboration and teamwork where the actual work is being done in their own units, there is at least the possibility that what is learned will diffuse, laterally but perhaps also upward, to improve the quality, speed, and agility of intelligence work throughout the community.

PART I · Teams in Intelligence

WHAT MAKES FOR A GREAT INTELLIGENCE TEAM? The three chapters that follow set the stage for answering that question. We will see how intelligence teams actually deal with hard problems, the different ways members can collaborate with one another, and what it means to say that an intelligence team has been "effective." The first chapter ("Teams That Work and Those That Don't") opens with an extended example of two teams—one planning a terrorist act, the other trying to head it off. Among the reasons one team succeeded and the other failed are the inherent advantages of playing offense vs. defense; team dynamics that inhibit the full use of members' resources; and the ways that stereotypes of other groups (including groups embedded within one's own team) can cripple team processes and performance.

The second chapter ("When Teams, When Not?") lays out the many different kinds of collaboration that exist within the intelligence community, ranging from communities of interest whose members never actually meet to teams whose members work together face to face over an indefinite period. We will see that teams are not always an appropriate means for accomplishing a particular piece of work, that certain kinds of tasks are better done by solo performers. And even when a team is called for, there remains the question of the *type* of team that should be created. The chapter identities five different types of teams and discusses the circumstances under which each of them is and is not appropriate.

The final chapter in this part of the book ("You Can't Make a Team Be Great") digs into what team "effectiveness" means and how it can be assessed. Although one cannot make a final judgment about a team's performance until its work is completed, three team processes can be monitored in real time to assess how a team is doing. These processes are: (1) the level of effort a team is applying to its work, (2) the appropriateness of its performance strategy for the task it is performing, and (3) the degree to which the team is using well the full complement of its members' knowledge, skill, and experience. When a team shows signs of slipping on one or more of these three process criteria, a coaching intervention may be appropriate. Or, more frequently, it turns out that the conditions under which the team is operating—how it is structured and the context within which it operates—are flawed in some way. The second part of the book is devoted to those conditions: what favorable conditions are, how they help, and what is needed to get them in place and help a team take full advantage of them.

CHAPTER 1

Teams That Work and Those That Don't

It was not all that different from his regular work. Jim, an analyst at the Defense Intelligence Agency (DIA), looked around at the other members of his team. He knew two of them—another analyst from DIA and an FBI agent he had once worked with; the rest were strangers. The team's job, the organizer had said, was to figure out what some suspected terrorists were up to—and to do it quickly and completely enough for something to be done to head it off. Okay, Jim thought, I know how to do that kind of thing. If they give us decent data, we should have no problem making sense of it.

For Ginny, it was quite a bit different from her regular work as a university-based chemist. She had been invited to be a member of a group that was going to act like terrorists for the next few days. Ginny had not known quite what that might mean, but if her day of "acculturation" into the terrorist mindset was any indication it was going to be pretty intense. She had never met any of her teammates, but she knew that all of them were specialists in some aspect of science or technology. She was eager to learn more about her team and to see what they might be able to cook up together.

Jim and Ginny were participating in a three-day run of a simulation known as Project Looking Glass (PLG). The brainchild of Fred Ambrose, a senior CIA intelligence officer, PLG simulations pit a team of intelligence and law enforcement professionals (the "blue team") against a "red team" of savvy adversaries intent on harming our country or its interests. A "white team"—a group of intelligence and content specialists—plays the role of the rest of the intelligence community. The charge to the red team was to use everything members knew or could find out to develop the best possible plan for doing the greatest possible damage to a target specified by the organizers—in this case, a medium-sized coastal city that was home to a large naval base. Members could supplement their own knowledge by consulting open sources such as the Internet and by seeking counsel from other individuals in their personal or professional networks. But what they came up with was to be entirely the product of team members' own imagination and ingenuity.

To help them adopt the perspectives of those who really are intent on doing damage to our country, red team members spent a day of acculturation. It was like an advanced seminar on terrorism, Ginny thought. Team members heard lectures from both scholars and practitioners on everything from the tenets of radical Islamic philosophy to the strategy and tactics of terrorist recruitment. By the end of the day, Ginny was surprised to find herself actually thinking and talking like a terrorist. Her red teammates seemed to be doing the same.

Ginny and her teammates were aware that the blue team would have access to a great many of their activities—they would be able to watch video captures of some of the red team's discussions, tap into some of their electronic communications and Internet searches, and actively seek other data that might help them crack whatever plot they were hatching. The blue team also had heard lectures and briefings about terrorists, including specific information on the backgrounds and areas of expertise of red team members. Jim found these briefings interesting, but mostly he was eager to get beyond all the warm-up activities and into the actual simulation. And, by the beginning of the second day, the game was afoot.

The start-up of the red and blue teams could hardly have been more different. The red team began by reviewing its purpose and then assessing its members' resources—the expertise, experience, and outside contacts that could be drawn upon in creating a devastating attack on the coastal city. Members then launched into a period of brainstorming about ways the team could use those resources to inflict the greatest damage possible and, moreover, do so in a way that would misdirect members of the blue team, who they knew would be watching them closely.

The blue team, by contrast, began by going around the room, with each member identifying his or her back-home organization and role.

Once that was done, it was not clear what to do next. Members chatted about why they had chosen to attend the simulation, discussed some interesting issues that had come up in the previous day's lectures, and had some desultory conversations about what it was that they were *supposed* to be doing. There were neither serious disagreements nor signs of a struggle for leadership, but also no discernable forward movement.

Then the first video capture of the red team at work arrived. The video made little sense. It showed the team exchanging information about each member's special expertise and experience, but nothing they said was about what they were actually planning to do. Assured that nothing specific was "up," at least not yet, blue team members relaxed a little. But it was frustrating not to have any hard data in hand that they could assess and interpret using their analytic skills and experience.

As blue team members' frustrations mounted, they turned to the white team—the broader intelligence community. To obtain data needed for their analytic work, including information about some of the activities of the red team they had seen on the video, blue team members were allowed to submit requests for information (RFIs) to the white team. Some RFIs were answered, sometimes immediately and sometimes after a delay; others were ignored. It was, Jim thought, just like being back at work.

By early in the second day of the simulation, the red team had turned the corner and gone from exploring alternatives to generating specific plans for a multipronged attack on the coastal city and its environs. Now blue team members were getting worried. They finally realized that they had no idea what the red team was up to, and they became more and more frustrated and impatient—with each other, certainly, but especially with the unhelpfulness of the white team. So the team did what intelligence analysts often do when frustrated: they sought more data, lots and lots of it. Eventually the number of RFIs became so large that a member of the white team, experiencing his own frustration, walked into the blue team conference room and told members that they were acting like "data junkies" and that they ought to slow down and figure out what they actually needed to know to make sense of the red team's behavior.

That did not help. Indeed, as accurate as the accusation may have been, it served mainly to increase blue team members' impatience. As tension escalated, both negative emotions and reliance on stereotypes also increased—stereotypes of their red team adversaries, to be sure ("How could that weird set of people possibly come up with any kind of serious threat?"), but also stereotypes of other blue team members. Law enforcement and intelligence professionals, for example, fell into a pattern of conflict that nearly incapacitated the team: When a member of one group would offer a hypothesis about what might be going on, someone from the other group would immediately find a reason to dismiss it.

Things finally got so difficult for the blue team that members could agree on only one thing—namely, that they should replace their assigned leader, who was both younger and less experienced than the other members, with someone more seasoned. They settled on a navy officer who was acceptable to both the law enforcement and the intelligence contingents, and she helped the group prepare a briefing that described the blue team's inferences about the red team's plans. The briefing would be presented the next day when everyone reconvened to hear first the blue team's analysis, and then a presentation by the red team describing what they actually intended to do.

The blue team's briefing showed that members had indeed identified some aspects of the red team's plan. But blue team members had gotten so caught up in certain specifics of that plan that they had failed to see their adversaries' elegant two-stage strategy. First there would be a feint intended to misdirect first responders' attention, followed by a technology-driven attack that would devastate the coastal city, its people, and its institutions. The blue team had completely missed what actually was coming down.

Participants were noticeably shaken as they reflected together on their three-day experience, a feeling perhaps best expressed during the debriefing by one blue team member who worked in law enforcement: "What we saw here," he said, "is almost exactly the kind of behavior that we've observed among some people we are tracking back home. It's pretty scary."

■ ■ ■

The scenario just described is typical of many PLG simulations that have been conducted in recent years. Fred Ambrose developed the idea for this unique type of simulation in response to a congressional directive to create a paradigm for predicting technology-driven terrorist threats. The simulation is an upside-down, technology-intensive version of the commonly used red team methodology, with the focus as much on detecting the red team's preparatory activities as on determining its actual attack plans. Again and again, the finding is replicated: The red team surprises and the blue team is surprised. The methodology has proven to be so powerful and so unsettling to those who participate in PLG simulations that it now is being adopted and adapted by a number of organizations throughout the U.S. defense, intelligence, and law enforcement communities.[1]

What accounts for the robust findings from the PLG simulations, what might be done to help blue teams do better, and what are the implications for those whose real jobs are to detect and counter terrorist threats? We turn to those questions next.

Why Such a Difference between Red and Blue Teams?

How are we to understand the striking differences between what happens in red and blue teams in PLG simulations? Although there is no definitive answer to this question, there are at least four viable possibilities: (1) it is inherently easier to be on the offense than on the defense, (2) red teams are better at identifying and using the special expertise of both their members and outside experts, (3) prior stereotypes compromise the ability of blue teams to take what they are observing seriously and deal with it competently, and (4) red teams develop and use more task-appropriate performance strategies.[2]

OFFENSE VS. DEFENSE. An obstacle that many intelligence teams must overcome is that they are, in effect, playing defense whereas their adversaries are playing offense. Data from PLG simulations affirm the observations of intelligence professionals that offense usually is considerably more motivating than defense. It also is much more straightforward for those on offense to develop and implement an effective way of proceeding. Even though offensive tasks can be quite challenging, they require doing just one thing well. Moreover, it usually is not that difficult to identify the capabilities needed for success. Those on defense, by contrast, have to cover all reasonable possibilities, which can be as frustrating as it is difficult.[3]

The relative advantage of offense over defense is seen not just in intelligence work but also in a wide variety of other activities. A football team on offense need merely execute well a play that has been prepared and practiced ahead of time, whereas the defenders must be ready for anything and everything. A military unit on offense knows its objective and has an explicit strategy for achieving it, whereas defenders cannot be certain when the attack will come, where it will occur, or what it will involve. As physicist Steven Weinberg has pointed out, it is impossible to develop an effective defense against nuclear missiles precisely because the defenders cannot prepare for everything that the attackers might do, such as deploying multiple decoys that appear to be warheads.[4]

Because athletic coaches and military strategists are intimately familiar with the difference between offensive and defensive dynamics, they have developed explicit strategies for dealing with the inherent difficulties of being on the defensive. The essential feature of these strategies is converting the defensive task into an opportunity to take the offense. According to a former West Point instructor, cadets are taught to think of defense as a "strategic pause," a temporary state of affairs that sometimes is necessary before resuming offensive operations. And a college football coach explained that a good defense is one that makes your opponents "play with their left hand." A "prevent" defense, he argued, rarely is a good idea, even when you are well ahead in the game; instead, you always should prefer an "attack" defense. These sentiments were echoed by a military officer: "Good defense is arranging your forces so your adversaries have to come at you in the one place where they least want to."

In the world of intelligence, there is an enormous difference between "How can we cover all the possibilities?" and "How can we reframe our task so that they, rather than we, are more on the defensive?" For all its motivational and strategic advantages, however, such a reframing ultimately would require far better coordination among collection, analytic, and operational staff than one typically sees in the intelligence community. Even with the creation of a single Director of National Intelligence, organizational realities are such that this level of integration may not develop for some time. In the interim, simulations such as PLG offer at least the possibility of helping those whose work involves defending against threats understand more deeply how adversaries think and act. Our observational data, for example, show that analysts who participate in PLG simulations do develop a capability to "think red" that subsequently serves them well in developing strategies that focus on the specific data most likely to reveal what their adversaries are up to.

IDENTIFYING AND USING EXPERTISE. To perform well, any team must include members who have the knowledge and skill that the task requires; it must recognize which members have which capabilities; and it must properly weight members' inputs—avoiding the trap of being more influenced by those who have high status or who are highly vocal than by those who actually know what they are talking about. Research has documented that these simple conditions are harder to achieve than one might suspect.[5] People commonly are assigned to teams based on their organizational roles rather than on what they know or know how to do. Moreover, teams often overlook expertise or information uniquely held by individual members, focusing instead on that which all members have in common.[6] Only rarely do teams spontaneously assess which members know what and then use that information in deciding whose ideas to rely on most heavily.

The challenge of identifying the expertise of team members and using it well is especially critical for those who would mount a terrorist attack since, as Fred Ambrose has pointed out in conversation, "It's not what they have in their pockets that counts most, it's what they have in their heads." The red teams in PLG simulations generally do a great job at using what is in members' heads. The teams are properly composed, to be sure: they consist of individuals who have in abundance the scientific, technical, and engineering skills needed to mount an attack in the setting specified in the simulation scenario. Almost all red teams also take the time to compare credentials early on so that everyone knows who has special expertise in what technical areas, which helps teams mold the details of their plans to exploit members' unique capabilities. And because red teams have both a clear offensive purpose and detailed knowledge of members' capabilities, they generally rely on the right members to address problems that come up as they formulate their plans. Finally, when red teams need knowledge or expertise that their members do *not* have, they are quick to turn to online sources or to their networks of colleagues to fill the gaps.

Blue teams in PLG simulations also are well composed. They consist of competent professionals from law enforcement, intelligence, and the military who make their livings finding, studying, and heading off individuals and groups who would do harm to the nation. (Red team members, by contrast, generally come from academia, industry, or the national laboratories and are not professionally involved in counterterrorism work.) Blue teams also exchange credentials shortly after they assemble, but these credentials are of a wholly different kind. Typically, blue team start-up involves each member identifying his or her home organization and role in that organization. Perhaps because the team's assigned task—to figure out what the red team is up to—is both defensive and a bit ambiguous, members do not know specifically what capabilities will turn out to be most relevant to the work. So they focus less on what members know how to do and more on the organizations where they work, which increases the salience of both their home organizations' institutional objectives and the methods they rely on to achieve them. Whereas early interactions in red teams pull people together in pursuit of a specific and challenging team purpose, early interactions in blue teams underscore the differences among members and tend to pull them apart.

OVERCOMING STEREOTYPES. The paradox about differences among people is this: To perform well, a team must have them—but, as has been seen in more than a few blue teams, differences also can do you in. They do you in when members cannot break through the stereotypes they arrive with to focus on the actual realities the team faces. Among the stereotypes that compromise counterterrorism activities are those about our adversaries. "What knuckle-draggers," one analyst declaimed after looking over information about a suspect group in a metropolitan area. "What could they possibly try that we couldn't catch and snuff out in a minute?" That person's stereotype so strongly denigrated the adversaries' considerable scientific and engineering capabilities that it surely lessened the likelihood of noticing, let alone properly interpreting, data that would point to the kind of technically sophisticated attacks commonly mounted by red teams—and that also are seen outside the simulation laboratory. Numerous commentators have noted terrorists' rapidly increasing exploitation of web-based technologies in planning and executing their activities.[7]

The power of stereotypes, not just of adversaries but also of colleagues, is unsettling. One hears a CIA analyst, for example, muttering that the only things a teammate from the FBI knows or cares about are his badge and gun. Or, from the FBI side: "Just what we need, another *summa cum laude* from Princeton who wouldn't know the chain of custody if he tripped over it." Now cross those institutional stereotypes with members' identity groups, such as race or gender, and team dynamics can turn irredeemably sour. In one simulation, a blue team was monitoring the computer activities of red team members. "Look at that," a male member from law enforcement said dismissively, "all they're doing is passing dirty pictures back and forth." Amusing, that was, but obviously not something the blue team needed to track. Then a female member who held a doctorate in computer science and worked at a research laboratory spoke up: "I think I may know what's actually going on here." What was going on, of course, was an exercise in steganography, in which messages were encoded within large image files, invisible to the naked eye. But the computer scientist was from the wrong discipline, she worked for the wrong organization, and she was the wrong gender. The response from her colleague: "Honey, just let us handle this. If we need your help, we'll ask for it."

I'm not making this up. Stereotypes, whether explicitly stated or kept to oneself, really can be that powerful in compromising the utilization of team member resources.[8] It has sometimes been suggested that conflict among team members about task-related matters is valuable because it stimulates creativity. Whether or not that is true (and recent research is less encouraging than earlier studies) there is no question that interpersonal conflicts spawn negative emotions within the group and can engender task conflicts that otherwise might not have developed.[9] So there is real reason to be concerned about conflict-riddled groups, especially when those conflicts stem from intergroup stereotypes.

The good news is that social science has identified what it takes to get beyond intergroup stereotypes. High on the list is the degree to which team members work together *interdependently* for some period of time on a task that members all care about.[10] That is what red teams do, and it is one reason why red team members from different disciplines and institutions are valued for the special resources they bring to the team rather than denigrated because they are different. For blue teams, stereotypes—internal to the team as well as external—turn out to be yet another hurdle that can be hard to surmount.

DEVELOPING AND DEPLOYING PERFORMANCE STRATEGIES. The development of a task- and situation-appropriate performance strategy for a team is something of a creative act. A member can suggest, "How about if we do it this way?" and then solicit teammates' reactions to the idea. Or the team might just fall into a particular way of operating without explicitly talking about it, only later stepping back to reflect on how well that approach has been working and how it should be modified. In either case, the basic process of developing a performance strategy is first to *generate* an alternative, then to *test* its likely efficacy in moving the team toward its objective, and then to *revise* it, continuing that cycle until the team settles upon something that works. Red teams in PLG simulations had what they needed to develop a good strategy: they were playing offense, their objective was clear and challenging, and team members knew their stuff. So when an idea came up about how to proceed, members could simply ask themselves, "Will that move us forward?" And because team members collectively were so knowledgeable and experienced, the chances of a wacky or horribly time-wasting idea being adopted were reasonably low.

Blue team members did not have it so good. Because their outcome was less clearly defined, it was harder for members to use the generate-test-revise model for coming up with alternative ways of proceeding. And because members came from different organizations, each of which had its own preferred collection and analytic methodologies, it was hard for them to reach agreement about any one way of moving forward. For a number of blue teams this created an internal microcosm of interorganizational rivalries and resulted in a lowest-common-denominator approach to information gathering—that is, scooping up all the data members could get about everything that conceivably could be relevant and hoping that an informative signal eventually would emerge from all the noise.

In most cases, this non-strategy did not work. Blue team members found themselves overwhelmed by a too-large pile of undifferentiated information. Worse, the response to that problem often was to seek even more information—or, in some cases, to ask for "hints" from the white team playing the role of the intelligence community. And, as things got increasingly difficult, members tended to rely even more on the already well-known and well-practiced strategies of their home organizations, which risked further escalating the frustration and conflict that now pervaded their teams.

The irony is that there *are* strategies that can help in trimming and focusing very large quantities of information, although teams in the PLG simulations almost never used them. These strategies, discussed in detail in Chapter 7, involve either reframing the analytic task from a defensive to an offensive activity, or engaging in what is known as "constrained brainstorming." In reframing, a blue team might shift its perspective from "How can we determine exactly what the red team is planning?" to something like "What would *we* do if we had their configuration of capabilities and resources?" Just that simple cognitive change can re-orient members toward the specific information that has the greatest potential analytic payoff. To use constrained brainstorming, the blue team might first examine the biographies and relationship networks of the adversaries. Those data would enable the team to focus mainly on the few possibilities that are most likely, given their adversaries' expertise and available resources. By radically shrinking the number of avenues the team needed to consider—perhaps down to only one or two—the team could proceed with its information-gathering much more efficiently and intelligently.

These examples are nothing more than that—examples. The point is that blue teams in PLG simulations, for all the reasons already discussed, found themselves in a reactive stance vis-à-vis their adversaries. In the absence of a shared performance strategy, they tended to rely on procedures imported from their home organizations in hopes of making sense later of all the data they were scooping up. There is a better way. As will be seen in subsequent chapters, an up-front investment in developing a performance strategy that takes explicit account of a team's task requirements, its performance context, and the outcomes it is charged with achieving can generate substantial dividends later.

Conclusion: Beyond Biases

Research has extensively documented the many cognitive biases and social dysfunctions that can compromise individual and group decision making.[11] Now researchers are supplementing that knowledge by exploring positive strategies for improving analytic processes.[12] But the lessons learned from PLG simulations suggest that merely facilitating group processes or introducing structured analytic methods may not be enough to help intelligence teams perform optimally. The reason is that the differences between the red and blue PLG teams are *foundational:* they have to do with basic features of the teams, their tasks, and their work contexts. If teamwork problems stem from basic flaws in the way a team is set up and supported, then improvements will require attention to those foundational features, not just to how members relate to one another or how they go about their work.

Team process problems, such as those encountered by blue teams in the PLG simulations, are therefore better viewed as *signs* of difficulties that actually may be rooted in a flawed structure or context. In such cases, the problems are unlikely to be resolved by even highly competent process facilitation. Indeed, process-focused interventions may introduce complexities that make an already unsatisfactory performance situation even more frustrating.[13] By contrast, teams that are properly structured and supported, as the red teams generally were in the PLG simulations, can indeed be helped by competent process consultation.

These issues are especially germane for counterterrorism teams because these days teams on the offense and those on the defense are no longer "matched" as they traditionally have been. Historically, it has been our spies vs. their spies, our fighter pilots vs. their pilots, our infantry squads vs. theirs. But now, it is our cat vs. their llama. There is no match, and that suggests that we may have to be more ingenious than ever before about structuring and supporting teams that will face off against adversaries whose operating model is wholly different from our own.

The question that will occupy us throughout the rest of this book, therefore, is how to help intelligence teams of all different kinds, not just counterterrorism analytic teams, perform as well as most of the red teams did in the PLG simulations. Perhaps it never will be possible to put teams whose mission is to defend on as solid a footing as those who are mounting an attack. But, as we will see, it is at least possible to get the defenders fully into the game.