Chapter Five

A COEVOLUTIONARY PERSPECTIVE OF DECEPTION AND COUNTERDECEPTION

> The complex adaptations and counteradaptations we see between predators and their prey are testament to their long coexistence and reflect the result of an arms race over evolutionary time. (Krebs and Davies, 1993)

DECEPTION AS ADAPTATION

> CCD [camouflage, concealment, and deception] is less costly than comparable *survivability* alternatives. While CCD and hardening yielded equivalent levels of survivability when attacked by the same system, CCD was always less costly and more quickly employed. (Joint CCD Program FY95 annual report)

In the course of this research, the authors have seen an interesting motif often repeated in descriptions of OPFOR, insurgents, guerrilla fighters, terrorist groups, overmatched conventional combatants, and the like. That theme is one of *adaptation*: of evolving tactics, technologies, targets, group dynamics, and other behaviors. The list of actors that have been characterized in this fashion—that is, by an invocation of biological principles—includes groups spanning the globe, from Northern Ireland, to the Balkans, to the Caucasus, to Kashmir and Sri Lanka, throughout Latin America, across the Pacific Rim, and, not incidentally, within the United States itself (Bell, 1991, 1997; Daalder and O'Hanlon, 2000; Pavkovic, 2000; Lieven, 1998; Gall and De Waal, 1998; Singh, 1999; Schofield, 2000; McCormick, 1990, 1992; Schultz, 1999).

There are numerous ways in which predators and prey adapt, as illustrated by Table 5, where it is easy to see the analogy between the biological and military domains. Though not exhaustive, the table illustrates what should be a familiar pattern to any student of conflict: the cycle of measure and countermeasure development between combatants. This same pattern is visible in numerous cases of human conflict, where descriptors such as "evolutionary," "adaptive," and similar terms were used to characterize the course of a combatant's development.

Note the frequency with which deception (crypsis, mimicry, "startles") appears. Since all entities seek accuracy in their perceptions, and accurate perceptions rely heavily upon the performance of an individual's sensors, improvements to sensors or sensory processing are significant contributors to survival; this is as true for human combatants as it is for any animal in any environment. It should not be surprising, therefore, that the reverse holds true: capabilities that engender *inaccuracy* in the perceptions of the foe (be they attacker or defender) tend to be highly advantageous. As discussed earlier, this capability is defined as *deception*, and the advantage it provides stems from the erroneous action that so often follows from inaccurate perception. As one component of this research, the authors have explored *how* deception capabilities evolve. Doing so supports both of our primary goals: developing better deception TTPs for

Table 5

Co-evolution of Adaptation and Counteradaptation

Activity	Adaptation	Counteradaptation
Searching	Improved visual acuity Search image Search limited area where prey abundant	Crypsis Polymorphism Space out (disperse)
Recognition	Learning	Mimicry
Catching	Crypsis Lures, traps Motor skills (speed, agility) Weapons of offense	Improved visual acuity Reconnaissance, learning Escape flights, "startle" response Weapons of defense
Handling	Subduing skills Toxins	Active defense, spines, tough integument Detoxification ability

NOTE: Drawn from Krebs and Davies (1993).

friendly forces, and prescribing better methods of preventing or countering adversary deceptions. (Note that while the focus of this work remains the role of deception in urban operations, the authors feel strongly that gains made in this area can be exported to other domains of conflict.) So, then, how do adaptations that attack an opponent's perceptual apparatus—that is, deceptions—arise? By this "how" we mean under what circumstances, requiring which resources, and regarding all the other particulars of adaptation.

It seems fair to state that different groups of combatants evolve differently over time. Some adapt to changing circumstances quite quickly; others adapt slowly. Some explicitly spend time investigating new technologies and TTPs; others stick to time-honored or traditional methods that they know best. Some institutionalize the learning process; others rely on on-the-job experience. The authors believe that a profile—which we might call the *adaptive index*—may be used to portray any battlefield element in terms of its *capability, likelihood,* and *swiftness to adapt.* Table 6 contains two very simple illustrations of the principle.

Table 6

Simple Illustrations of the Adaptive Index

Quality Under Scrutiny	Low Adaptive Index	High Adaptive Index
Connectivity; ability for ideas or information to spread through population	*Cellularized insurgent force*: fighters who don't know each other and seldom communicate. A lesson learned or technological advance by one progresses through the population very slowly.	*Intranetted insurgent force*: fighters with superb internal communications. A lesson learned or technological advance by one rapidly spreads through the community.
Propensity for innovation in methods	*Traditionalist insurgent force*: combatants who, whether by ideology or lack of resources, stick to well-established TTPs. Diversity of TTPs looks normally distributed. Innovation arises through natural selection (i.e., whoever survives adversary actions passes along their version of TTP).	*Experimentalist insurgent force*: combatants consider R&D and diversity of TTPs a priority. Diversity of those TTPs has a much flatter and broader distribution (percent of population killed by adversary actions is smaller, and variations in TTPs are greater).

Table 7

Components of the Descriptor Adaptive Index as Applied to a Subject Group

Diversity	How much baseline heterogeneity exists in the group?
Innovation	How much baseline innovation is occurring?
Forces at work	Is innovation self-directed (i.e., R&D) or other-directed (i.e., natural selection)?
Intensity of forces	How intense are the selective pressures?
Turnover	What is the baseline speed of innovation?
Learning	How well do members of the group learn?
Organization	Does the organization of the group enhance or hinder innovation?
Leadership	Does the leadership embrace innovation or discourage it?
Scope of effort	What is the overall volume of group activity?
Supply	How abundant are needed resources?
Transmission speed	How fast can information travel between members of the group?
Transmission error rate	How much information loss occurs in transmission?

While the descriptions in the table are oversimplified, they should make the point nonetheless: as one side is wargaming the possibilities for adversary courses of action (COA), they ought to take a long, explicit look at the inherent adaptability of any battlefield element as well as the potential for the environment to support adaptation. Consider just one of many critical elements in operations: *time*. If time is long (e.g., in an ongoing peacekeeping operation or drawn-out occupation), an adversary with a high adaptive index is very likely to demonstrate new technical capabilities, new tactics, new target sets, and the like. This is certainly a concern for friendly force commanders. On the other hand, if time is short (e.g., a noncombatant evacuation operation (NEO)), then adversary evolution is likely to be less of a concern.

What intelligence is required to construct an adaptive index? The authors hypothesize that the measure would comprise both endogenous and exogenous factors, a partial list of which may be found in Table 7. (Note that adaptive index as defined here is a *qualitative* descriptor meant to provoke decisionmakers' careful consideration.)

Clearly, answers to the questions in the table are intelligence products; they are the refined outcomes of thorough and competent intelligence analysis. "Adaptive index" would be a term useful to military decisionmakers (at any operational level) in much the same way that the term "fitness" is useful in biology to describe a population and make predictions about likely survivability outcomes given particular perturbations to the equilibrium. That is, a battlefield element's adaptive index could be used in conjunction with other descriptors (e.g., order of battle, cultural intelligence, likely courses of action) in wargaming as a measure of how much any element is likely to advantageously change over time.

COUNTERDECEPTION AS COUNTERADAPTATION

> Hezbollah, the Shiite Muslim guerrilla organization that forced Israel from the slice of southern Lebanon it had occupied for 22 years, grew from a small band of amateurish gunmen to a highly sophisticated tactical operation . . . From once relying on teenage suicide bombers to crash cars into Israeli installations in the mid-1980s, Hezbollah tactics—primarily ambushes, assassinations and roadside bombs—became increasingly well planned and executed, military observers in the region say . . . "When they first started, they thought they could do it with a bunch of people on a hill yelling 'Allah-u akbar,'" a United Nations official in the area said of the Hezbollah fighters, "They would lose 40 in an operation. Now they are very sophisticated, very disciplined" . . . In an interview, [the top Hezbollah commander in southern Lebanon] Sheik [Nabil] Qaouk said that the guerrillas had been able to improve their effectiveness by studying each operation, learning from their mistakes and developing new uses for their weaponry. (*The New York Times,* July 19, 2000)

> Anyone dumb enough to get killed by a HARM [high-speed anti-radiation missile] is dead already. Everyone left standing is going to innovate with their [integrated air defenses]. (Joint Suppression of Enemy Air Defenses (JSEAD) staff member, discussion with author, May 9, 2000)

As described above, a historically significant form of adaptation is deception, and the authors believe that recognizing this leads to a fruitful area of counterdeception: preventing adversaries from mounting sophisticated deceptions through a systematic program of counteradaptation.

In a word: *friendly actions should be planned with adversary adaptability in mind.* Why? It is wise to engage adversaries with high adaptive indices in such a way to reduce their ability to change. To reuse an earlier example: if preventing the adversary's adaptation is considered a priority, then he should be deined the luxury of time. How is this to be accomplished? Speed: mobility, agility, and quickness should be among the key components of the friendly operation (if feasible). Those components of friendly operations that impede or altogether thwart adversaries from making advantageous adjustments may be called "counteradaptive." Reflecting upon natural selection and adaptation as it occurs in nature, the authors believe that a list of "counteradaptive" measures (including speed) would resemble Table 8 .

Note that this list represents a set of hypotheses to be tested, and it may well turn out that some elements are more or less effective than others in a counteradaptation role. For example, deceiving the enemy as to the success of their methods might delay innovation more than simply shutting down their telecommunications network would do. It is also conceivable that even *effective* counteradaptation measures only contribute a small amount to the variance of this complex phenomenon. For example, an adversarial nation-state may actively pursue R&D irrespective of day-to-day battlefield developments; or a rigidly traditional nonstate actor might eschew innovation for religious reasons.

The authors believe that a model for "thinking counteradaptively" is to be found in Allied management of ULTRA: extreme steps were taken to ensure that Allied decisionmaking did not seem to be a result of code-breaking, and therefore the Germans were not encouraged to alter Enigma (Montagu, 1978). The Special Operations Executive understood that penetration of German codes was an immensely valuable, but precarious, advantage. While the stakes may not be quite so high in contemporary deployments, the model is nevertheless quite instructive. Counteradaptation is a means of

Table 8

Operational Measures That May Counter or Minimize Adversary Adaptation

Element	Counteradaptive Effect
Overwhelming speed	Without enough time to react, it is very difficult to generate, test, evaluate, and field countermeasures. Example: Kuwait City, 1991.
Complete destruction of enemy	A 100% enemy kill leaves no survivors to transmit information about friendly techniques, countermeasures, etc.
Degradation/destruction of communications infrastructure	If information cannot be transmitted effectively, it is exceedingly difficult for new countermeasures to spread across a population.
OPSEC and deception to protect methods	Often the adversary must gather intelligence about friendly capabilities. The less they know (or the less correct their assessments), the more difficult their job of innovating.
Multiple modes of action	This is essentially an attempt at making the burden of innovation too heavy to bear. If friendly measures are diverse, it forces adversary countermeasures to be similarly diverse—an expense in effort, time, and resources. Moreover, the more complex and varied the countermeasures must be, the more likely it is that some portion of them will be ineffective.
Interdiction of R&D resources	As resources (food, money, sanctuary, personnel, laboratories, etc.) become scarcer, it is increasingly difficult to innovate. This will vary greatly by the type of countermeasure in question; new means of jamming global positioning system (GPS) or spoofing identification friend or foe (IFF) transponders will require more infrastructural resources than new means of using terrain shadows to thwart the joint surveillance, targeting and reconnaissance system (JSTARS).
Deception introduced into enemy adaptation process	Covert/clandestine or other actions taken to introduce errors into the innovation process may significantly hamper adaptation. The possibilities are numerous: disinformation may be placed in the adversary's hands that purports to reveal a GPS vulnerability, or an adversary's tank that is *poorly* camouflaged may be allowed to go unmolested in order to allow replication of the poor procedures by other tanks (and incidentally, in order to discourage innovation).

Table 8—continued

Purposeful unpredictability or built-in randomization	If adversaries have some uncertainty about the friendly force's rules of engagement (ROE), operating parameters, or munition probability-of-kill (P_k), then they are likely to expend more effort in their innovation process and end up with errors in their assessments (and thus fielded countermeasures). The question of how much randomness *(r)* needs to be injected in order to generate a specified amount of uncertainty *(u)* is an interesting issue.
Judicious timing and application of methods (see Axelrod, 1979)	In order to experiment broadly, generate heterogeneity, and evaluate results, there usually needs to be a significant volume of activity. If an asset is tightly husbanded and therefore exposure to the adversary is small, then the information gained about the technique may be too little or too late for useful adaptation.

wedging open the adversary's window of vulnerability. Consider, for example, if U.S. forces deployed in an urban peacekeeping venture fielded powerful, portable chemical detectors that tremendously improved bomb-sniffing capabilities. An adaptive enemy would soon find ways of either jamming the devices, spoofing them, or overloading them, or they would simply resort to new bomb-placement strategies, requiring new innovations by friendly forces, and so forth. The commander ordering the deployment of such devices in the first place would be well advised to consider adversary adaptability upon deployment. What is the time frame of the operation? What resources are available to the adversary? How good is adversary intelligence gathering with respect to friendly capabilities? How fast does news spread in-theater? How is the adversary's organization structured? Do they have a history of innovation? Have we penetrated their communications? These and other questions could provide intelligence of significant prescriptive value. Perhaps every bomb discovery should be loudly attributed to means other than this new chemical sensor. Alternately, friendly forces could conveniently "misplace" a false sensor to be discovered and reverse-engineered by the adversary. A third counteradaptive strategy might be to husband the sensor and then employ it aggressively, widely, and in an acute time frame, perhaps even coupled with martial law or other drastic measures (the goal of this third strategy would be to virtually eliminate adversary adaptation over a short interval, as opposed to the previous two strategies, the goal of which would be to suppress adversary adaptation over a longer period).