Chapter 13

PARADIGM SHIFTS IN SECURITY STRATEGY

Why Does It Take Disasters to Trigger Change?

DOMINIC D. P. JOHNSON AND ELIZABETH M. P. MADIN

If men could learn from history, what lessons it might teach us! But passion and party blind our eyes, and the light which experience gives is a lantern on the stern, which shines only on the waves behind us.
SAMUEL COLERIDGE

Prior to 9/11, U.S. counterterrorism policy and intelligence suffered from numerous problems. The striking feature about this is not the flaws themselves, but rather that these flaws were long appreciated and nothing was done to correct them. It took a massive disaster—3000 American deaths—to cough up the cash and motivation to address what was already by that time a longstanding threat of a major terrorist attack on the U.S. homeland.

A second striking feature is that this failure to adapt is no novelty. Pearl Harbor, the Cuban Missile Crisis, and the Vietnam War were also belated wake up calls to adapt to what in each period had become major new challenges for the United States.

Just as the military is accused of "fighting the last war," nations fail to adapt to novel security threats. The status quo persists until a significant number of lives or dollars are lost. Only at these times can we be sure that nations, institutions, and elected representatives will fully adapt to novel security threats. If we understand why this is so, we will be better able to avoid further disasters in the future.

We suggest that it takes disasters to trigger change because (1) dangers that remain hypothetical fail to trigger appropriate sensory responses, (2) psychological biases serve to maintain the status quo, (3) dominant leaders entrench their own idiosyncratic policy preferences, (4) organizational behavior and bureaucratic processes resist change, and (5) electoral politics offers little incentive for expensive and disruptive preparation for unlikely and often invisible threats.

The Curse of the Status Quo

Even a highly adaptable state might be able to prevent only 99 out of 100 disasters from happening. Such successes rarely make the news. By contrast, the 1% of disasters that do occur will be dramatic and visible and may therefore attract undue attention. Even so, the argument of this chapter is that human nature, and the nature of the institutions that humans create, exhibits a number of self-defeating phenomena that impede efficient adaptation to novel security threats, increasing the probability of periodic disasters. Indeed, under certain unfavorable conditions, we may be pathologically and institutionally unable to avoid disasters. This curse is sustained by a number of biases rooted in biology, psychology, advocacy, organizational behavior, and politics, all of which converge to preserve the status quo.

The same phenomenon is evident in everyday life. Accident-prone highways, dangerous machinery, or hazardous flight paths are often not altered until after significant numbers of people are killed or injured, or significant financial losses are incurred. In one sense this is logical: since disasters are hard to predict, only cumulative data exposes whether the costs of occasional disasters outweigh the costs of change (Perrow 1999). However, this logic is often flawed or inapplicable for two reasons. First, the costs of disasters, if they are measured in human lives, may be unacceptable. We cannot simply wait to see if or how often they happen. Second, the costs of disasters, however they are measured, are often known beforehand to outweigh the costs of not acting, yet still nothing is done to prevent them.

This phenomenon has parallels in other disciplines, including the history of science, epistemology, policy analysis, and economics, suggesting that it is a common denominator of human nature and human institutions, not something specific to a particular issue, culture, or context. For example, Thomas Kuhn described how scientific progress is characterized by lengthy periods of relative stasis where established models reign supreme, but that this status quo is punctuated by "paradigm shifts" that follow from exceptional findings such as those by Gallileo or Einstein (Kuhn 1970). Similarly, Michael Foucault argued that history itself does not proceed smoothly as a steady, linear continuum but is defined, rather, by moments of rupture that overturn prevailing systems of knowledge (Foucault 1970, 1977). Another example is the "punctuated equilibrium" theory in policy analysis, which describes how U.S. domestic policy follows periods of relative stasis during which decision processes and bureaucracies act to preserve a status quo, but this is punctuated by major periods of reform following the adoption of innovations, attention-riveting external events that grab government or public attention, and windows of opportunity when conducive factors coincide or when advocacy groups rise to prominence (Baumgartner and Jones 1993, 2002; Busenberg 2003). Finally, economics is famous for its quip that the field progresses only with each funeral.

Individuals corroborate, advertise, and propagate their favored theories as they grow older and more powerful. Only when they are gone can fresh alternatives take solid root. The same is true of other disciplines and organizations.

In many aspects of human endeavor, it appears that we fail to adapt to changing circumstances until there is a major event that wrenches us from established paradigms. We argue that this failure to adapt is, if anything, more likely in the domain of international politics than other domains because the ambiguity inherent in judgments of other cultures, ideologies, and motives allows false interpretations to prosper and persist at especially high levels (Johnson and Tierney 2006). We are, simply put, doomed to periodic foreign policy disasters.

The good news is that research in biology, psychology, organizational behavior, and political science reveal systematic causes of this phenomenon, offering the opportunity to predict when and where it will occur, and ways to correct it in the future. Policy makers may therein find ways to improve national security as well as maximize public and congressional support. Before expanding on the biases at work, we outline a series of events that illustrate the failure to adapt to novel security threats: the 1941 attack on Pearl Harbor, the 1962 Cuban Missile Crisis, the Vietnam War, and the terrorist attacks of 9/11.

Examples of Disasters Triggering Change

The Japanese attack on Pearl Harbor in December 1941 is widely regarded as a colossal U.S. intelligence failure spanning the lowest to the highest levels of command (Iriye 1999; Kahn 1999). The striking thing is not that U.S. intelligence and strategic posture were inadequate, it is that they were known to be inadequate and yet failed to be changed. Although U.S. intelligence had no specific information or dates regarding the raid on Pearl Harbor, Japanese diplomatic codes had been broken, and a number of sources pointed to the likelihood of some kind of Japanese attack on the United States. It was the failure of the U.S. government to recognize the changing motives and intentions of the Japanese decision makers that led to a poor level of readiness in the U.S. Pacific Fleet. These inadequacies reflect a status quo bias in U.S. strategy toward Japan in the prewar period, summed up by historian of intelligence David Kahn (1999, 166):

> American officials did not think Japan would attack their country. To start war with so superior a power would be to commit national hara-kiri [suicide]. To Western modes of thought, it made no sense. This rationalism was paralleled by a racism that led Americans to underrate Japanese abilities and will. Such views were held not only by common bigots but by opinion-makers as well. These preconceptions blocked out of American minds the possibility that Japan would attack an American possession. . . . An attack on Pearl Harbor was seen as all but excluded. Though senior army and navy officers knew that

> Japan had often started wars with surprise attacks, and though the naval air defense plan for Hawaii warned of a dawn assault, officials also knew that the base was the nation's best defended and that the fleet had been stationed that far west not to attract, but to deter, Japan.

Having committed errors of planning and intelligence that heightened both the probability and severity of the Pearl Harbor attack, the shock and moral outrage following the "day of infamy" led to major changes in U.S. security strategy. The entire foundations of U.S. intelligence were uprooted. The National Security Act of 1947 established the Department of Defense, the National Security Council, and the Central Intelligence Agency, in large part to ensure the integration of military and diplomatic intelligence so that such a disaster could never befall the country again. The Pearl Harbor disaster was exacerbated by the status quo bias in U.S. policy, but the shock of the attack itself caused a paradigm shift in U.S. security strategy.

The Cuban Missile Crisis of 1962 also represented a massive failure of U.S. intelligence (Allison and Zelikow 1999). When Soviet SS-4 and SS-5 missile sites were discovered on the island in October 1962, it sparked a major diplomatic crisis and military standoff in which the superpowers came perilously close to war. "American leaders," wrote Robert Jervis, "were taken by surprise in October 1962 because they thought it was clear to the Soviet Union that placing missiles in Cuba would not be tolerated" (Jervis 1983, 28). The U.S. deterrence strategy, in other words, had failed. War was in the end averted through a negotiated agreement, but the popular memory of U.S. victory masks the significant concessions that the United States also made, and the brinkmanship that could so easily have resulted in war (Johnson and Tierney 2004). Khrushchev is widely regarded, by Soviet as well as western contemporaries and historians, as having taken an enormous risk in deploying missiles on Cuba (Lebow 1981; Fursenko and Naftali 1997). In the face of such extreme risk taking, U.S. deterrence was based on faulty premises. The crisis sparked significant changes in U.S. policy, including opening direct lines of communication between the White House and the Kremlin, and a major restructuring of chain of command authority in the U.S. military (including the President's control over nuclear weapons). The Cuban Missile Crisis was exacerbated by the status quo bias in U.S. policy, but the shock of the crisis itself caused a paradigm shift in U.S. Cold War security strategy.

The Vietnam War also represented a failure of U.S. policy and intelligence. Policy suffered from the Cold War obsession with halting the spread of communism and failed to address the root cause of the insurgency as a war of national liberation (Gilbert 2002). Military strategy suffered because it sought to replicate traditional tactics of open combat. Intelligence suffered because it focused on conventional war metrics, such as body counts

and weapons captured, and only belatedly shifted to address the key elements of nationalist sentiment and counterinsurgency (Gartner 1997). The realities of guerilla war were widely understood after the experience of the British in Malaya (1948–1960) and the French in Vietnam (1946–1954), but this had little impact on U.S. policy. The U.S. leaders believed that the gradual escalation of American military power combined with coercive diplomacy, which seemed to have worked well in the past, would work just as well in Vietnam. President Lyndon B. Johnson's press secretary, Bill Moyers, said after resigning in 1967 that in Johnson's inner circle "there was a confidence, it was never bragged about, it was just there—a residue, perhaps of the confrontation over the missiles in Cuba—that when the chips were really down, the other people would fold" (Janis 1972, 120). It came as a major shock for the United States to lose a war for the first time in its history. Following the withdrawal of U.S. troops in 1973, and the fall of Saigon in 1975, the "Vietnam syndrome" made the U.S. public, Congress, and subsequent administrations especially wary of military intervention overseas (limiting the country to small-scale actions, such as in Grenada and Panama). When the next big confrontation did occur, the 1991 Persian Gulf War, the Powell doctrine of overwhelming force and limited military objectives represented an enormous shift in strategy (Powell 1995). The Vietnam War was exacerbated by the status quo bias in U.S. policy, but the shock of defeat caused a paradigm shift in U.S. foreign policy with a legacy that survives to this day.

This now familiar pattern repeated itself on September 11, 2001. As William Rosenau put it, "although some policymakers and analysts have tried, it is impossible to deny that the events of 11 September 2001 represented a massive failure of intelligence" (Rosenau 2007, 143). The 9/11 commission and other sources reveal that a major terrorist attack on the U.S. homeland was by no means unexpected (Simon and Benjamin 2000; 9/11 Commission 2004; Clarke 2004). Intelligence agencies and counterterrorism experts had long argued that al-Qaeda presented a growing and significant threat in the 1990s—indeed, major terrorist plots of the scale of 9/11 had already been averted—but U.S. policy makers failed to adapt to meet this new threat (Gellman 2002; Rosenau 2007). In a replica of Pearl Harbor, the precise timing and method of attack was of course not predicted, but not preparing for an attack of this kind was the result of a huge intelligence failure. The structure and function of government agencies, as well as many key individuals, were stuck in a Cold War mindset, and had not adjusted adequately to the new threats of transnational terrorism. It took 9/11 to set in motion—too late of course—sweeping changes of government and intelligence organization that many had clamored for years to achieve (the U.S. Commission on National Security for the Twenty-first Century, for example, had warned of terrorist attacks on the United States in early 2001 and recommended the creation of a Department of Homeland Security). Today, "combating al-Qaida has

become the central organizing principle of U.S. national security policy" (Rosenau 2007, 134). Why did it take 9/11 to get it there?

Common Patterns

Although the examples above have much to distinguish them—different periods, locations, opponents, ideologies, geopolitics, and administrations—they nevertheless share common properties. In each event (1) the United States was faced with a novel threat, (2) the potential consequences of this threat were evident, and (3) the United States failed to adapt to this new threat. Nor are these cases anomalies in an ocean of otherwise efficient adaptation; numerous other such cases throughout history could fill several volumes (see, e.g., Dixon 1976; Perlmutter 1978; Snyder 1984; Tuchman 1984; Gabriel 1986; Cohen and Gooch 1991; Regan 1993; Perry 1996; David 1997; Hughes-Wilson 1999). All sides in World War I expected the war to be short and victorious, despite copious evidence to the contrary, and only the carnage of the war itself brought the end of an era in military thinking and the establishment of the League of Nations (Snyder 1984). In the 1930s, the allies thought Hitler had limited goals, despite his accumulating gains, and the horrors of World War II led to the dismemberment of Germany, an open-ended commitment to U.S. military deployments overseas, and the establishment of the United Nations. Similarly, the U.S. reliance on the use of force as a tool of policy was significantly curtailed by the Presidential War Powers Act (triggered by the shock of defeat in Vietnam), and the Goldwater-Nicholls Department of Defense Reorganization Act (triggered by the failed Iranian hostage rescue attempt in 1980). The need for these changes was well appreciated long before they came about, but only major disasters actually made them happen.

It is not only the United States that is subject to these failures. The same phenomenon is common in the history other nations. For example, the 1973 Yom Kippur War exposed a massive failure of Israeli intelligence. There were numerous warning signs of a joint Egyptian and Syrian attack that Israeli military and political leaders failed to acknowledge (Blum 2003; Rabinovich 2004). Following the hugely successful 1967 Six-Day War, and Israeli preconceptions of what it would take for the Arabs to fight Israel again, war was believed to be all but impossible. It took a full-scale invasion for Israel to reject these faulty beliefs. Following the war, Israel's security and foreign policy shifted dramatically. Prime minister Golda Meir resigned along with much of her cabinet, and both the military chief of staff and the chief of intelligence were dismissed. Not only did Israelis tend to see the war as a disaster (even though they won a military victory on the ground), the Yom Kippur War paved the way to a peace process that Israel would never have considered prior to the war (Johnson and Tierney 2006).

Relying on massive shocks to trigger change in security policy is bad for at least seven reasons. First, it increases the probability of disasters happening in the first place (because the victim fails to act to prevent them). Second, it increases the costs of disasters when they do happen (because the victim is unprepared). Third, it limits future policy options because Congress and/or public opinion disallow similar policies or ventures, even in unrelated contexts (e.g., the "no more Vietnams" rhetoric significantly constrained U.S. military power). Fourth, enemies perceive the victim as vulnerable and ill prepared, encouraging future exploitation or attacks (e.g., 9/11 proved that the U.S. homeland can be struck). Fifth, enemies and allies alike perceive that the victim's deterrence policy has failed, leading them to reconsider their own strategies (e.g., NATO allies were rattled by the Cuban Missile Crisis). Sixth, suffering a disaster compromises a state's credibility, which can demote its effective influence in subsequent international relations (e.g., following the Vietnam war, communists in Southeast Asia could do what they wanted without fear of U.S. intervention, as exemplified by their take over of Cambodia and Laos in 1975). Seventh, the immediate consequences of the disaster give the opponent a first-mover advantage (e.g., the naval losses at Pearl Harbor meant the United States was unable to engage Japanese forces in the Pacific for several months, giving them free reign to conquer the Philippines, Malaya, Hong Kong, Thailand, and numerous Pacific islands, making the Pacific war harder for the United States once it was under way). Any or all of these seven factors can undermine a state's immediate national security, its future influence and power, and the electoral success of its leaders.

Does It Always Take Disasters to Trigger Change?

Our hypothesis is not that adaptation to novel security threats *only ever* occurs after major disasters, but rather that they often do. But perhaps the United States usually does, in fact, adapt appropriately to new security threats before disaster strikes, and the examples above are merely prominent exceptions to the norm. Further work is needed to provide a comprehensive test of these competing claims. Nevertheless, we offer here a minitest of our hypothesis, as a way of checking how universal the basic problem may be. In order to test the hypothesis that adaptation to novel security threats tends to occur after major disasters, we need an unbiased sample of case studies. For this purpose, we use a list of "watersheds" or turning points in U.S. security policy since World War II, a list that originated in the National Security Department of the U.S. Air War College and has been used in other studies since (True 2002). Table 13.1 lists these cases and, for each, tests the following predictions:

TABLE 13.1. The Seven Post–World War II "Policy Watersheds" in U.S. Security Strategy and Their Conformity to, or Violation of, The Predictions of Our Hypothesis

	Precipitating Event	*Predictions*		
		Disaster?	Unexpected?	Unprepared?
Truman Doctrine; Marshall Plan, 1947–1949 [Hogan 1998]	Postwar Soviet influence in Europe	Yes (Iron Curtain falls; spread of communist insurgencies)	**Partially (e.g., Truman doubted implications)**	Yes (massive U.S. policy goals took many years)
Rearmament for U.S. containment policy, 1950–1953 [Hastings 1987]	Korean War	Yes (South Korea invaded)	Yes (as Dean Acheson assured Congress 5 days before the invasion)	Yes (U.S. troops unavailable to assist)
Kennedy defense buildup, 1961–1963 [Allison and Zelikow 1999]	Berlin and Cuban crises	Yes (Soviet nuclear missiles in Cuba; West Berlin threatened)	Yes (Kennedy surprised; deterrence strategy failed)	Yes (no plans for a superpower crisis of this type)

Americanization, 1964–1968 [Kaiser 2000]	Vietnam War	Yes (communist expansion in Asia)	**No (but the cost of the war was)**	Yes (badly aligned goals, methods and strategy)
Vietnamization, 1969–1973 [Wirtz 1991]	Vietnam War	Yes (Tet offensive in 1968; ultimate defeat)	Yes (Tet was a major intelligence failure; U.S. didn't expect to lose war)	Yes (at Tet troops deployed in wrong places; war strategy misguided)
Reagan defense buildup, 1979–1985 [Hayward 2001]	Soviet invasion of Afghanistan	Yes (Soviet expansion)	Yes (full-scale invasion not expected)	Yes (realignment of budget and forces)
Reordering of entire U.S. strategic posture, 1990–1991 [Gaddis 1988]	Dissolution of the Soviet Union; Gulf War	**Mixed (collapse of U.S.S.R.; Kuwait invaded)**	Yes (end of Cold War and invasion of Kuwait unexpected)	Yes (U.S. policy changed overnight; Kuwait undefended)

NOTE: From True 2002. Conformity to predictions is indicated by plain text, and violation of predictions is indicated by boldface text.

1. Disasters tend to precede major changes in security policy.
2. Disasters tend to be unexpected (confirming a failure to foresee it).
3. Disasters tend to be unprepared for (confirming a failure to plan for it).

These predictions are tested against the null hypothesis that the seven policy watersheds resulted from events that were not disasters, and that the United States both expected and was prepared for—in other words, representing a rational, timely adaptation to shifting security threats.

As is clear from Table 13.1, all seven policy watersheds followed dramatic disasters, none of which the United States expected, and for all of which the United States was unprepared. There are just three partial exceptions (boldface text): (1) Postwar Soviet influence in Europe was not entirely unexpected, although the United States and western European allies did not fully recognize Stalin's wider goals until late in World War II. (2) The Vietnam War itself was not unexpected—the United States had already been escalating its commitment under two previous administrations (Eisenhower and Kennedy). Nevertheless, the fighting was far more costly than had been expected. Therefore, the Vietnam War was no less an unexpected disaster than any of the other cases. (3) The collapse of the Soviet Union was a disaster only for the U.S.S.R.; it was the opposite for the United States. However, associated events such as the invasion of Kuwait (along with the spread of civil conflicts in Europe, Asia, and Africa) were very much disasters.

Why Does It Take Disasters to Trigger Change?

Although states rarely face extinction, their failure to adapt to novel security threats incurs significant costs in blood and treasure. With such a premium on effective adaptation, the pattern of repeated failure in human history begs the question: why does it take disasters to trigger change? It would surely be better to adapt to novel threats incrementally as they arise. Waiting for disasters to happen before adapting begets and worsens those disasters in the first place, and signals weakness to enemies and allies.

Three basic factors impede change. First, change is hard to assess—the consequences are unknown and disasters are rare. Second, change brings uncertainty—if the status quo has worked until now, why risk an uncertain outcome over a familiar one? Third, change entails costs—the reorganization or acquisition of extra resources adds weight to the argument to do nothing.

Beyond these three basic factors, however, a failure to adapt is powerfully exacerbated by converging biological, psychological, organizational, and political phenomena, summarized in Figure 13.1 and explored in detail below.

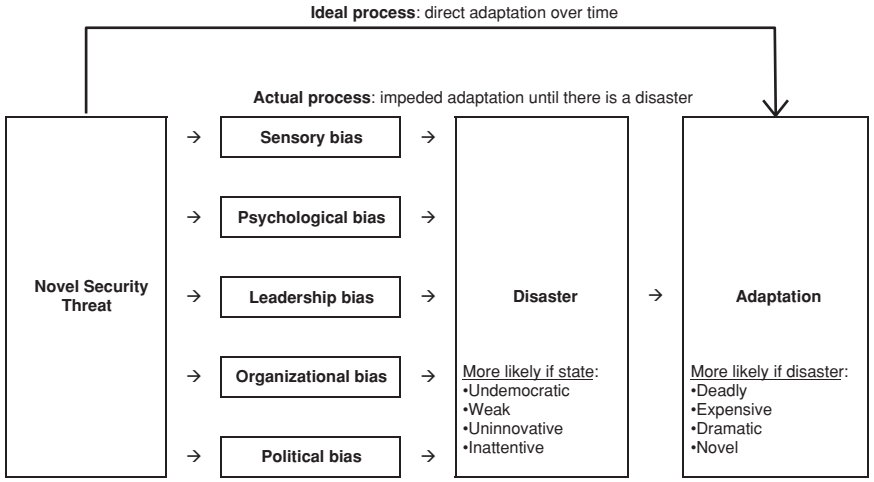

FIGURE 13.1 Scheme of our hypothesis that adaptation to novel security threats tends to occur after major disasters. The causal mechanism is that key biases preserve the status quo and impede adaptation until there is a disaster.

Sensory Bias

A number of sensory and physiological biases predispose us to maintain the status quo and to avoid expending resources on threats outside our personal realm of experience (see also Blumstein, this volume). Humans have a biological predisposition to react to stimuli that reach our five senses (sight, hearing, taste, smell, and touch), and not to stimuli that remain beyond our personal experience. The machinery of the brain does not fully react to something until we experience it in the flesh. This is unsurprising. Our sensory organs, cognitive architecture, and mental processing evolved in order to respond to real threats and opportunities in our immediate local environment, not to abstract, vague, distant, or hypothetical threats that happen elsewhere, or to others. Of course, our brain does generate vicarious emotional reactions to events that we observe or learn is happening to others, but not as powerfully as if we experience them for ourselves (Simonsohn et al. 2006). Such effects are evident in international relations as well. Decisions about military intervention were found to be influenced more by a state's own experience than merely observing the experience of others (Levite et al. 1992). The United States, for example, was unperturbed about the French experience of war in Vietnam—Kennedy reminded a reporter, "That was the *French*. They were fighting for a colony, for an ignoble cause. We're fighting for freedom" (Tuchman 1984, 287). Later on, the Joint Chiefs of Staff, citing French errors

and indecision in the conflict, noted wryly, "The French also tried to build the Panama Canal" (U.S. Department of Defense 1971, Vol. 3, 625).

Also very important is the general principle, across a wide range of psychological phenomena, that negative events and information are processed more thoroughly and have greater impact than positive events, and negative impressions and stereotypes are quicker to form and more resistant to disconfirmation than positive ones (Baumeister et al. 2001). In terms of the effects of experience on human psychology, "bad is stronger than good." In international politics as well, failure, as opposed to success, appears to have an intrinsic leverage: "People learn more from failure than from success . . . past success contributes to policy continuity whereas failure leads to policy change" (Levy 1994, 304). This appears to result from an interaction with expectations. "Outcomes that are consistent with expectations and achieve one's goals generate few incentives for a change in beliefs, whereas unexpected results and those that fall short of one's goals are more likely to trigger a change in beliefs and policy. Thus the most likely outcomes to trigger learning are failures that were either unexpected at the time or unpredictable in retrospect" (Levy 1994, 305). A classic study by Dan Reiter found that alliance behavior was most influenced by a state's experience of success or failure in previous wars, and ignored actual current threats (Reiter 1996). States switched their policy only if it was deemed a failure in the past.

In summary, we are most likely to react to a threat (1) if it reaches us through first-person experience (rather than via newspapers, radio, the Internet, or television), and (2) if it is a negative event (such as a disaster) rather than a positive one. It may therefore take a Pearl Harbor of 1941, a threat of nuclear holocaust as in 1962, defeat in war, or a 9/11 to surmount our sensory barriers, acknowledge major new threats, and goad us into action.

Psychological Bias

A number of psychological biases also predispose us to maintain the status quo and to avoid expending resources on threats outside our normal realm of perception. Perhaps most important is cognitive dissonance. Conflicting information must be resolved in order to generate a coherent interpretation, and cognitive dissonance tends to select, organize, or distort incoming information so that it matches our preferred or preexisting beliefs (Vertzberger 1990; Tetlock 1998; Sears et al. 2003; McDermott 2004). Even experts often discount potential problems due to the cognitive demands of complex events (Dorner 1996). For example, Irmtraud Gallhofer and Willem Saris found that despite at least seven distinct strategies being floated during the Cuban Missile Crisis executive committee meetings, decision makers tended to consider only two at a time (Gallhofer and Saris 1996).

Experimental research in cognitive and motivational psychology reveals a vast array of biases that tend to preserve the status quo: *deformation professionelle* (a tendency to see things from the perspective of the conventions of one's profession); the mere exposure effect (a preference for things that are more familiar); the availability heuristic (a tendency to make predictions that are based on perceived rather than actual salience); projection bias (a tendency to assume that others share similar beliefs to oneself); the bandwagon effect (a tendency to do or believe the same as others); false consensus effect (a tendency to expect others to agree with oneself); discounting (to prefer immediate over long-term payoffs); and, finally, the well-documented and pervasive effects of in-group favoritism and out-group derogation, groupthink, and overconfidence (Janis 1972; Jervis 1976; Kahneman et al. 1982; Vertzberger 1990; Tetlock 1998; Johnson 2004).

Overconfidence appears to have a particular importance. We tend to hold positive illusions of our abilities, our control over events, and of the future, all of which lead to overconfidence about our vulnerability to risk, and therefore to discount the need for change (Johnson 2004). Positive illusions in U.S. decision making may account for the failure to deter Japan in 1941, the Soviet Union in 1962, and Saddam Hussein in 2003, among other cases. However, harking back to the importance of sensory biases, once personally involved in a disaster, optimistic illusions disappear. Psychologists found that Californians were overly optimistic about the risk of earthquakes until they lived through one (Burger and Palmer 1992). Yechiel Klar's study of Israelis living with the threat of terrorist attacks found that people maintain positive illusions as long as threats are "hypothetical" and "psychologically unreal." But, "when the group to which people belong is the target of some significant ongoing calamity, even when the participants themselves are currently not the direct victims, the unreality of the event dissolves and optimism (both absolute and comparative) decreases or vanishes altogether" (Klar et al. 2002, 216). Disasters serve to wake us up to reality. They are very effective at doing so, but, by definition, the wake up call comes too late.

Leadership Bias

Particular leaders and their ideas often compel us to maintain the status quo and to avoid expending resources on threats outside the accepted realm of attention. These individuals' preferences can also become institutionalized such that they persist beyond their worth until, or sometimes even after, the original proponent falls from power, resigns, or dies. It has been a recurrent historical theme for leaders to derail their own intelligence services by favoring positive reports, punishing the bearers of bad news, setting different agencies in competition with each other, and interfering with the methods

and targets of information gathering (Handel 1989; Van Evera 2003). A recent example is the Bush administration's use of intelligence on weapons of mass destruction and the postwar challenges of Iraq in order to support their favored policy (Clark 2003; Jervis 2003; Fallows 2004; Woodward 2005). With such strong incentives to control information and policy, and to protect their political reputation, leaders can exert enormous impediments to effective adaptation.

Organizational Bias

Numerous organizational biases also predispose us to maintain the status quo and to avoid expending resources on threats outside the realm of standard operating procedures. Bureaucratic procedures, vested interests, competition for promotions, sunk costs, access to the elite, and turf wars over budgets and responsibilities favor a rigid focus on past events and successes, and a rigid avoidance of rocking the boat to advocate some new and unproven revision of strategy (Kovacs 1997; Allison and Zelikow 1999; Van Evera 2003). An entire literature has built up around this principle (organizational learning) and forms the classic "bureaucratic politics model" of decision making in political science—a default explanation for bizarre or failed policies (Allison and Zelikow 1999). Although organizational biases may create problems, these very characteristics are to some extent intentional: "Indeed, the value of institutions typically lies in their persistence or 'stickiness,' which allows actors to make plans, invest and organize their affairs around institutions and, in general, lends certainty and predictability to their interactions" (Viola and Snidal 2006, 5).

At times, however, the costs will outweigh the benefits. Prior to 9/11, the machinery, professionals, and mindsets of the Cold War era still exerted a significant legacy. There was a "failure of imagination"—a dearth of lateral thinking or fresh ideas—in the intelligence community even though the threats of transnational terrorism were evident (Simon and Benjamin 2000; Rosenau 2007). In addition to the failures to actually plan for novel threats, Stephen Van Evera has laid out reasons why institutions have little incentive to self-criticize or evaluate their own performance at all (Van Evera 2003). The entire institutional environment is hostile to adaptation: "Myths, false propaganda, and anachronistic beliefs persist in the absence of strong evaluative institutions to test ideas against logic and evidence, weeding out those that fail" (Van Evera 2003, 163). The maintenance of bureaucracy itself can sometimes become an all engrossing task. When Donald Rumsfeld took over at the Pentagon, for example, he began issuing numerous white memos ("snowflakes") around the Pentagon demanding information on who actually does what and how they do it, until some people were spending more time answering snowflakes than doing normal work (Woodward 2005).

A further problem with organizations is that the "sensors"—the people with their ears to the ground—are disjointed from the decision-making structure (in an interesting corollary to the sensory failures noted above). Leaders are sometimes the last to know about impending (or even actual) disasters. The middle managers or those below them are the ones who deal on an everyday basis with the outside world and are therefore more likely to detect novel threats, or to recognize that old methods are no longer appropriate. For example, when a minor flaw was found in the Pentium processor in 1994, Intel suffered half a billion dollars of damage in under six weeks. The fault caused a rounding error in division just once every nine billion times, however, this tiny flaw quickly became significant—the news spread rapidly on the Internet and was amplified by Intel's new global prominence and identity. According to Intel CEO Andrew Grove, "I was one of the last to understand the implications of the Pentium crisis. It took a barrage of relentless criticism to make me realize that something had changed—and that we needed to adapt to the new environment" (Grove 1999, 22).

This echoes the intelligence situation before 9/11 and the reaction of administration officials. CIA director George Tenet and terrorism expert Cofer Black say they could not have laid out the serious possibility of a major attack on U.S. soil any clearer to Condi Rice in a meeting in July 2001. "The only thing we didn't do," according to Black, "was pull the trigger to the gun we were holding to her head" (Woodward 2005, 79). If the National Security Adviser is unreceptive to such an issue, then it is unlikely to win the President's attention. The administration as a whole was simply not geared to respond to the growing threat of al-Qaeda (Gellman 2002; Clarke 2004). Even if they had been receptive, as one insider noted, "The U.S. government can only manage at the highest level a certain number of issues at one time—two or three. You can't get to the principals on any other issue" (Gellman 2002).

Organizational and bureaucratic impediments to security appear to be severe. Eventually, budgets or political obstacles get in the way. Richard Betts's analysis of surprise attacks in international relations found that "most of the options available to the West for reducing vulnerability to surprise are limited by political or financial constraints" (Betts 1983, 311). Effective readiness against major threats was simply too expensive or complicated to maintain on a regular basis.

Political Bias

Electoral politics also predispose us to maintain the status quo and to discount genuinely important threats in favor of politically salient ones. There is no reason to expect efficient adaptation (or sometimes any adaptation at all) to address the most important national security threats. What is

threatening in secret intelligence reports is irrelevant to an oblivious public—or rather, an oblivious electorate. Politics provides numerous alternative motivations for individual leaders, political parties, lobby groups, and the public to steer policy and incentives in their own preferred direction, often to the detriment of adaptation to national security threats. The reality of politics means that radical shifts in policy, especially toward a novel hypothetical threat (about which the key intelligence information may be known only to elites) are often indefensible in Congress, hard to obtain the necessary budget to initiate or complete, and politically suicidal. There are few points to be scored (or as many to lose) in pushing for rapid or comprehensive change, for admitting mistakes, or for adapting. As long as the threat is at least four years away, or can be blamed on extraneous causes or opposing political parties, other concerns are likely to take precedence.

Incumbency is an important component of this problem. A high turnover of civil servants or politicians allows for continual and gradual adaptation to changing circumstances over time. By contrast, a low turnover reduces the ability and inclination to adapt, gradually bottling up problems until the whole system collapses under the pressure of a major disaster. In the U.S. government, a number of factors operate to empower incumbents and entrench particular elites and procedures. Disasters may be particularly effective at bringing down an incumbent regime, whose failings—real or perceived—often become a central motivation and electoral strategy for opposition parties or congressional inquisitions.

To summarize this section, numerous features of human nature and the nature of institutions that humans create limit our ability to detect and react appropriately to novel security threats. Because these features stem from independent sources at different levels of analysis (e.g., individual behavior, organizational behavior, elite decision making, etc.), they are likely to generate a status quo bias across a wide range of circumstances. For example, even a forward-looking bureaucracy may have to work against a short-sighted leadership, or vice versa. To put it bluntly, society seems predisposed to preserve the status quo until something goes wrong. As Henry Petroski noted in his book *Success through Failure*, "Good design always takes failure into account and strives to minimize it. But designers are human beings first and as such are individually and collectively subject to all the failings of the species, including complacency, overconfidence, and unwarranted optimism" (Petroski 2006, 193–194).

When Are Disasters More or Less Likely to Trigger Change?

When are states more likely to suffer disasters? And what *types* of disasters are more or less likely to generate appropriate and lasting change? In other words, what are broad-brush circumstances (or "independent variables")

that work to exacerbate or suppress the biases we have noted above? Such sources of variation are crucial to future tests of our hypothesis. But they also have practical significance: if we can get a handle on the basic conditions that make disasters more or less likely, we can attempt to steer our behavior and institutions toward those conditions that reduce the probability of being the victim of disaster. Below we consider characteristics (of both states and disasters) that are most and least likely to cause adaptation to novel security threats.

Characteristics of States That Promote Adaptation

Democracy. Democracies promote journalistic inquiry, congressional review, opposition criticism, and the regular turnover of political representatives. By contrast, authoritarian regimes deter or silence messengers of bad news and favor long-term incumbents. Hitler's generals, for example, rarely told him the truth about the impending disasters such as at Stalingrad (Handel 1989; Beevor 1998). The influence of democracy is a matter of degree, however, rather than just a binary distinction between democracy and tyranny. For example, the Bush administration's handling of intelligence prior to the Iraq War served to undermine the Washington system of checks and balances, handing the authority to wage war to the President—exactly what the founding fathers designed the U.S. government to avoid (Fisher 2003).

Power. Powerful states can create expensive and extensive intelligence agencies, equipment, and personnel. By contrast, weak states are more likely to be constrained by the resources they have to detect, prepare for, and react to disaster. Of course, 9/11 and many other examples given above demonstrate that even massive amounts of resources available to powerful states such as the United States do not solve the problem. Power must be applied effectively. Nevertheless, on average, more powerful states should be more likely to achieve effective adaptation.

Innovation. Security strategies adapt more effectively in a more innovative culture. For example, Germany and Britain were far more innovative in developing their military strategies and tactics than the French in the interwar period, and this directly led to differential combat outcomes in World War II (Posen 1984).

Attention. When a state is focused and committed to dealing with a potential threat, it has a much higher chance of adapting to meet it. By contrast, when a state is mired in serious domestic or international crises, it is far less likely to detect or respond appropriately to novel threats.

Characteristics of Disasters That Promote Adaptation

Deadly. High numbers of casualties, especially civilians.
Expensive. High levels of damage (or lost opportunity).
Dramatic. Symbolic or salient targets.
Novel. Not just a big version of an existing threat.

Can Change Occur without Disaster?

Our hypothesis is that adaptation to novel security threats tends to occur after major disasters. Like any hypothesis, this does not mean that policy changes *only ever* occur following major disasters. We only suggest that it may be more commonly the case than the other way around. But there are likely to be exceptions. Indeed, our discussion above sets out explicit conditions under which we may expect major policy change to occur without disaster—powerful, democratic states that are innovative and attentive, especially ones with minimal biases in their psychology, organizational behavior, leadership, and politics. Therefore, not only do we expect there will be exceptions, but we propose specific variables that will characterize these exceptions. Future studies could test this hypothesis with, for example, matched pairs of otherwise similar cases: one that adapted successfully, and one that did not.

One can think of a number of potential counterexamples in which security strategy changed significantly without any disaster. For example, people often cite the remarkable lack of a disaster following the break up of the Soviet Union and the democratization of Eastern Europe after the fall of the Berlin Wall. However, it is important to realize that this is a distinctly western perspective. From the perspective of the U.S.S.R., it was the biggest disaster of its history—indeed, it signaled its own extinction. Even from a western perspective, though, the lack of disaster may be misleading: the new security environment represented the collapse of a formidable enemy, followed by a power vacuum, not the emergence of a new threat per se. There was no agent to bring disaster (barring a renegade general with Soviet nuclear missiles, or something along those lines). Similar problems arise with many other prominent examples of major security changes that appeared to escape disaster: the fall of the British Empire, the reunification of Germany, the nuclear armament of India and Pakistan. Such cases deserve further scrutiny in the context of our hypothesis.

It is easier to think of counterexamples that do not reside in the realm of security. For example, numerous social, economic, and technological transformations occur without disaster, ranging from awarding women the right to vote, to the introduction of the Euro, to the space race. One could also argue that major environmental efforts are underway to avert the looming

disaster of global climate change (as evidenced by such forward thinking as the Stern Review). However, it is not at all clear that anywhere near enough is actually being done, whatever the proposals and plans.

Perhaps, then, there is something special about the domain of security that links change and disaster. After all, lapses in security are almost by definition associated with violence, death, and destruction, so security disasters may be more dramatic, more visible, and more likely to compel policy makers and organizations to change.

Even if adaptation is rare in the domain of security, future studies can identify cases where adaptation was more successful than others. One example might be the Malaya Emergency of 1948–1960 (see Johnson and J. Madin, this volume). In that conflict, the British and Malayan counterinsurgency forces revealed themselves as organizations able to learn and adapt—though tellingly this occurred *through* a series of disasters. According to a recent survey, "one of the things that allowed the British army to innovate and adapt during its counterinsurgency operations in Malaya in the 1950s (and thus attain success) was its willingness at all levels to admit failure" (Metz and Millen 2004, 26; Nagl 2002). The key comparison may therefore be between states that do learn from disasters, and states that do not learn even from disasters. On that note, we now turn to possible solutions to minimize the likelihood of disasters.

Solutions

The bright side of this story is that the reasons for our failure to adapt are systematic, not random. Empirical evidence from cognitive and social psychology offers a taxonomy of causes and consequences of key biases (reviewed in Jervis 1976; Tetlock 1998; Sears et al. 2003; Van Evera 2003). We therefore have scientific tools to identify when, where, and why we fail to adapt to new threats, who is most susceptible, and how to make corrections to compensate (or even overcorrections as insurance policies against these biases). It is likely, however, to be a difficult task—we are often blissfully unaware of these biases in the first place, and that is precisely why we fall prey to their influence. Moreover, solutions require us to look beyond our typical experience and plan for things that seem unlikely and farfetched—hardly things that motivate urgent action. Nevertheless, a careful study of causes and consequences can, in principle, help to design institutions and decision-making procedures that will improve adaptation to novel security threats.

Some of the problems outlined above are already well recognized by the policy community. Indeed, many of the key problems are already being addressed by the post-9/11 reorganization of the intelligence services. For example, the U.S. National Intelligence Council was set up to look ahead at

emerging threats that remain "over the horizon." Other changes include more scenario-based planning exercises, more "red teaming" (role-playing the enemy), and recruiting lateral and imaginative thinkers such as the novelist Tom Clancy to think through possible future threats. However, reforms may be more successful if they exploit the scientific insights emerging from biology and psychology. If history is any guide, the same mistakes will be repeated unless we try something new. We need innovative solutions if we are to escape the recurrent failures of imagination that litter the past so liberally. We discuss a number of potential solutions below.

Lessons from Evolutionary Biology

The best model of successful adaptation to changing security threats may lie in evolutionary biology, where adaptation is the core process underlying billions of years and millions of examples of survivors. Adaptive processes in nature are magnificently diverse, fine tuned over countless generations of trial and error, and well documented. In his analysis of security insights from biological evolution, Vermeij (this volume) notes seven key strategies that can be employed in the face of novel security threats: tolerance, active engagement, increase in power or lifespan, unpredictable behavior, quarantine and starvation of the threatening agent, redundancy, and adaptability. He finds that "the most successful attributes of life's organization—redundancy, flexibility, and diffuse control—are also the characteristics of human social, economic, and political structure that are best suited to cope with unpredictable challenges." We list Vermeij's conclusions in Table 13.2, along with some suggested applications to security.

Vermeij's key insight is that adaptations to everyday threats often also turn out to be effective adaptations to unpredictable threats. The owners of these serendipitous adaptations will be more likely to avoid or withstand rare and unpredictable disasters. As Vermeij puts it, a trait that enabled an organism to "endure the extraordinary conditions prevalent during times of mass extinction cannot be considered an adaptation to those circumstances but is instead an accidental if welcome consequence of adaptation to more commonplace phenomena" (Vermeij, this volume). There are numerous examples in human history in which commonplace adaptations were used to deal with novel threats. For example, when Soviet tanks escorting convoys in Afghanistan discovered they could not elevate their guns high enough to engage hostile forces high on the mountainsides, the Soviet Army resorted to using self-propelled anti-aircraft artillery instead (Beckett 2001). States that accumulate diverse and flexible technologies, practices, or institutions over time are more likely to be able to fall back on a broader range of alternatives in unusual circumstances.

TABLE 13.2. Vermeij's Lessons from the History of How Biological Organisms Evolved to Deal with Unpredictable Threats in Nature (Vermeij, this Volume), and Some Possible Applications to Security Policy Derived from Our Study

Lessons	*Application*
There will always be unpredictable threats, and no adaptations to them can ever be perfect.	We should expect ongoing arms races rather than perfect solutions. Even imperfect adaptations lead to improved strategies.
Adaptation to threats comes with costs and constraints.	Adaptation may be costly, but stasis may be worse. Adaptation must be allocated rolling budgets (not one-off lump sums).
Passive resistance, though highly effective, is inconsistent with activity and the exercise of power and by itself is not an acceptable option for most human societies.	Proactive strategies are essential if a state wants to play other international roles. U.S. isolationism is inconsistent with its defense.
Exclusively active engagement exposes entities to ecological collapse engendered by interruptions in resource supplies and, therefore, by itself is an unreliable long-term strategy.	Unlimited commitment to active engagement is risky and may be counterproductive.
Redundancy and a modular structure of semiautonomous parts under weak central control provide the most flexible, adaptable, and reliable means of making unpredictable challenges predictable.	Policymaking, military, and intelligence resources should be decentralized, granted independence, and have back-up systems.
The history of life in general, and of extinction in particular, shows that adaptation to everyday as well as unpredictable circumstances has improved over the course of time.	Adaptations that can be co-opted to alternative uses offer dual protection against commonplace and unpredictable threats.

Lessons from the Immune System

Immune systems also offer intriguing models for human security. They are especially interesting because of their efficiency, lying low in normal times but wielding an extraordinary capacity for an enormous surge in response to a threat. As Villarreal (this volume) writes, "Biological systems are inherently local, rapid, robust and adaptable systems. They are able to rapidly

marshal all the needed diverse and central resources, but inherently reduce resource consumption when no longer needed. They are capable of searching for, finding, destroying, and sterilizing threats, both hidden and apparent. They are even able to respond to threats never before seen." The prominence of immune responses in nature attests to the advantages of flexibility and adaptability in the face of novel threats. However, the immunity model presents an additional point: locally focused responses may be far more adept at contending with new threats than those requiring central control or approval. This has potential implications for security strategy in human systems; central command and control structures are often less able to detect, understand, and respond adequately to new threats than local organizations in direct and immediate contact with the threat. Interestingly, there are cases in which the immune system can overreact, drain significant resources, and become dangerous to the organism itself. This also has parallels in human security, in which perceived threats can initiate overblown and costly responses (Mueller 2005; Blumstein, this volume).

Lessons from Institutional Design

Institutions and organizations could be redesigned to hard wire mechanisms for effective adaptation, just as DNA and the process of natural selection assure adaptation in biology. A recent study by Viola and Snidal (2006) argues that evolutionary mechanisms offer a "potentially powerful way to account for the persistence, adaptation, and abandonment of international institutions" (Viola and Snidal 2006, 3). Although current international institutions exhibit many features that arose by design, they also exhibit many other features that arose from a process of "decentralized emergence" over time, without conscious planning. For example, norms of sovereignty, diplomacy, and customary international law arose largely "from the on-going practices of states" (Viola and Snidal 2006, 1). Ideally, institutions would include such organic attributes in order to "adapt and respond to unanticipated elements in their environment" (Viola and Snidal 2006, 4). Designers could identify how these processes of adaptation occur, the conditions under which they are successful, and ways to exploit them. Of course, adaptability often already exists: some degree of flexibility is granted in most organizations, decisions may be delegated to lower level units, and mechanisms are often in place to seek and respond to feedback. Nevertheless, an evolutionary approach may help to identify successful adaptive processes, their likely causes, and their likely consequences.

In addition, the methods and quantitative tools developed in biology to study adaptation may prove useful in understanding the adaptation of human institutions as well. Viola and Snidal note that "it is unlikely that institutions would develop without growing in some way out of the previous institutions," and "in a given issue area it is common to see institutions with

family resemblances" (Viola and Snidal 2006, 8). These echo the notions of common ancestry and evolutionary legacy central to evolutionary biology, for which there are well-developed statistical methods to test for evidence of adaptation, correlations with associated traits, and points of divergence, all while controlling for characteristics shared by common ancestry.

In a fast-moving world of rapid communication, some have argued that even forward planning is no longer the best strategy to prepare for the future. Instead, organizations can be structured to be automatically adaptable and flexible by nature, so that the system is self-geared to adapt and exploit change as it happens (Brown and Eisenhardt 1998). This violates many traditional views of organizational design, but at least one prominent firm is based on this kind of unstructured system: Google (Lashinsky 2006). Google actively promotes innovation and experimentation through the independence of its subunits and workers. One strategy is encouraging its engineers to spend one day a week working on pet projects and submitting new ideas for product development to the Google "ideas list" (Elgin 2005). This list is monitored by the upper levels of management (as opposed to first passing through multiple middle levels) and screened for highly innovative and potentially investment-worthy ideas.

Finally, even if an organization itself cannot easily be restructured, incentive structures can be created within it (via financial, budgetary, or professional rewards) to encourage flexibility, adaptation, and review instead of rigidity, policy stasis, and nonevaluation.

Lessons from the Insurance Industry

In order to remain financially viable, insurance companies must be able to either predict or build in buffers against novel catastrophes. The insurance industry thus provides another interesting model for contending with future threats—both known and unknown. In a sense, these companies provide a form of "preadaptation" to novel threats—a guarantee of being able to rebuild following damage. Although it is inherently costly, adopting insurance strategies can provide the necessary buffers against occasional disasters. Although the disasters themselves may not be possible to avoid, their negative consequences can be mitigated. However, it is important to recognize that insurance companies have the luxury of passing on these costs to their clients; government agencies do not.

Lessons from Futures Markets

If humans are bad at detecting novel threats, an alternative is to maximize the number of individuals contributing to assessment. It is a well-recognized phenomenon that the average of a large number of estimates can be extremely accurate—the so called "wisdom of crowds" (Surowiecki

2004). As long as the group is diverse, independent, and decentralized, then individual biases will cancel each other out, leaving available information from a wide range of sources to converge on the correct assessment. For exactly this reason, even expert analyses by intelligence agencies, such as the CIA, may be expected to be inaccurate, because they are not diverse (analysts are all Americans), not independent (analysts share methods, sources, and information), and not decentralized (they work for the same organization). By contrast, an ideal assessment would include opinions from across the globe, including the full spectrum of ideological, cultural, and political differences, and exploiting multiple sources of local information. This has direct practical applications. Harnessing this phenomenon and using it for predictions can be achieved by the use of "futures markets," in which one buys a contract that will pay, say, $10 if a given event occurs by a certain date. The market price of these futures contracts then reveals a probability that the event will happen (Leigh et al. 2003). For example, on February 14, 2003, the price of $10 futures on Saddam Hussein no longer being president of Iraq on June 30 were trading at $7.50 on tradesports.com, suggesting the probability of war was 0.75.

The Pentagon proposed a "Policy Analysis Market" to exploit the opportunities of futures prediction in 2003. The idea was to use futures markets to evaluate growth, political stability, and military activity in eight nations, four times a year. The project swiftly attracted the misnomer of "terrorism futures" and was scrapped by nervous politicians—yet another example of institutional bias working against innovation. Nevertheless, a number of political futures markets do exist on commercial web sites. One can bet, for example, on the likelihood of U.S. military action against North Korea, air strikes against Iran, or the capture of Osama bin Laden. If these futures markets can be expanded, they may well outperform expert assessments of the likelihood of important events in national security, bypassing the impediments and biases to adaptation outlined above.

Conclusions

If humans, institutions, and states were rational, security policy would change in step with the shifting threats of the day. Our examples of Pearl Harbor, Cuba, Vietnam, and 9/11 indicate that this logic is often violated, and the United States failed to adapt to novel security threats until they caused a major disaster. Our mini case study suggests that these examples are not unusual (Table 13.1). On the contrary, all seven U.S. security policy "watersheds" since World War II were initiated by major disasters, which the United States neither expected nor prepared for. This is further supported by the fact that the U.S. defense budget has not changed in line with shifting

threats but rather as significant step-changes after major international events (True 2002). Adaptation to novel security threats is most likely to occur when a state suffers a major disaster—especially among states that are democratic, powerful, innovative, and attentive, and especially if the disaster is deadly, expensive, dramatic, and novel. In other, "normal" times, adaptation to novel security threats is severely impeded because (1) dangers that remain hypothetical fail to trigger appropriate sensory responses, (2) psychological biases serve to maintain the status quo, (3) dominant leaders entrench their own idiosyncratic policy preferences, (4) organizational behavior and bureaucratic processes resist change, and (5) electoral politics offers little incentive for expensive and disruptive preparation for unlikely and often invisible threats. The sudden disasters that break intervening periods of stasis are analogous to the paradigm shifts that Thomas Kuhn (1970) noted in the progress of science, and the punctuated equilibrium theory that Frank Baumgartner and Bryan Jones (1993, 2002) proposed to explain the dynamics of U.S. policy making.

Even when adaptations do follow disasters, they often turn out to be short-lived. Soon enough the powerful impediments to change, whether psychological, organizational, or political, come to the fore. The human brain tends to cast our perception of past events in an overly positive light (Greenwald 1980; Schacter 1995). Even after the unprecedented carnage of World War I, for example, John Stoessinger noted that the "old people to whom I spoke about the war remembered its outbreak as a time of glory and rejoicing. Distance had romanticized their memories, muted the anguish, and subdued the horror" (Stoessinger 1998, xii). Organizations and societies also work to downplay failure and construct myths that deflect blame and reinterpret history (Van Evera 1998; Schivelbusch 2004; Johnson and Tierney 2006). For example, German society embraced the myth after World War I that the army was undefeated on the battlefield and had been stabbed in the back by politicians. Meanwhile, political elites go through the motions, creating the image of change without any intention of bearing its real costs, or doing just enough to tick the boxes in the eyes of Congress or the public. Even with 9/11, for example, the disaster appears to have paled enough into the past that essential reforms have fallen far below the recommendations of the 9/11 commission (9/11 Public Discourse Project 2005). A similar process occurred after the bombing of the London Underground: "The atrocities of July 7th 2005 turn out to have been the kind of alarm call that is followed by intemperate grunts and a collective reaching for the snooze button" (Economist 2006). It is noticeable that political, media, and public attention has already strayed from terrorism and the war on terror in favor of a new sensory-rich disaster on which everyone is focused: Iraq.

Fortunately, cumulative major disasters such as 9/11 usually generate a kind of ratchet effect, such that even after the initial impact wears off, we

TABLE 13.3. Policy Prescriptions to Maximize Effective Adaptation in Each of the Key Problem Areas

Bias	*Policy Prescriptions*
Sensory bias	Ensure decision makers see frontline personnel and victims
	Ensure decision makers hear opposing viewpoints
	Ensure decision makers travel to places at issue
Psychological bias	Increase diversity and sources of information
	Increase turnover in appointees and decision-making groups
	Install high-level devil's advocates in policy discussions
Leadership bias	Limit power
	Limit terms of office
	Insist on periodic reevaluation of existing policies
Organizational bias	Encourage "bottom-up" development and communication of ideas (Google model)
	Solicit recurring internal and external review
	Create incentives for continual change
Political bias	Increase public information (so that electorate and government see the same threats)
	Increase congressional oversight of security policy
	Reduce campaign financing and duration

are still left with some, perhaps imperfect, novel adaptations (e.g., improved airport security, or the U.K. Civil Contingencies Secretariat to "prepare for, respond to and recover from emergencies," see www.ukresilience.info). It is often noted that in Chinese, the word for "crisis" includes the notion of opportunity as well as danger. If humans are not good at avoiding disasters, we should at least learn to react to them in ways that best utilize the opportunity for change. Cumulative change can be maximized even if it is frustratingly imperfect.

Democratic, powerful, innovative, and attentive states may have the best chance of avoiding security disasters. But whether a state meets these conditions or not, there are a number of policy prescriptions that could improve effective adaptation to novel security threats (Table 13.3). Future studies will be able to improve, expand, and test these ideas, and there is clearly a wealth of models from which to derive effective tricks of adaptation, including evolutionary biology, the immune system, institutional design, futures markets, and insurance.

Although there is room for improvement, history suggests that humans need disasters to occur before waking up to novel security threats, whether they are disasters of national security, disease, starvation, poverty, or

Hypothesis and Predictions

HYPOTHESIS

Adaptation to novel security threats tends to occur after major disasters.

PREDICTIONS

Disasters tend to precede major changes in security policy.
Disasters tend to be unexpected (confirming a failure to foresee it).
Disasters tend to be unprepared for (confirming a failure to plan for it).

environmental change. This does not bode well for the future. Even when a threat poses a clear and present danger, such as global climate change, political actors do almost nothing to adapt to the threat until it is too late. As a recent *New Scientist* editorial recognized (New Scientist 2006): "The world will one day act with urgency to curb greenhouse gases: the likely violence of the atmosphere's reaction to our emissions makes that inevitable. Climate change awaits its 9/11."

ACKNOWLEDGMENTS

We thank Rafe Sagarin and Terence Taylor for their ideas, advice, criticism, and invitation to join the Working Group on Ecological and Evolutionary Models for Homeland Security Strategy; and the National Center for Ecological Analysis and Synthesis for hosting us. Dominic Johnson is indebted to the Branco Weiss Society in Science Fellowship, the International Institute at UCLA, and the Society of Fellows and the Woodrow Wilson School of Public and International Affairs at Princeton University. Elizabeth Madin would like to thank the U.S. Department of Homeland Security, the U.S. National Science Foundation, and Steve Gaines. We also owe our thanks to Richard Cowen, Robert Mandel, Dominic Tierney, and all the members of the working group for excellent comments and criticisms on the manuscript.

REFERENCES

9/11 Commission. 2004. *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States.* New York: W. W. Norton.

9/11 Public Discourse Project. *2005 final report on 9/11 Commission recommendation.* December 5. Available at www.9-11pdp.org/.

Allison, G., and P. Zelikow. 1999. *Essence of decision: Explaining the Cuban missile crisis.* New York: Longman.

Baumeister, R. F., E. Bratslavsky, C. Finkenauer, and K. D. Vohs. 2001. Bad is stronger than good. *Review of General Psychology* 5: 323–370.

Baumgartner, F. R., and B. D. Jones. 1993. *Agendas and instability in American politics.* Chicago: University of Chicago Press.

Baumgartner, F. R., and B. D. Jones. 2002. *Policy dynamics.* Chicago: University of Chicago Press.

Beckett, I. F. W. 2001. *Modern insurgencies and counter-insurgencies: Guerrillas and their opponents since 1750.* New York: Routledge.

Beevor, A. 1998. *Stalingrad.* London: Penguin.

Betts, R. 1983. *Surprise attack: Lessons for defense planning.* Washington, DC: Brookings Institution Press.

Blum, H. 2003. *The eve of destruction: The untold story of the Yom Kippur War.* New York: HarperCollins.

Brown, S. L., and K. M. Eisenhardt. 1998. *Competing on the edge: Strategy as structured chaos.* Cambridge, MA: Harvard Business School Press.

Burger, J., and M. Palmer. 1992. Changes in and generalization of unrealistic optimism following experiences with stressful events: Reactions to the 1989 California earthquake. *Personality and Social Psychology Bulletin* 18: 39–43.

Busenberg, G. J. 2003. Agenda setting and policy evolution: Theories and applications. Paper presented at The Midwest Political Science Association 2003 Conference. Chicago, IL, April 3–6.

Clark, W. K. 2003. *Winning modern wars: Iraq, terrorism, and the American empire.* New York: PublicAffairs.

Clarke, R. A. 2004. *Against all enemies: Inside America's war on terror.* New York: Free Press.

Cohen, E. A., and J. Gooch. 1991. *Military misfortunes: The anatomy of failure in war.* New York: Vintage.

David, S. 1997. *Military blunders: The how and why of military failure.* London: Robinson.

Dixon, N. 1976. *On the psychology of military incompetence.* London: Jonathan Cape.

Dorner, D. 1996. *The logic of failure: Recognizing and avoiding error in complex situations.* Cambridge, MA: Perseus.

Economist. 2006. One year on: The wake-up call that wasn't. *Economist,* July 8, 29–30.

Elgin, B. 2005. Managing Google's idea factory. *Business Week Online,* October 3. http://www.businessweek.com/magazine/content/05_40/b3953093.

Fallows, J. 2004. Blind into Baghdad. *Atlantic Monthly,* January/February, 53–74.

Fisher, L. 2003. Deciding on war against Iraq: Institutional failures. *Political Science Quarterly* 118: 389–410.

Foucault, M. 1970. *The order of things: An archaeology of the human sciences.* New York: Random House.

Foucault, M. 1977. Nietzsche, geneology, history. In *Language, counter-memory, practice: selected essays and interviews,* ed. D. F. Bouchard, 139–164. Ithaca, NY: Cornell University Press.

Fursenko, A., and T. Naftali. 1997. *One Hell of a gamble: Khrushchev, Castro, and Kennedy, 1958–1964.* New York: W. W. Norton.

Gabriel, R. 1986. *Military incompetence: Why the American military doesn't win.* New York: Noonday Press.

Gaddis, J. L. 1988. *We now know: Rethinking cold war history.* New York: Oxford University Press.

Gallhofer, I. N., and W. E. Saris. 1996. *Foreign policy decision-making: A qualitative and quantitative analysis of political argumentation.* Westport, CT: Praeger.

Gartner, S. S. 1997. *Strategic assessment in war.* New Haven, CT: Yale University Press.

Gellman, B. 2002. A strategy's cautious evolution. *Washington Post,* January 20.

Gilbert, M. J. 2002. *Why the North won the Vietnam War.* New York: Palgrave.

Greenwald, A. G. 1980. The totalitarian ego: Fabrication and revision of personal history. *American Psychologist* 35: 603–618.

Grove, A. S. 1999. *Only the paranoid survive: How to exploit the crisis points that challenge every company.* New York: Currency.

Handel, M. I., ed. 1989. *Leaders and intelligence.* London: Frank Cass and Co.

Hastings, M. 1987. *The Korean War.* London: M. Joseph.

Hayward, S. F. 2001, *The age of Reagan: The fall of the old liberal order.* Roseville, CA: Prima.

Hogan, M. J. 1998. *A cross of iron: Harry S. Truman and the origins of the national security state, 1945–1954.* Cambridge: Cambridge University Press.

Hughes-Wilson, J. 1999. *Military intelligence blunders.* New York: Carroll and Graf.

Iriye, A. 1999. *Pearl Harbor and the coming of the Pacific War: A brief history with documents and essays.* Boston: Bedford/St. Martin's.

Janis, I. L. 1972. *Victims of Groupthink: Psychological studies of policy decisions and fiascoes.* Boston: Houghton Mifflin.

Jervis, R. 1976. *Perception and misperception in international politics.* Princeton, NJ: Princeton University Press.

Jervis, R. 1983. Deterrence and perception. *International Security* 7: 3–30.

Jervis, R. 2003. The confrontation between Iraq and U.S.: Implications for the theory and practice of deterrence. *European Journal of International Relations* 9: 315–337.

Johnson, D. D. P. 2004. *Overconfidence and war: The havoc and glory of positive illusions.* Cambridge, MA: Harvard University Press.

Johnson, D. D. P., and D. R. Tierney. 2004 Essence of victory: Winning and losing international crises. *Security Studies* 13: 350–381.

Johnson, D. D. P., and D. R. Tierney. 2006. *Failing to win: Perceptions of victory and defeat in international politics.* Cambridge, MA: Harvard University Press.

Kahn, D. 1999. Pearl Harbor as an intelligence failure. In *Pearl Harbor and the coming of the Pacific War: A brief history with documents and essays,* ed. A. Iriye, 158–169. Boston: Bedford/St. Martin's.

Kahneman, D., P. Slovic, and A. Tversky. 1982. *Judgment under uncertainty: Heuristics and biases.* Cambridge: Cambridge University Press.

Kaiser, D. 2000. *American tragedy: Kennedy, Johnson, and the origins of the Vietnam.* Cambrige: Harvard University Press.

Klar, Y., D. Zakay, and K. Sharvit. 2002. "If I don't get blown up . . . ": Realism in face of terrorism in an Israeli nationwide sample. *Risk, Decision, and Policy* 7: 203–219.

Kovacs, A. 1997. The nonuse of intelligence. *International Journal of Intelligence and Counter Intelligence* 10: 383–417.

Kuhn, T. S. 1970. *The structure of scientific revolutions.* Chicago: Chicago University Press.

Lashinsky, A. 2006. Chaos by design: The inside story of disorder, disarray, and uncertainty at Google. *Fortune Magazine,* Vol. 154, No. 7, October 2, 2006.

Lebow, R. N. 1981. *Between peace and war: The nature of international crisis.* Baltimore: John Hopkins.

Leigh, A., J. Wolfers, and E. Zitzewitz. 2003. What do financial markets think of war in Iraq? NBER Working Paper 9587. National Bureau of Economic Research, Cambridge, MA.

Levite, A., B. W. Jentleson, and L. Berman. 1992. *Foreign military intervention: The dynamics of protracted conflict.* New York: Columbia University Press.

Levy, J. S. 1994. Learning and foreign policy: Sweeping a conceptual minefield. *International Organization* 48(2): 179–312.

McDermott, R. 2004. *Political psychology in international relations.* Ann Arbor: University of Michigan Press.

Metz, S., and R. Millen. 2004. *Insurgency and counterinsurgency in the twenty-first century: Reconceptualizing threat and response.* Carlisle, PA: U.S. Army War College, Strategic Studies Institute.

Mueller, J. 2005. Simplicity and spook: Terrorism and the dynamics of threat exaggeration. *International Studies Perspectives* 6: 208–234.

Nagl, J. A. 2002. *Learning to eat soup with a knife: Counterinsurgency lessons from Malaya and Vietnam.* Chicago: Chicago University Press.

New Scientist. 2006. Editorial: Kyota in crisis. July 8, 2006, 3.

Perlmutter, A. 1978. Military incompetence and failure: A historical comparative and analytical evaluation. *Journal of Strategic Studies* 1: 121–138.

Perrow, C. 1999. *Normal accidents: Living with high-risk technologies.* Princeton, NJ: Princeton University Press.

Perry, J. M. 1996. *Arrogant armies: Great military disasters and the generals behind them.* New York: John Wiley and Sons.

Petroski, H. 2006. *Success through failure: The paradox of design.* Princeton, NJ: Princeton University Press.

Posen, B. 1984. *The sources of military doctrine: France, Britain, and Germany between the world wars.* Cornell studies in security affairs. Ithaca, NY: Cornell University Press.

Powell, C. 1995. *A soldier's way.* London: Hutchinson.

Rabinovich, A. 2004. *The Yom Kippur War: The epic encounter that transformed the Middle East.* New York: Schocken Books.

Regan, G. 1993. *Snafu: Great American military disasters.* New York: Avon.

Reiter, D. 1996. *Crucible of beliefs: Learning, alliances, and world wars.* Ithaca, NY: Cornell University Press.

Rosenau, W. 2007. U.S. counterterrorism policy. In *How states fight terrorism: Policy dynamics in the West,* ed. D. Zimmermann and A. Wenger, 133–154. Boulder, CO: Lynne Rienner Publishers.

Schacter, D. L., ed. 1995. *Memory distortion: How minds, brains, and societies reconstruct the past.* Cambridge, MA: Harvard University Press.

Schivelbusch, W. 2004. *The culture of defeat: On national trauma, mourning, and recovery.* New York: Picador.

Sears, D. O., L. Huddy, and R. Jervis. 2003. *Oxford handbook of political psychology.* Oxford: Oxford University Press.

Simon, S., and D. Benjamin. 2000. America and the new terrorism. *Survival* 42: 59–75.

Simonsohn, U., N. Karlsson, G. F. Loewenstein, and D. Ariely. 2006. The tree of experience in the forest of information: Overweighing experienced relative to observed information. SSRN Working Paper. Social Science Research Network. October 2006. http//ssrn.com/abstract=521942.

Snyder, J. 1984. *The ideology of the offensive: Military decision making and the disasters of 1914*. Ithaca, NY: Cornell University Press.

Stoessinger, J. G. 1998. *Why nations go to war*. New York: St. Martin's.

Surowiecki, J. 2004. *The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies and nations*. New York: Doubleday.

Tetlock, P. E. 1998. Social psychology and world politics. In *Handbook of Social Psychology,* ed. D. Gilbert, S. Fiske, and G. Lindzey, 868–912. New York: McGraw Hill.

True, J. L. 2002. The changing focus of national security policy. In *Policy Dynamics,* ed. F. R. Baumgartner and B. D. Jones, 155–187. Chicago: University of Chicago Press.

Tuchman, B. 1984. *The march of folly: From Troy to Vietnam*. New York: Alfred A. Knopf.

U.S. Department of Defense. 1971. *The Pentagon papers: United States–Vietnam Relations, 1945–1967*. Washington, DC: U.S. Government Printing Office.

Van Evera, S. 1998. Hypotheses on nationalism and war. *International Security* 18: 5–39.

Van Evera, S. 2003. Why states believe foolish ideas: Non-self-evaluation by states and societies. In *Perspectives on structural realism,* ed. A. K. Hanami, 163–198. New York: Palgrave Macmillan.

Vertzberger, Y. Y. I. 1990. *The world in their minds: Information processing, cognition, and perception in foreign policy decisionmaking*. Stanford, CA: Stanford University Press.

Viola, L., and D. Snidal. 2006. The evolutionary design of international institutions. Working Paper, Program on International Politics, Economics, and Security, University of Chicago, Chicago.

Wirtz, J. J. 1991. *The Tet Offensive: Intelligence failure in war*. Cornell studies in security affairs. Ithaca, NY: Cornell University Press.

Woodward, B. 2005. *State of denial: Bush at war. Part III*. New York: Simon and Schuster.

Paradigm shift. Cloud strategy. Refactor. Rearchitect. Replace. Cloud security. Paradigm shift.Â Microsoft Cloud Security Expert Rob Polly led the security element of the companyâ€™s journey to the cloud to ensure that the company was evolving specifically for cloud security and addressing privacy concerns, geopolitical issues, and data sovereignty regulations. As more and more devices are designed to connect to the intelligent cloud, Microsoft is planning initiatives that will allow us to provide data protection in a device-agnostic, cloud-only ecosystem. Featured content. March 28, 2018. Cloud security with Rob Polly. SEE VIDEO. June 22, 2017.