Strategic Studies Quarterly

An Air Force–Sponsored Strategic Forum on National and International Security

VOLUME 4 FALL 2010 NUMBER 3

Commentary

Feature Article

Perspectives

Book Review Essay

Air Diplomacy

Protecting American National Interests

An American withdrawal from Iraq underway, significant troop reductions in Afghanistan planned for 2011, and the defense budget to begin declining next year—all of these scenarios demand vigorous debate over the future of American engagement in the world. As the Obama administration looks to move away from dependence on hard power, the US Air Force has an opportunity to become a vital diplomatic tool through air diplomacy.

Air diplomacy is a proactive approach to preventing conflict by employing airpower in nonkinetic operations as an instrument of national power. It can be critical in supporting US foreign policy in the years to come. For the Air Force to remain relevant in a dynamic international environment, it must turn away from using an ad hoc and often disparate approach and move toward conducting deliberate diplomatic missions aimed at conflict prevention. The service needs a strategy to guide its diplomatic contribution to national objectives, consolidate its diplomatic missions, and maximize the utility of air diplomacy. After developing the air diplomacy concept, the Air Force should then promote it as a cost-effective alternative to the reactive use of hard power. Air diplomacy can also reduce a large overseas presence while maintaining relationships built over more than half a century.

For air diplomacy to play a leading role in American foreign policy requires a discussion of its strengths and weaknesses. Four questions come to mind: (1) How does the US Air Force conduct air diplomacy? (2) Why is air diplomacy increasingly important? (3) Where does air diplomacy fit on the diplomatic spectrum? and (4) What are the ends, ways, and means of an air diplomacy strategy?

How Does the US Air Force Conduct Air Diplomacy?

The US Air Force has an illustrious history of conducting public, humanitarian, military, commercial, traditional, preventive, coercive, and deterrence diplomacy. Dating to the earliest days of aviation, decision makers have employed airpower for diplomatic purposes—and that practice is unlikely to change. Thus, presenting air diplomacy as an option

to policymakers bodes well for the Air Force in the future as it seeks to play a part in the success of American foreign policy. Some past examples of the diplomatic use of airpower illustrate the breadth of the Air Force's contribution to furthering the national interest.

Air Diplomacy: Public

When aviation enthusiasts within the Army first attempted to convince its leaders, the Congress, and the American people that aviation deserved their support, they undertook a large-scale public diplomacy campaign. In perhaps the earliest example of air diplomacy, members of the fledgling Aviation Section sent its small fleet of aircraft on a successful cross-country tour in 1910, eventually leading to widespread support for military aviation. Throughout the first three decades of its existence, the Army's Aviation Section (1914–18), Air Service (1918–26), and Air Corps (1926–41) became adept at conducting diplomacy at home, as leading aviators such as Brig Gen William "Billy" Mitchell and Maj Gen Mason Patrick worked tirelessly to increase the budget and prestige of military aviation.

Well before the establishment of an independent air force, the Army Air Corps conducted what may well have been the first overseas air diplomacy mission. In an effort to showcase the new B-17, demonstrate American power, and counterbalance growing German and Italian influence in Latin America, six B-17s under the command of Lt Col Robert Olds flew a public diplomacy mission to Buenos Aires for the inauguration of Pres. Roberto Ortiz in February 1938. This mission established an engagement between the US Air Force and Latin American air forces that continues today. Other such missions include regularly participating in international air shows, hosting international conferences, transporting foreign dignitaries and media aboard Air Force aircraft, and regularly conducting "show the flag" flights to foreign locales. Perhaps the 89th Airlift Wing carries out the most well-known US Air Force public diplomacy mission by flying Air Force One, certainly one of the most widely recognized symbols of the United States in the world.

Air Diplomacy: Humanitarian

Humanitarian diplomacy is a particular specialty of the US Air Force because of the speed with which it can respond to a crisis. For example, during the Berlin airlift (24 June 1948–12 May 1949)—perhaps the best-known relief operation in American history—the Air Force provided vital

food, water, and fuel to the people of West Berlin. Initially led by United States Air Forces in Europe, the operation included Airmen from the United States, Britain, and the Commonwealth, who supplied Berlin with more than enough necessities for survival. Operation Vittles managed to deliver 13,000 tons of fuel and provisions per day. A resounding success, the Berlin airlift highlighted the ability of the Allies to provide humanitarian assistance on a massive scale while avoiding a conflict between the United States and the Soviet Union.

More recent examples of US Air Force participation in humanitarian diplomacy include Operations Provide Hope (1992–94) in the former Soviet Union, Provide Promise (1992–96) in Bosnia-Herzegovina, and Support Hope (1994) in Rwanda. After a 7.9-magnitude earthquake struck a remote region of Sichuan Province, China, on 12 May 2008, two US Air Force C-17s deployed from Hickam AFB, Hawaii, and Elmendorf AFB, Alaska, with desperately needed relief supplies, arriving on 18 May. Joint Task Force Port Opening is assisting with relief to victims of the 2010 Haitian earthquake. Because of its ability to deploy rapidly to locations around the world, the Air Force is undoubtedly the United States' best tool for providing immediate assistance. These relatively low-cost diplomatic missions build goodwill with governments and citizens around the globe.

Air Diplomacy: Military, Commercial, and Traditional

In recent years, the Departments of Defense and the Air Force have formulated plans for conducting a combination of military, commercial, and traditional diplomacy—*Building Partnership Capacity: QDR Execution Roadmap* (2006) and *United States Air Force Global Partnership Strategy* (2008), respectively. However, current efforts are not the first for the Air Force. During World War II, the Army Air Forces equipped Britain and the Allies with a number of aircraft and supplies under the auspices of the Lend-Lease Program (1941–1945).

Current efforts often fall within the "train, advise, and equip" realm of military diplomacy. Although the sale of weapons systems to foreign governments—through an embassy's office of defense cooperation—often receives the most attention, commercial diplomacy is limited in scope. Traditionally, the US Air Force directs most of its effort toward training and assisting foreign air forces, as through the Inter-American Air Forces Academy (IAAFA) at Lackland AFB, Texas. By offering Latin American officers and enlisted members a range of training courses in their native

language, the IAAFA assists in creating professional air forces in the region, strengthening ties between the United States and Latin America, and building relationships with future Latin American leaders. Officers who attend the IAAFA may also receive additional US professional military education, giving the best officers a stronger grounding in the skills necessary to lead a professional air force, one capable of operating jointly with the US Air Force. These officers also find themselves more adept at correctly reading the many cultural and linguistic nuances of US diplomatic signals.

Air Diplomacy: Preventive

During Operations Provide Comfort and Northern Watch (1991–2003), the Air Force conducted preventive diplomacy by protecting Kurds in northern Iraq from Saddam Hussein's depredations and was an overwhelming success. Similarly, in Operation Southern Watch (1992–2003), it denied Saddam's regime the use of airspace south of the 33rd parallel in an effort to protect the Shia from further atrocities. Although not completely successful in this regard, it did prevent the Iraqi air force from using airpower in the south.

Air Diplomacy: Coercive

When incentive-based diplomacy cannot fulfill American objectives, the nation often calls upon the Air Force to conduct coercive diplomacy, which can sometimes straddle the line between diplomacy and force. Operations such as El Dorado Canyon (1986), Deliberate Force (1995), and Allied Force (1999) are examples of airpower serving both purposes. During the Cuban missile crisis (1962), however, the Air Force conducted coercive diplomacy that did not blur the line between diplomacy and force. Soon after the crisis began in mid October, Strategic Air Command (SAC) deployed a large number of its nuclear-armed bombers to Florida and the southeastern United States. At Florida Air Force bases such as Homestead, MacDill, and McCoy, B-47s sat wingtip to wingtip, waiting to drop their nuclear payloads on Cuba. Aware of SAC's redeployment of nuclear bombers, among other efforts, the Soviet leadership backed down.

Air Diplomacy: Deterrence

For more than 60 years, nuclear deterrence has played a central role in shaping the composition and culture of the Air Force. By maintaining a fleet of nuclear-capable bombers and intercontinental ballistic missiles—

along with the US Navy's submarine-launched ballistic missiles—the United States has successfully deterred nation states from attacking the American homeland with conventional or nuclear weapons. Additionally, conflicts that may have otherwise escalated were kept in check by the fear that limited war could become nuclear. Undoubtedly, the nuclear arsenal is a key tool of American diplomacy.

Why Is Air Diplomacy Increasingly Important?

Air diplomacy is likely to become an increasingly important capability of the US Air Force in the years ahead for three principal reasons. First, entitlement spending will continue to consume a larger portion of the federal budget. Second, the service is unlikely to receive the acquisition dollars required to maintain its current, hard-power capabilities. Third, airpower is less resource intensive and can respond to a changing security environment with a level of speed and flexibility unmatched elsewhere.

"Guns versus Butter"

Increasing entitlement demands will soon force defense spending to decline. As baby boomers retire and an increasing number of able-bodied Americans come to depend on the government for basic necessities, pressure will mount on Congress and the president to increase entitlement spending. This problem is presenting itself sooner than expected. For example, despite predictions of Social Security's insolvency no sooner than 2016, the Social Security Administration's chief actuary recently announced that entitlement outlays will exceed payroll taxes in 2010. An unprecedented one in six Americans depends upon the government for some or all basic necessities. If economic indicators are correct, discretionary spending (e.g., defense spending) will decline, as a percentage of the federal budget, at an accelerated rate that exceeds the decline of the past half century. Air diplomacy may prove an effective approach to partially addressing and preventing the adverse impact of a declining defense budget.

Projected spending will increase steeply for just three entitlement programs: Social Security, Medicare, and Medicaid (fig. 1). Projections indicate that the recently passed health care reform bill (H.R. 4872) will add $1 trillion dollars of entitlement spending over the coming decade—likely a low estimate.

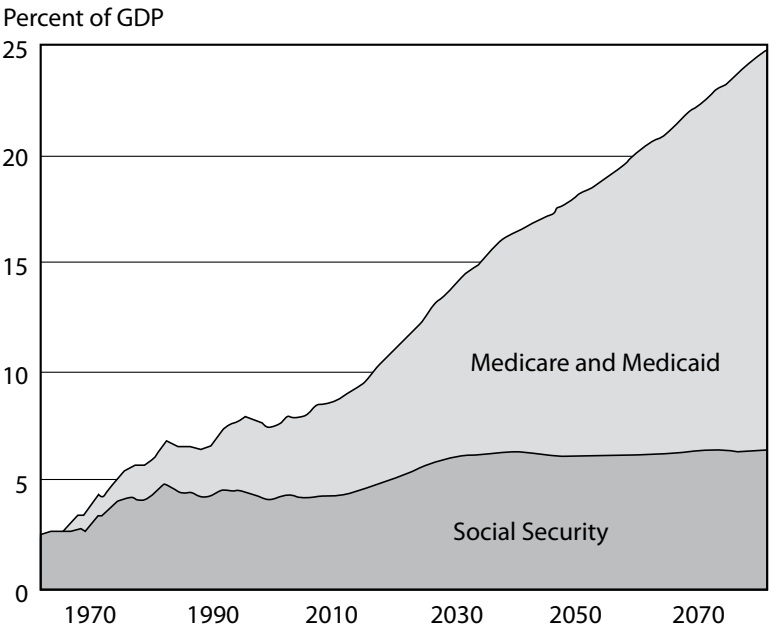

Figure 1. Long-run federal spending on Social Security, Medicare, and Medicaid, CY 1962–2082 (extended baseline)

Source: Congressional Budget Office, *Long-Term Budget Outlook* (Washington: Congressional Budget Office, December 2007), table 1.1.

Thus, one may reasonably suggest that the future of defense spending in the United States *may* soon resemble that of Europe, where most North Atlantic Treaty Organization members struggle to meet the 2 percent of GDP minimum requirement for defense spending. The federal government cannot spend more than it generates in revenue indefinitely. And, as scholarship suggests, there is an inverse relationship between tax rates and economic growth.

Because air diplomacy is less resource and manpower intensive—on average—than the use of hard power, it presents an attractive option for a fiscally constrained military and political leadership. It also enables greater flexibility in its conduct. During flush economic times, air diplomacy can easily expand, while during an economic downturn, air diplomacy missions can be reduced. The sunk costs of overseas bases and the need to win ongoing conflicts do not allow such flexibility. For example, the average annual cost of maintaining a single Soldier in Afghanistan is $500,000. At an annual cost of $30 billion, the Afghanistan war is far more expensive than any air diplomacy alternative. Focusing on conflict prevention through strong diplomatic efforts presents an opportunity to preserve limited resources for circumstances that demand hard power. Air diplomacy offers a proactive

approach to this problem by employing airpower for the purpose of building and strengthening partnerships with current and prospective allies while preventing conflicts.

Acquisition Armageddon

An examination of prospective defense spending presents some serious difficulties for acquisition programs. Forecasts of slowing economic growth and declining defense spending suggest that future Air Force budgets will also decline. Thus, they are unlikely to include sufficient acquisition funding to replace aging platforms. Arguably, this deficit will make it difficult for the Air Force to maintain current combat capabilities, even as next-generation systems enter service. The potential for a decline in hard power is exacerbated by three problems. First, rapidly increasing per-aircraft procurement costs make the fiscal cost of replacing current *capabilities* unsustainable. Although next-generation platforms are more capable, quantity has a quality all its own. Second, acquisition budgets may also face pressure from increasing personnel costs, which Secretary Gates recently addressed. The cost of each service member is increasing at an alarming rate. Third, maintaining aging platforms, as Congress is mandating, places a greater burden on the Air Force's operations and maintenance (O&M) budget. Thus, conflict prevention—the focus of air diplomacy—becomes ever more important, as it offers a way to defend national interests at a lower cost.

A decline in defense spending is likely, based on President Obama's budget submissions (fig. 2).

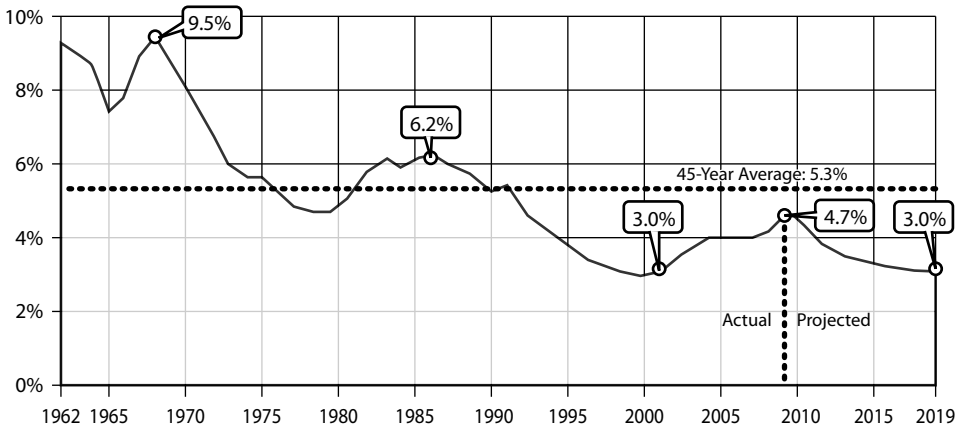

Figure 2. Defense spending as a percentage of gross domestic product

Source: Heritage Foundation, "Obama's Budget Would Reduce National Defense Spending," http://www.heritage.org/BudgetChartbook/obama-budget-defense-spending.

A reduction in defense spending from 4.5 to 3.0 percent of the gross domestic product will present difficulty for every service. The "procurement holiday" of the 1990s plus 20 years of elevated aircraft utilization rates—Operations Desert Shield/Desert Storm (1990–91), Northern Watch (1992–2003), Southern Watch (1992–2003), Joint Endeavor (1995–96), Allied Force (1999), Enduring Freedom (2001–present), and Iraqi Freedom (2003–present)—have exacerbated the problem. Combining the effects of declining budgets and the need to replace worn-out aircraft easily illustrates how these issues can prove particularly difficult for the Air Force. This problem is occurring just as the service is attempting to develop and field several new airframes. Moreover, a sense of the Congress suggests that it will not allocate funds needed by the Air Force to meet projected acquisition requirements. Even if next-generation aircraft are more capable than those they replace, combat capability will likely decline.

Speed, Flexibility, and Limited Footprint

Air diplomacy is likely to become more important because of the speed, flexibility, and limited footprint of airpower. The US Army's dominance in military decision making during America's involvement in Afghanistan and Iraq over the past decade has left the nation focused on the use of hard power. The ground-centric nature of these two conflicts provided the leverage needed by the Army to reassert itself after a long period of perceived subservience to the Air Force. As the president looks for an alternative to current strategy, air diplomacy will seem an attractive choice.

Simply stated, air diplomacy is an effective way of defending vital national interests, building necessary partnerships, preventing conflict, and expanding American influence without creating the anti-American sentiment that often accompanies thousands of boots on the ground. Practicing air diplomacy deliberately and coherently has greater potential to effectively leverage the capabilities of the Air Force in the interests of the nation than the current approach.

One obvious point argues against further development of air diplomacy as an Air Force capability, however—the contention that it does not fall within the service's core mission. On the contrary, air diplomacy is a more complete conceptualization of "building partnerships," currently one of 12 Air Force core functions. As currently understood, building partner-

ships fails to encompass many Air Force missions that would fall within air diplomacy. Every service builds partnerships, but only the Air Force conducts air diplomacy.

Although the Air Force prepares—in peacetime—to fight the nation's wars, preventing war is equally desirable. Air diplomacy is a primary contributor to that mission.

Where Does Air Diplomacy Fit on the Diplomatic Spectrum?

Generally associated with peaceful relations between states, diplomacy nevertheless comes in many forms. States use diplomacy to promote economic interests (trade), protect citizens abroad, propagate culture and ideology, enhance national prestige, promote friendship, and isolate adversaries. Moreover, diplomacy is certainly a less expensive way to exercise power in international affairs. Diplomacy is one of two primary elements of foreign policy, the other being war. Both diplomacy and war are means to an end rather than ends in themselves.

Dividing diplomacy into two broad groups—incentive-based and threat-based—may offer additional clarity. On the one hand, incentive-based diplomacy does not rely on the threat of force for success. Rather, it succeeds when states engaged in diplomatic negotiations reach a mutually beneficial agreement. On the other hand, threat-based diplomacy relies on coercive means, such as the threat of force or sanctions. For the United States, the use of incentive-based diplomacy is likely to increase as the Obama administration may well signal a clear shift away from the use of hard power. This policy will give the US Air Force an opportunity to play a greater role in the conduct of soft power or, more specifically, incentive-based diplomacy.

Diplomatic theory and practice suggest that states typically conduct 13 types of diplomacy, each differentiated by the means employed and the ends sought. Although the types of diplomacy vary to a significant degree, their methods and objectives are not necessarily mutually exclusive. A description of each type of diplomacy clarifies corresponding examples of air diplomacy.

Incentive-Based Diplomacy

Traditional diplomacy relies on a professional diplomatic corps that applies intelligence and tact to the conduct of official relations between the governments of independent states. *Commercial diplomacy* focuses on securing trade agreements that promote the economic interests of individuals, corporations, and industries (public or private) believed to support national interests. It is designed to influence the policies of foreign governments with respect to regulatory decisions, foreign direct investment, and trade. *Conference diplomacy*, dating back to the Concert of Europe, is most widely known for its reliance on international committees such as the United Nations. *Public diplomacy*, according to Amb. Christopher Ross, "articulate[s] U.S. policy clearly in as many media and languages as are necessary to ensure that the message is received." *Preventive diplomacy*, coined by Dag Hammarskjöld in the introduction to the *15th Annual Report* (1960) of the UN General Assembly, seeks to deescalate tensions by negotiating a resolution to grievances through an impartial arbiter. *Resource diplomacy* emphasizes the acquisition of four vital interests: food, energy, water, and minerals. *Humanitarian diplomacy*, developed in the aftermath of World War II, is often designed to aid at-risk populations after a natural or manmade disaster by providing food, shelter, clothing, and security. *Protective diplomacy* aims to provide physical protection to citizens abroad or to groups of civilians (ethnic or religious minorities, tribal groups, etc.) that may face persecution or find themselves in harm's way.

Threat-Based Diplomacy

Totalitarian diplomacy is marked by its forceful, inflexible, and seemingly irrational nature—propaganda and deception serving as two primary tools of conduct. As the example of North Korea illustrates, totalitarian diplomacy can often take the form of threats to members of the international community or to stability within the international system. According to James Willard, *military diplomacy* is "the conduct by military diplomats of negotiations and other relations between nations, nations' militaries, and nations' citizens aimed at influencing the environment in which the military operates." *Coercive diplomacy* applies the threat of violence in a manner and magnitude sufficient to persuade an opponent to cease aggression without requiring the actual use of violence.

Anne Sartori best describes *diplomacy by deterrence* as "the use of a particular subset of language—deterrent threats—to attempt to convey the

information that a state is willing to fight over a disputed issue or issues. Thus, deterrent threats are a form of diplomacy." Former secretary of state Condoleezza Rice describes *transformational diplomacy* as a multinational effort to build and sustain democracy while developing well-governed and responsible states.

This brief discussion of modern diplomacy places the US Air Force's specific contributions to the conduct of diplomacy in the proper context. In reality, airpower is a dual-use capability equally adept at producing threat-based diplomacy and kinetic effects on the battlefield or preventing conflicts through incentive-based diplomacy.

What Are the Ends, Ways, and Means of an Air Diplomacy Strategy?

Turning the previous conceptual discussion into a viable service strategy is a difficult task. However, if those approximate descriptions of the future fiscal, political, and security environment are correct, then developing an air diplomacy strategy is worth the effort. Examining its development in terms of ends, ways, and means offers a useful framework.

Ends

The ends (objectives) of an air diplomacy strategy should focus on three central tenets. First, the strategy should develop cost-effective approaches to building and maintaining partnerships with current or prospective allies. By doing so, the United States will expand the number of potential partners available for support during a future conflict. Second, the strategy should develop proactive approaches to engaging with current or prospective adversaries (e.g., China, Iran, North Korea, and Venezuela) for the specific purpose of addressing contentious issues without resorting to the use of hard power. Not all adversaries can be persuaded to alter their behavior through diplomacy, but it should always remain a method of first resort. Third, the strategy should consolidate the disparate diplomatic missions conducted across the service. Currently, the Air Force lacks a unifying strategy capable of effectively leveraging a wide array of its missions.

Ways

Ways, or "the methods that the organization uses to achieve those ends," are perhaps more difficult to develop than are the ends. Although

the following list is not complete, some of the recommendations may prove useful in developing the "ways" of an air diplomacy strategy.

First, incorporating existing strategies, programs, plans, and approaches related to air diplomacy will simplify the process of creating a service strategy. For example, the Air Force's strategy for building partnerships and the DoD *Report on Strategic Communication* represent a useful starting point for a larger air diplomacy strategy.

Second, it is important to know where air diplomacy begins and ends. Like all other tools for conducting foreign policy, it has strengths and weaknesses. Air diplomacy differs from the Air Force's destructive capabilities in the same way that soft power differs from hard power. Discussing air diplomacy's contribution to preventing conflict may provide a sufficient rationale for its use as an alternative to hard power.

Third, an air diplomacy strategy must give clear direction to the service, enabling the chief of staff to carry out his responsibilities for organizing, training, and equipping so the Air Force can present the combatant commander with forces prepared to conduct a range of diplomatic missions. The employment of force (planes and personnel) particularly deserves consideration in an air diplomacy strategy. Adapting the air and space expeditionary force construct may provide an adequate dual-use capability with the needed flexibility to fight a major conflict or conduct air diplomacy.

Fourth, the Air Force must actively promote air diplomacy as an alternative approach in foreign policy. A seamless transition from the use of hard power (Afghanistan and Iraq) to soft power (air diplomacy) will have great appeal over the next two years. The Obama administration is looking for a distinct alternative to the present strategy. An approach to foreign policy that demands less American blood and treasure, with a smaller overseas presence, while offering greater flexibility, may well generate a strong attraction in the wake of a major conflict. Air diplomacy has the potential to be that alternative, if properly employed.

Means

The means required to develop an air diplomacy strategy are straightforward. Four components within the Air Force should share principal responsibility for creating a service-wide strategy—with other components also playing an important role. The office of the secretary of the Air Force for international affairs, which has already developed the *United States*

Air Force Global Partnership Strategy and directs a large number of commercial, military, traditional, and public diplomacy missions, is a logical choice to lead the effort. Because Air Mobility Command supplies critical airlift for humanitarian and other diplomatic missions, it deserves a role in the strategy development process. Global Strike Command merits inclusion in the process by virtue of its responsibility for deterrence. Finally, Air Combat Command provides the combat forces required to conduct preventive and coercive diplomacy, so any air diplomacy strategy would be incomplete without its participation.

Conclusion

One criticism the air diplomacy concept is certain to face is that it usurps the State Department's principal role. This is not the intent. In the end, the wide range of missions regularly performed by Airmen makes airpower an attractive option for building partnerships, assuring allies, and dissuading enemies. Leveraging existing capabilities by developing an air diplomacy strategy that can, for example, serve as part of a post–Afghanistan/Iraq War foreign policy is in the best interest of the nation and the Air Force. With defense spending likely to decline, the service must innovate or face becoming irrelevant. The Air Force is uniquely positioned to offer the president a clear course through what are likely to be turbulent skies.

Adam B. Lowther, PhD
Air Force Research Institute

Guidelines for Nation Builders

James F. Dobbins

Nation building, as commonly understood in the United States, involves the use of armed force as part of a broader effort to promote political and economic reforms with the objective of transforming a society emerging from conflict into one at peace with itself and its neighbors. In recent years the frequency of such operations has greatly increased. During the Cold War, the United States embarked upon a new military intervention on the average of about once a decade, while the United Nations launched a new peacekeeping mission on the average of once every four years.[1] Few of these US– or UN–led operations developed into full-blown nation-building missions. Since the end of the Cold War, the pace of American military interventions has risen to about one every two years, while the frequency of new UN peacekeeping missions is up to nearly one every six months. The duration of these missions has also risen, most now lasting five to 10 years. The effect is thus cumulative. The United States finds itself manning three or four such interventions simultaneously, while the United Nations must manage up to two dozen different missions at the same time.

The character of these undertakings has also evolved. During the Cold War, UN troops were usually deployed to separate combatants, police demilitarized zones, or monitor cease-fires. In recent years, the objectives for these missions have expanded to include reuniting divided societies, disarming adversaries, demobilizing former combatants, organizing elections, installing representative governments, and promoting democratic reform and economic growth. American-led operations have also become larger, longer, and more ambitious in scope.

Even with some notable setbacks, the overall impact of this heightened international activism has been beneficial. International military interven-

---

Amb. James F. Dobbins directs RAND's International Security and Defense Policy Center. He has held high-level posts in the State Department and in the White House, including ambassador to the European Community, and has handled a variety of crisis management assignments in the Clinton administration and as the Bush administration's first special envoy for Afghanistan. He is lead author of the three-volume *RAND History of Nation-Building* and *Occupying Iraq: A History of the Coalition Provisional Authority*.

tions have proved to be the best and, indeed, the only reliable means of preventing societies emerging from civil war from slipping back into conflict.[2] Since the end of the Cold War, the number of civil wars around the world has been more than cut in half. The number of people being killed, maimed, or driven from their homes as a result of armed conflict has also dropped even further.

Despite this wealth of experience, the American occupation of Iraq was marked by a myriad of unforeseen challenges and hastily improvised responses. Observers might be forgiven for thinking the United States had never mounted such an operation. Yet Iraq was the seventh major American-led intervention in little more than a decade, preceded by operations in Kuwait, Somalia, Haiti, Bosnia, Kosovo, and Afghanistan. Of those seven societies, six are Muslim, Haiti being the sole exception. At the commencement of the Iraq occupation, therefore, no Western military had more modern experience operating in Muslim societies than the US Army, and no country had more experience managing large nation-building enterprises than the United States of America.

Unfortunately, neither the American military nor the government as a whole had made a systematic attempt over the preceding decade to reflect upon the experience of those earlier operations and apply those lessons in preparing for what was likely to be the biggest and most difficult such challenge to date, in Iraq. This attitude has changed. In response to initial setbacks in Iraq and Afghanistan, the Bush and now Obama administrations have begun to put in place institutional arrangements designed to ensure a more professional approach to future such contingencies. In 2005 the Defense Department issued a directive making *stability operations*, its term for nation building, a core mission of the American military, on par, in principal at least, with preparation for major combat. At about the same time the State Department established the Office of the Coordinator for Reconstruction and Stabilization to oversee the civilian aspects of nation-building-type missions. More recently, President Obama released a new *National Security Strategy* that emphasizes the need to host security and reconstruction in the aftermath of conflict and sets out a "whole of government" approach to doing so.

Other governments, notably the British, Canadian, and German, have set up similar structures. The United Nations has established the Peace Building Commission for the same purpose. These various initiatives and new strategies are all premised on the view that nation building is still an

unavoidable burden and that concepts presented here still apply. Practitioners must do a better job applying the lessons from prior missions into an evolving doctrine for future ones. They must better integrate military and civilian efforts across multiple agencies as well as across national and international lines; and build cadres of experts available to go from one operation to the next.

Nation-Building Providers

There are a variety of providers for nation-building missions. Since 1989, the United States has led coalitions of the willing into Somalia, Haiti, Afghanistan, and Iraq. NATO mounted its first such mission in 1995 in Bosnia, went into Kosovo in 1999, and into Afghanistan in 2004. The European Union sent its first military force abroad to Macedonia in 2003 and has since conducted larger peacekeeping operations in the Democratic Republic of the Congo and in Chad. The EU also replaced the NATO peacekeeping force in Bosnia with one of its own in 2005. The African Union has become the "peacekeeper of last resort" for that continent, assuming responsibilities for operations too risky for anyone else. Finally, the UN has conducted the largest number of such missions. As of this writing, more than 100,000 blue-helmeted soldiers and police are deployed in 16 UN–led peacekeeping missions around the world.

Each of these institutions has its own strengths and weaknesses. The UN has the widest experience; NATO has the most powerful forces; the EU has the most developed array of civil competencies, and the African Union is the least risk averse. The United Nations has the most widely accepted legitimacy and the greatest formal authority. Its actions, by definition, enjoy international sanction. Alone among international organizations, it can require financial contributions even from those opposed to the intervention in question. The United Nations has the most straightforward decision-making apparatus and the most unified command and control arrangements. The UN Security Council is smaller than its NATO, EU, or AU equivalents and is the only one making all decisions by qualified majority—only five of its members have the capacity to block decisions unilaterally.

Once the Security Council determines the purpose of a mission and decides to launch it, further operational decisions are left largely to the secretary-general and his professional staff, at least until the next Security

Council review, generally six months hence. In UN operations, the civilian and military chains of command are unified and integrated, with unequivocal civilian primacy and a clear line of authority from the UN secretary-general through the local civilian representative to the local force commander.

The UN is also a comparatively efficient force provider. In its specialized agencies, it possesses a broad panoply of civil as well as military capabilities needed for nation building. All UN–led operations are planned and directed by a few hundred military and civilian staffers at UN headquarters in New York. Most UN troops come from developing countries whose costs per deployed soldier are a small fraction of those of any Western army.

NATO, by contrast, is capable of deploying powerful, heavily equipped, highly mobile forces and of using them to force entry where necessary. But NATO has no capacity to implement civilian activities; it depends on the United Nations, the European Union, and other institutions and nations to perform all the nonmilitary functions essential to the success of any nation-building operation. NATO decisions are by consensus; consequently, all members have a veto. Whereas the UN Security Council normally makes one decision with respect to any particular operation every six months and leaves the secretary-general relatively unconstrained to carry out that mandate during the intervals, the NATO Council's oversight is more continuous, its decision making more incremental. Member governments consequently have a greater voice in operational matters, and the NATO civilian and military staffs and local commanders have correspondingly less.

Like NATO, and unlike the UN, EU decision making in the security and defense sector is by consensus. The European Union has a much leaner military and political staff than NATO, in part because it can call on NATO if it chooses for planning or other staff functions. The EU, like the UN but unlike NATO, can draw upon a wide array of civilian assets essential to any nation-building operation. Like NATO soldiers, EU soldiers are much more expensive than their UN counterparts. EU decision-making mechanisms, like those of NATO, offer troop-contributing governments more scope for micromanaging military operations on a day-to-day basis than do the UN's.

The African Union disposes of the least-capable military forces and the least-developed capacity for its command, control, and sustainment. The

organization is completely reliant on non-African donors to finance its peacekeeping activities. In practice this means that while the United States and Europe foot about half the bill for UN peacekeeping, they end up paying nearly 100 percent of the AU's peacekeeping costs.

The AU does possess one advantage. Its members are those most affected by the conflicts in what is the world's most conflict-prone region. Proximity means these states get the bulk of refugees, criminality, terrorism, disease, and commercial disruption that comes from having a failed state on their doorstep. As a result of this vulnerability, AU member governments are often ready to move faster and under more discouraging conditions than are those who dominate the more capable but more distant organizations like the EU, NATO, or the UN. This willingness to go where others fear to tread has led to a rather perverse division of labor in which the most powerful peacekeeping provider (NATO) is completely unengaged in Africa; the second most powerful (the EU) does only the easiest of missions, most recently in Chad; and the UN does most of the rest, leaving the least-capable organization to deal with the most hopelessly difficult situations—to wit Somalia and, until recently, Darfur.

The US and UN Ways of Nation Building

The American approach to these missions differs considerably from that of the United Nations, reflecting its different character and capabilities. The United Nations is an international organization entirely dependent upon its members for the wherewithal to conduct nation building. The United States is the world's only superpower, commanding abundant resources of its own and having access to those of many other nations and institutions.

When compared to US–organized efforts, UN operations have almost always been undermanned and underresourced. This is not because UN managers believe smaller is better, although some do, but because member states are rarely willing to commit the manpower or the money any prudent military commander would desire. As a result, small, weak UN forces are routinely deployed into what they hope, on the basis of best-case assumptions, will prove to be postconflict situations. Where such assumptions prove ill founded, UN forces have had to be reinforced, withdrawn, or, in extreme cases, rescued.

Throughout the 1990s the United States adopted the opposite approach to sizing its nation-building deployments, basing its plans on worst-case

assumptions and relying upon an overwhelming force to quickly establish a stable environment and deter resistance from forming. In Somalia, Haiti, Bosnia, and Kosovo, US–led coalitions originally intervened in numbers and with capabilities that discouraged even the thought of resistance. When American force was quickly drawn down in Somalia, the resultant casualties reinforced the Clinton administration's determination to establish and retain a substantial overmatch in its future nation-building operations.

Unfortunately, George W. Bush's administration did not initially follow this precedent. In the aftermath of the September 2001 terrorist attacks, US tolerance of military casualties significantly increased. In sizing its stabilization operations in Afghanistan and Iraq, the new American leadership abandoned the strategy of overwhelming preponderance (sometimes labeled the Powell Doctrine after former chairman of the Joint Chiefs of Staff Gen Colin Powell) in favor of the "small footprint" or "low profile" force posture that had previously characterized UN operations.

The United States slowly improved at nation building throughout the 1990s. The Haitian operation was better managed than Somalia, Bosnia better than Haiti, and Kosovo better than Bosnia. This learning curve was not sustained into the current decade. The Bush administration was initially disdainful of nation building, viewing it as an unsuitable activity for US forces. When compelled to engage in such missions, first in Afghanistan and then in Iraq, the administration sought to break with the strategies and institutional responses that had been honed throughout the 1990s to deal with these challenges. The result, in both cases, was a failure to translate rapid and overwhelming conventional military victories into enduring peace.[3]

In both cases the initially small American-led forces proved unable to establish a secure environment. Spoiler elements were not deterred; they were instead given time and space to organize violent resistance movements. In both cases the original US force levels have had to be significantly increased, but not before what might have been conducted as robust peace-enforcement missions evolved into full-scale counterinsurgency operations.

The United Nations has largely avoided the institutional discontinuities that have marred US performance. UN nation-building missions have been run over the past 20 years by an increasingly experienced cadre of international civil servants. Similarly in the field, many peacekeeping operations are headed and staffed by veterans of earlier operations. Only in the last couple of years has the US government begun to establish its own doc-

trine for the conduct of nation-building endeavors (labeled stabilization and reconstruction missions in official USG jargon) and started to build a cadre of professionals prepared to serve in one such endeavor after another.

It would appear that the low-profile, small-footprint approach to nation building is much better suited to UN–style peacekeeping—where there is a preexisting peace settlement and an invitation by the parties for third-party intervention—than to the more demanding US–style peace enforcement. The United Nations has an ability to compensate, to some degree at least, for its "hard power" deficit with "soft power" attributes of international legitimacy and local impartiality. The United States does not have such advantages in situations where it is a party to the conflict being terminated or where it has acted without an international mandate. Military reversals also have greater consequences for the United States than the United Nations. To the extent that UN influence depends more upon the moral than the physical, more upon its legitimacy than its combat prowess, military rebuffs do not fatally undermine its credibility. To the extent that America leans more on hard rather than soft power to achieve its objectives, military reverses strike at the very heart of its potential influence.

The United Nations and the United States also tend to enunciate their nation-building objectives very differently. UN mandates are highly negotiated, densely bureaucratic documents. UN spokespersons tend toward understatement in expressing their goals. Restraint of this sort is more difficult for US officials, who must build congressional and public support for costly and sometimes dangerous missions in distant and unfamiliar places. As a result, American nation building rhetoric tends toward the grandiloquent. The United States often becomes the victim of its own rhetoric when its higher standards are not met.

Thus UN–led nation-building missions tend to be smaller than American, take place in less-demanding circumstances, are more frequent and therefore more numerous, and define their objectives more circumspectly. By contrast, American-led nation building has taken place in more-demanding circumstances, has required larger forces and more robust mandates, has received more economic support, has espoused more ambitious objectives, and has sometimes encountered greater resistance.

Whether a UN–led peacekeeping mission or a US–led peace enforcement operation, there are certain broad guidelines, or best practices, which the experience of the past 20 years strongly suggests be adopted.[4]

Mission Planning

Planning is a routine military activity, but one less developed among civilian authorities. The lead up to most nation-building missions affords ample time for detailed planning, and this should involve both the civilian as well as military components of the mission. Among the first issues to be addressed are the mission's objective, the intended scale of commitment, and the institution arrangements for managing the intervention.

Setting the mission objective requires looking beyond its immediate purposes to appreciate the impact an external military intervention will have both upon the society in question and the surrounding region. It also requires plotting an outcome commensurate with the likely scale of commitment.

Most interventions are launched for some immediate, usually negative purpose, such as to halt aggression, civil war, famine, genocide, or the proliferation of weapons of mass destruction. This purpose may be achieved quite quickly, but the intervening authorities will then be left with the more difficult, time-consuming, and expensive task of refashioning the society in which it has intervened. The intervention itself will change power relationships within that society and among its neighbors. Those advantaged by the intervention may begin to abuse their positions. Those disadvantaged may move to frustrate the intervening authorities' purposes.

Co-option versus Deconstruction

Broadly speaking, there are two alternative approaches to instigating reforms that can turn a violent society into one at peace with itself and its neighbors. One might be labeled *co-option*, under which the intervening authorities try to work within existing institutions and to deal, more or less impartially, with all social forces and power centers to redirect their ongoing competition for power and wealth from violent to peaceful channels. The alternative approach might be labeled *deconstruction*, under which the intervening authorities first dismantle an existing state apparatus and then build a new one, in the process consciously disempowering some elements of society and empowering others.

Most UN peacekeeping operations aspire to the first approach. Most American-led peace enforcement missions are compelled to adopt something closer to the second. A near-perfect exemplar of the co-option strategy would be the UN mission in El Salvador in the early 1990s. The embodiment of deconstruction would be the American-led occupation of

Germany in the late 1940s. Most missions fall somewhere between these poles. Peacekeeping, impartiality, and co-option are clearly the less-costly approach. But peacekeeping alone will not halt aggression, civil war, genocide, or nuclear proliferation. At best, it can prevent their reoccurrence. Nor can the intervening power remain impartial in conflicts to which it has become party.

Where to position any given intervention along this spectrum from deconstruction to co-option depends not just upon the needs of the society being refashioned but also on the resources the intervening authorities are willing to commit to that task. The more sweeping a mission's objectives, the more resistance it is likely to inspire. Resistance can be overcome, but only through a well-considered application of manpower and money over extended periods of time. In planning any mission, therefore, it is essential to ensure a match between ends and means. Missions that aim to impose peace upon unwilling parties and alter long-standing power relationships are likely to require much greater resources than operations designed to perpetuate existing truces while drawing contending factions into peaceful, but potentially mutually advantageous, power-sharing relationships.

Mismatches between inputs, as measured in manpower and money, and desired outcomes, as measured in imposed social transformation, are the most common causes for nation building to fail. In estimating the resource demands of such operations, this study provides ranges that encompass both approaches. The intent is to allow those planning the missions to increase the necessary manpower and money if committed to promoting sweeping change, or to dial down the objective if resources are likely to be limited.

Institutional Frameworks and Consultative Forums

All nation-building missions involve a mix of national, multinational, and international actors. The nature of that mix is largely determined by the purpose and scope of the operation. Even nationally led interventions, such as the American invasion of Iraq or the Australian intervention in the Solomons, quickly find roles for other national partners, for the United Nations, and for other organizations. At the other end of the spectrum, no UN–led mission is likely to get very far without the cooperation of regional states and the backing of major powers.

The United Nations provides the most suitable institutional framework for most nation-building missions, one with a comparatively low

cost structure, a comparatively high success rate, and the greatest degree of international legitimacy.[5] The United Nations does not do invasions, however, and seldom deploys more than about 20,000 troops in any given operation. For missions which require forced entry or demand more than a reinforced division of troops, a coalition led by a nation or alliance such as NATO will probably be necessary, at least for the first phase of the operation. Although NATO is militarily much more potent than the United Nations, it possesses none of the other attributes needed for successful nation building. Thus NATO–led military operations will always require the United Nations or other national and international actors to provide the various civil components without which no nation-building mission can succeed.

Nation building always requires the integration of national and international efforts. Larger missions require several layers of consultative machinery to operate effectively. The first inner circle should include the major powers that care most about the success of the enterprise and are prepared to commit troops and money to it. The second circle should involve the major financial donors. The third should involve the neighboring powers. Without such coordination, international efforts are likely to be disjointed, with the various organizations concerned competing for turf while shirking the riskier or less-rewarding tasks.

When nations disintegrate, the competing contenders for power inevitably turn to external sponsors for support. Faced with the prospect of a neighboring state's failure, the governments of adjoining states seek to develop local clientele and back rival aspirants to power. It is, therefore, practically impossible to put a broken state back together if its neighbors are committed to frustrating that effort. Much as one may regret and deplore such activity, neighbors can neither be safely ignored nor effectively barred from exercising their considerable influence. It is the adjacent states, after all, that suffer the consequences of state failure and civil conflict most directly. It is they that must shelter the refugees and cope with the endemic diseases, increased criminality, spreading terrorism, and disruptions to their commerce generated by such conflicts. They cannot afford to remain uninvolved. It has always proved wise, therefore, to find ways to engage them constructively, no matter how unhelpful their activities may have been in the past. Failure to do so can condemn even the most generously resourced operation to failure.

Setting Priorities

The prime objective of any nation-building operation is to make violent societies peaceful, not to make poor ones prosperous or authoritarian ones democratic. Economic development and political reform are important instruments for effecting this transformation but will not themselves assure it. Rather, such efforts need to be pursued within a broader framework, the aim of which is to redirect the competition for wealth and power which takes place within any society from violent into peaceful channels.

The first-order priorities for any nation-building mission are public security and humanitarian assistance. If the most basic human needs for safety, food, and shelter are not being met, any money spent on political or economic development is likely to be wasted. Accordingly, these missions should be organized around a hierarchy of nation-building tasks, which flow in the following order:

- security—peacekeeping, law enforcement, rule of law, and security-sector reform;
- humanitarian relief—return of refugees and response to potential epidemics, hunger, and lack of shelter;
- governance—resuming public services and restoring public administration;
- economic stabilization—establishing a stable currency and providing a legal and regulatory framework in which local and international commerce can resume;
- democratization—building political parties, a free press, civil society, and a legal and constitutional framework for elections; and
- development—fostering economic growth, poverty reduction, and infrastructure improvements.

This is not to suggest that the above activities should necessarily be initiated sequentially. If adequate funding is available, they can and should proceed in tandem. But if higher-order priorities are not adequately resourced, anything spent upon lower-order ones is likely to be wasted.

Seizing the Moment

The weeks immediately following the arrival of foreign troops tend to be a time of maximum possibility. The appearance of an intervening

force normally produces a combination of shock and relief in the local population. Resistance is unorganized, spoilers unsure of their future. The situation is highly malleable, but the capacity of intervening authorities to capitalize on these opportunities is usually limited by the absence of many mission components. If one is to take advantage of what has been called the "golden hour" that follows the end of major combat operations, the intervening authorities need to have at their disposal upon arrival a minimum set of assets: enough troops, police, civil administrators, and humanitarian supplies to secure and supply at least the capital. These can then be followed quickly by judicial and penal experts with funded plans for the disarmament, demobilization, and reintegration of former combatants and training or retraining of the police force.

Soldiers

Soldiers are among the first elements of any nation-building mission to arrive. They are often called upon initially to perform many functions that would be better fulfilled by civilian experts, were such available in sufficient numbers. Their first priority, however, should be to establish a modicum of security in what may be a chaotic situation. Success in this task will be key to obtaining support of the population and introducing the civilian components of the mission in adequate numbers. Unless individuals feel safer by reason of the external military presence, they will not collaborate in reporting on criminals, terrorists, or other "spoilers." Unless goods, services, and people can again circulate normally, political and economic reforms cannot begin to take hold. Intervening forces will normally require help from the local police and at least the passive cooperation of the local military to establish a secure environment. Even when available, however, indigenous security services will usually prove incompetent, corrupt, and abusive, requiring close oversight, mentoring, and institutional change.

Once a minimal level of security has been established, the disarmament, demobilization, and reintegration of former combatants should normally become the next priority. Agreement among the contending parties to take part in such a process is often a prerequisite for deployment of an international force. In heavily armed societies with a long tradition of gun ownership, depriving individuals of their small arms may prove impractical. At a minimum, heavy arms should be gathered, stored, or destroyed, and the display of small arms by anyone except state security forces should

be banned. Armed units should be broken up and individuals offered alternative livelihoods. It is important the mission arrive with a plan and adequate funding to perform these tasks.

In societies with little formal employment, it will not be possible to find long-term positions for all former combatants. At a minimum, the reintegration program should occupy and support these individuals for a period long enough to allow units to be broken up and the ties among their members to be loosened.[6]

The military component should establish extensive links with the civilian population. One avenue is through active intelligence collection, surveillance, and reconnaissance. The second is a program of civic action, through which military units support humanitarian and reconstruction assistance. Such tasks fall primarily to the civilian agencies, but the military can often supplement those efforts in useful and visible ways. This needs to be done with some sensitivity, recognizing that humanitarian organizations attach great importance to maintaining their impartiality in conflict environments and will resist close association with an intervening military force, even one operating on behalf of the United Nations.

While most postconflict societies will have more of their own soldiers than they need, they will probably have fewer police. Even as local armies need to be scaled back and reformed, police forces need to be bolstered and also reformed. The military contingent of the mission is often involved in the former process and sometimes in the latter, although the police training function is better assigned to civilian police where available.

Forced entries are often the prelude to demanding peace enforcement operations. The entries themselves may not prove particularly difficult—indeed, in recent decades these have invariably been achieved rapidly and with minimal loss to the entering force. By contrast, the postcombat stabilization and reconstruction phase has been much more time-consuming and costly.

Stabilizing an internally divided society without significant indigenous capacity for security can require an external military force of 10 to 20 soldiers per 1,000 inhabitants. In circumstances where the parties to the conflict have jointly sought external intervention and are prepared to collaborate with it, that requirement can be reduced on occasion to less than one soldier per 1,000 inhabitants. Where only this lower force ratio is likely to be achieved, deployment should normally be conditioned upon

prior agreement among the contending parties to disarm and collaborate with the intervening force.

The cost for fielding an American or NATO force is about $200,000 per soldier per year. The cost of fielding the normal UN peacekeeping force is about $45,000 per soldier per year. High-end peace enforcement operations require, on average, 10 times more military manpower per inhabitant than standard peacekeeping missions. Clearly, then, peace enforcement is appropriately a last rather than first resort, to be employed only where the stakes are great and the intervening powers highly committed.

Police

Public security is the first responsibility of any intervening authorities. That security is sometimes imperiled by contending armies and always threatened by criminals, gangs, and violence-prone political groups. International military forces are best suited for dealing with the first sort of threat, police with the rest.

Military police are better than standard infantry for some public security functions—such as crowd control—but less suited than civilian police for criminal investigations or community policing. On the other hand, most international civilian police are not well equipped to deal with well-organized crime or large-scale violence. In many ways the ideal police for nation-building missions are gendarmerie-type units that combine military discipline with a high level of investigative, forensic, and intelligence collection skills. Unfortunately, only a few countries maintain such forces. Consequently, they are always in short supply.

UN peacekeeping forces typically deploy about one policeman for every 10 soldiers. These international police monitor, mentor, and train local police forces. Where the local police have disintegrated entirely, international police may need to undertake law enforcement functions themselves. This requires a much larger contingent of international police, something only really feasible for extremely well-resourced operations in smaller countries.

Local police will need to be quickly vetted and closely supervised. In the medium term, they will need to be thoroughly reformed or replaced entirely. In the longer term, the new or retrained police will need to be mentored, supported, and held accountable. Intervening authorities should arrive with plans, funding, and personnel to begin performing at least the first two functions immediately.

In addition to the United Nations, the European Union has developed the capacity to deploy significant numbers of international police. The UN currently deploys over 7,000 police in postconflict situations; the EU has set a goal of being able to deploy up to 5,000. The United States currently deploys some 300 international police officers, mostly in Kosovo. It continues to rely on private contractors for this purpose. This arrangement is clearly inferior to a system wherein the deployed police would be US government employees rather than contractors, with the greater reciprocal degree of loyalty, discipline, and commitment that relationship implies. In both Afghanistan and Iraq, the United States has failed to deploy any civilian police whatsoever.[7]

Most postconflict societies require at least two of their own policemen for every 1,000 inhabitants. The intervening authorities should anticipate the need to rebuild, reequip, and, for the first several years at least, pay a police force of this magnitude. The annual cost per local police officer will be approximately three times that country's per capita GDP. International police, by contrast, cost about $150,000 per person per year. Where the responsibilities of international police are limited to oversight, mentoring, and training of local police, one for every 10,000 inhabitants may be adequate. Where they assume a direct law enforcement role, one for every 1,000 inhabitants may be needed.

Rule of Law

In most nation-building operations, efforts to rebuild the judiciary and corrections systems have taken second place to police reform. This is unfortunate and counterproductive. Police who lack prisons in which to put criminals and judges before whom to bring them will inevitably be left with the invidious choice of either punishing miscreants themselves or letting them go. Either alternative will corrupt and demoralize the best-trained force.

A first-order issue to be addressed in most nation-building missions is what law to enforce. The usual answer is to take the country's most recently promulgated criminal code, purge it of obviously abusive statutes, and employ it as the law of the land. In some cases, intervening authorities may have to go further into the past to find a criminal code acceptable to the population. Occasionally, it may have to promulgate laws of its own. These are decisions that should be made as part of the preparation for the

mission so newly arriving troops and police have a clear idea of what rules are to be enforced.

In societies emerging from prolonged civil war, the legal system will likely have ceased to function. There will be an absence of judges, and those available may be unqualified. Courts and prisons may have been destroyed, and those which survive will be stripped of essentials. As with the police, the short-term objective will be to vet the judiciary and corrections staff and oversee their activities; in the medium term to reform and rebuild both these institutions; and in the long term to foster the development of a rule of law culture. These activities should proceed in parallel with police reform.

Establishing the balance between retribution and reconciliation in societies emerging from conflict or tyranny presents a particular challenge. Who to punish and who to forgive, who to exclude from the new dispensation and who to co-opt into it, are choices that cannot be entirely avoided.

War crimes tribunals provide a judicial vehicle for holding accountable those most responsible for past atrocities. The local society will seldom be capable of mounting a credible legal process. International tribunals, on the other hand, are hugely expensive and may lack legitimacy in the eyes of the affected populations. Mixed tribunals, in which international and local judges sit together, can help address some of these difficulties.

Lustration represents an administrative approach to the same problem. Here the intention is to assess group rather than personal responsibility. The objective is not so much to punish as to exclude the affected group from future influence, usually by barring members from public employment and sometimes stripping them of other civil rights. Denazification in post–WWII Germany, demilitarization in Japan, and debaathification in Iraq are examples of this process.

Truth commissions lie near the opposite end of the retribution/reconciliation spectrum. These are nonjudicial inquiries into past abuses with a view to assessing blame but not levying penalties. In going this route, society is saying, "We are prepared to forgive but not forget."

It is clearly easier to exact retribution in circumstances where the conflict has produced clear winners and losers, particularly if the losers have lost so badly as to preclude any further resistance. This is seldom the case. In other circumstances, any effort to impose accountability for crimes committed in the course of conflict, whether through judicial or admin-

istrative processes, may occasion more resistance than the intervening authority is capable of suppressing.

War crimes tribunals are sometimes employed by the international community as an alternative to intervention rather than as an adjunct. In such instances, tribunals serve principally as a means of assuaging the international community's conscience without requiring it to commit the troops and money needed to actually stop the crimes it abhors and punish the perpetrators. Proponents argue that the simple threat of judicial action at some indefinite point in the future will curb abusive behavior. As yet, there is scant empirical support for this thesis.

In the context of nation building, war crimes tribunals and lustration should be employed only in those rare situations where the intervening authority is equipped to enforce the outcome and ready to deal effectively with the resultant resistance. Applied in any other circumstances, the effect is likely to be increased polarization of the society in question and may make an eventual resumption of violence more, rather than less, likely.

Humanitarian Relief

Humanitarian operations often precede nation-building missions, having been initiated in response to the conflict and sustained in many cases throughout its course. Thus, while the arrival of peacekeepers may signal the opening of an operation for most of its constituent elements, it can signal the beginning of the end for those engaged in lifesaving humanitarian relief efforts, as displaced persons are helped to return to their homes, refugee camps are closed, and public services restored.

Most major humanitarian relief agencies are professionally staffed, highly experienced, and comparatively well resourced. While funding for nation building is almost always in short supply, humanitarian relief is that aspect donors are most inclined to fund, thus relief efforts are usually among the least problematic of any nation-building mission. We have found no mission whose overall success was compromised by inadequacies in this aspect of its operations. On the other hand, there are many examples of situations in which the intervening authorities' failure to establish a modicum of public security has made it impossible for humanitarian agencies to complete their tasks or even to sustain lifesaving assistance to threatened populations.

In cases where the intervening authorities quickly establish a reasonably secure environment, relief operations usually proceed smoothly. Refugees return, sometimes with surprising rapidity. Public services are

gradually restored, including public health services. The economy revives, and within a year or two, most humanitarian agencies move on to another emergency or shift their emphasis from lifesaving to developmental activities.

Coordination between military and humanitarian organizations is never easy. The number of such organizations has grown vastly in recent years; not all are of the highest quality. All humanitarian organizations seek to remain impartial, even when the United Nations is lined up on one side and local outlaws on the other. This may seem anomalous, as it is often the same donor governments who are funding the humanitarian efforts and manning the intervening military force. Humanitarian organizations feel strongly, however, that their ability to gain access to exposed populations depends upon maintaining strict impartiality. Accordingly, representatives of such organizations carefully limit their interactions with international peacekeepers, even when they look to these forces for security.

Coordination becomes particularly difficult when intervening authorities have failed to establish a secure environment. The usual division of labor between international military forces and humanitarian organizations is then difficult to maintain. Humanitarian organizations may find themselves unable to provide relief in very dangerous areas. International military units may feel compelled to step into this void and begin delivering relief supplies, in the process blurring the distinction between combatant and humanitarian worker. While such arrangements are preferable to a complete absence of humanitarian relief, it is generally best if the military and the humanitarian organizations each concentrate upon their respective primary tasks: maintaining security and delivering assistance.

Governance

Societies emerging from conflict may be able to wait for democracy, but they need a government immediately if there is to be any law enforcement, education, or health care. National governments are usually responsible for regulating and in some instances providing electricity and telecommunications. In most cases, municipal governments provide water and sanitation.

While the intervening authorities may initially serve as the government, they will never be in a position to deliver these services long-term. They must rely on host country nationals and, in most cases, local institutions to provide public services. The intervening authorities may provide fund-

ing, guidance, and oversight, but teachers, health care workers, and most of the police force must be drawn from the host country.

Intervening authorities select people and organizations to deliver these services. These individuals and organizations are provided funds and power. The intervening authorities must be attentive from the start to ensure that their choices do not discriminate against groups, especially those that were party to the conflict. They need to choose partners carefully with a view to creating a government and distribution of power that will be sustainable when they leave.

Many services can best be provided at the local level. Rebuilding government from the bottom up allows new leadership to emerge, including individuals unassociated with the recent conflict. On the other hand, empowering local officials before the national government has been reconstituted can feed sectional conflict in circumstances where the relationship between the center and the periphery is unsettled.

The intervening authorities will have to meet much, perhaps all, of the initial costs of restoring basic government services. The requirement for financing for public health, education, and general government administration can be expected to run about 10 percent of the country's preconflict GDP.

Economic Stabilization

The resumption of commerce requires the availability of a reasonably stable medium of exchange. Sustained growth is virtually impossible in periods of very high inflation. While donors may initially finance the resumption of government services, it is important to quickly reconstruct the host state's capability to allocate that funding and oversee its expenditure and to expand its capacity to collect its own sources of revenue. As more money is pumped into government, there are greater opportunities for corruption, which will require institutions for auditing and accountability and the creation of a professional civil service for control.

Early attention should be given to creating or strengthening a central bank, ministry of finance, and civil service commission to meet these needs. Occasionally a foreign currency is adopted as the medium of exchange, but more often a national currency is preferred to preserve the option of adjusting the exchange rate to better manage economic activity. Among the most difficult tasks facing the central bank will be ensuring that commercial banks become and remain solvent.

Donor budget support will be required to keep government expenditures and revenue in balance, avoiding the need to print more money. Donor conferences are the usual vehicle for assuring an adequate flow of funding. It is usually best to hold at least two such meetings, the first for immediate humanitarian, security, and economic stabilization needs; the second, a year or two later, to focus upon longer-term development. The World Bank and the UN Development Program should be asked to prepare a needs assessment for these conferences. The International Monetary Fund should take the lead in establishing or reforming the central bank and providing it the wherewithal to manage the currency.

Democratization

Neither the United States nor the United Nations deploys military forces to make poor nations rich or even to make authoritarian states democratic. They do employ armed force to transform violent societies into peaceful ones. Democratization alone will not ensure this outcome. On the contrary, elections may be polarizing events in already divided societies. Thus, in the context of nation building, the process of democratization should be seen, not as an end in itself, but as a practical means of redirecting the ongoing competition for wealth and power that exists in all human societies from violent into peaceful channels.

With most international interventions, the preexisting forms of government will have been irremediably disrupted or discredited in the preceding conflict. The sole modern exception to this rule was Kuwait in 1991, where the United States was able to liberate the country and immediately turn it back over to its hereditary ruling house. In most cases this option will not be available, and the establishment of representative institutions based on popular sovereignty will offer the only viable basis for reconstituting state authority in a manner likely to be acceptable to most of the population.

In considering constitutional design, a first step is to analyze the sources of violent conflict in the society. An exceptionally strong and committed intervening authority may be able to dispossess one group and empower another in an enduring fashion. In most circumstances, however, success in nation building will depend more upon co-option than exclusion of potential spoilers. In societies divided by sectarian strife, it may be necessary to craft power-sharing arrangements that limit the authority of the

majority and provide guarantees to the minorities beyond those found in more developed democracies.

Democracies come in many shapes and sizes. Left to their own devices, intervening powers will tend toward replicating their own institutions, while local populations will be inclined to opt for a system with which they are familiar, even if that system has served them poorly in the past. In most cases, it will be better to adapt the locally familiar to new circumstances, rather than import wholly new arrangements unfamiliar to host country citizens. Nevertheless, some degree of innovation will be necessary, since the forms of government with which the society is fully familiar will have usually failed them in the past and would likely do so in the future if resurrected.

Ideally, national elections should be preceded by the disarmament, demobilization, and reintegration of former combatants, the growth of civil society, the establishment of independent media, the development of political parties, and the holding of local elections. This sequence may not always be fully achievable. In some instances the intervening authorities may be too weak to resist the call from dominant elements in the society for early elections or to administer the society without the support of a government legitimized through the electoral process.

The United Nations is the best source of expertise on the development of transitional and permanent political systems. The Organization for Security and Cooperation in Europe (OSCE) has developed considerable expertise in the promotion of civil society, the establishment of independent media, and the development of political parties, although its activities have so far been limited to Eurasia. Several nations, including the United States and Germany, maintain publicly financed party-based organizations that specialize in helping foster the development of political parties in emerging democracies. The International Federation for Election Systems (IFES) has organized elections in dozens of countries around the world under the most challenging of conditions.

Infrastructure and Development

Postconflict societies are attractive candidates for development assistance. Dollar-for-dollar aid to nations emerging from war will result in much higher levels of growth than the same amount provided to more-settled societies. Postconflict societies also can use more assistance, as measured as a share of GDP, than more-settled societies. Whereas most

developing societies cannot usefully absorb assistance representing more than about 20 percent of their annual GDP, postconflict nations can make good use of aid representing up to 40 percent of their GDP, and in the first year following conflict, up to 70 percent.

The quality of policies adopted by the intervening authorities and the host government will be as important as the volume of assistance in determining the latter's utility. Controlling inflation, balancing the government budget (in the early years via large transfer payments from international donors), creating regulatory and tax systems conducive to growth, reducing or eliminating subsidies, attracting investment, and operating utilities and state-owned enterprises on a sound market-oriented basis will be essential to fostering sustained growth. Reforms of this nature will necessarily occasion resistance. The process needs to be managed in ways that draw the society's major contending factions into a process of peaceful competition and away from a return to violent conflict.

The term *reconstruction*, when used to describe the reform of postconflict societies, conveys the sense that physical rebuilding of homes, factories, roads, and power plants destroyed in the war is the prime need. This is misleading. Even more than infrastructure, nations emerging from conflict need better institutions. In most cases, these institutions need to be refashioned, not just rebuilt, since it is the old institutions that will have failed in the first place. This is as true in the economic sphere as in the political. Novelty, however, is not necessarily a virtue. Institutions should be refashioned with an eye to local history and culture as well as to efficiency if the changes are to secure broad and enduring acceptance.

As regards physical infrastructure, the intervening authorities should give priority to fixing those related to security, health care, education, power, water, and sanitation in an effort to raise these services to something approaching prewar levels. The focus should be on emergency repair, not new investment. The improvement as opposed to the repair of infrastructure should be funded through project finance by international financial institutions like the World Bank or other lenders rather than through bilateral grant assistance. Project finance imposes disciplines that are too frequently absent from schemes funded with grant assistance, requiring as the former does all the parties to address issues of size, cost, and repayment in light of demand, anticipated revenues, and rate setting.

Security is an essential precondition for productive investment. Money spent on infrastructure and development will be largely wasted if people, goods, and services are subject to high levels of kidnapping or attack.

The Cost of Nation Building

Most historical nation-building operations have fallen into one of two categories. The first is peacekeeping missions mounted on the basis of prior agreement among the warring parties. The second is peace enforcement operations launched over the opposition of one or more of the indigenous factions. Interventions of the first type have typically been led by the United Nations; those of the second by a major global or regional power or alliance of such powers. Peace enforcement actions have proved much more expensive than peacekeeping operations and particularly so for the leading participants.[8]

The chart below looks at the requirements for the two types of operations in the same hypothetical country. The nation in question is rather small and very poor, with a population of 5 million and a per capita income of $500, thus similar in size and level of development to Haiti, Sierra Leone, or Liberia. The light peacekeeping operation assumes a permissive entry, acquiescent population, and some level of remaining local capacity for governance and security. The heavy peace enforcement mission assumes a forced entry, a more hostile or divided population, and little or no immediately available indigenous capacity for governance and security. In both cases the society is assumed to be generating no significant government revenue, thus requiring that nearly all public services be initially funded by the intervening authorities. More prosperous postconflict societies are usually able to fund some appreciable share of their own government operations themselves, but their reconstruction may nevertheless pose a larger burden on external donors because public services in such societies are more expensive to provide due to higher wage rates. Thus, somewhat counterintuitively, nation building can be more expensive in relatively developed societies, like Bosnia or Iraq, than in highly underdeveloped ones like Afghanistan or Sierra Leone.

A light peacekeeping operation in this hypothetical society is estimated to require 9,000 international soldiers and police at a total cost of $1.5 billion per year. A heavy peace enforcement mission could require up to 80,000 troops and cost $15 billion per year.[9] These figures are consistent

with the actual costs and manning levels of UN–led peacekeeping and US–led peace enforcement operations over the past several decades. Over this period, heavy nationally or alliance-led peace enforcement missions have proved, on average, to require approximately 10 times more manpower and money, on a per capita basis, than lighter, UN–led peacekeeping missions.

The Costs of Nation Building

(in a hypothetical country of 5 million people with a per capita GDP of $500)

Light Peacekeeping				Heavy Peace Enforcement			
SECTOR	PERSONNEL Local	Int'l	COST (Million$)	SECTOR	PERSONNEL Local	Int'l	COST (Million$)
Military		8,000	360	Military		65,000	13,000
	15,000		50		15,000		50
Police		1,000	170	Police		8,000	1,250
	11,000		18		11,000		18
Rule of Law			18	Rule of Law			18
Humanitarian			170	Humanitarian			170
Governance			260	Governance			260
Economic Stabilization			30	Economic Stabilization			30
Democratization			50	Democratization			50
Development and Infrastructure			390	Development and Infrastructure			750
TOTAL	26,000	9,000	1,520	**TOTAL**	26,000	73,000	15,600

The expense of any nation-building mission is shared among troop contributors, aid donors, and the international community as a whole according to various burden-sharing formulae. The costs for UN–led operations are spread most widely. Those for nationally led peace enforcement missions fall more heavily upon the lead nation and its principal allies.

Is Nation Building Cost Effective?

Even the lighter, more consensual, less ambitious approach to nation building epitomized by UN peacekeeping operations represents an expensive enterprise, although not more expensive than allowing a conflict, once halted, to be renewed. Put differently, conflicts generally impose greater costs upon the international community than the expense neces-

sary to ensure that the cycle of violence, once halted for whatever reason, is not renewed. While it may be prohibitively expensive to forcefully halt a civil war in full swing, experience has shown that interventions intended to consolidate and perpetuate tentative peace are cost effective.

In addition to the horrendous human costs, war inflicts extraordinary economic costs on societies. And no wars inflict such damage as civil wars. The destruction of homes and facilities, the disruption of commerce, and the killing and maiming of citizens have impoverished all the states we have analyzed. Paul Collier and Anke Hoeffler have attempted to quantify some of the economic costs of civil war. They find that on average civil wars reduce prospective economic output by 2.2 percent per year for the duration of the conflict. However, once peace is restored, economic activity resumes, and in a number of cases, the economies grow.

Collier and Hoeffler examine various policy options to reduce the incidence and duration of civil wars. They find postconflict military intervention to be highly cost effective, in fact, the most cost-effective option they analyze.[10] The historical record demonstrates that unless peacekeeping forces are deployed as part of the international community's overall response, most societies emerging from conflict return to it within a few years, no matter how much money, advice, or other forms of assistance they may receive. By contrast, the majority of postconflict societies where peacekeepers have been deployed remain at peace after the international troops are finally withdrawn.

The effects of successful interventions may also be measured in a sharp overall decline in deaths from armed conflict around the world over the past decade. During the 1990s, deaths from armed conflict were averaging over 200,000 per year. In 2003, this number had come down to 27,000, a fivefold decrease in deaths from civil and international conflict. Since 2003, the numbers of civil conflicts and resultant casualties have continued to drop, although more slowly.[11]

The cost of UN nation building tends to look quite modest when compared to the cost of larger and more demanding US–led operations. Over the past several years the United States has been spending some $4 billion per month to support its military operations in Iraq. This is approximately what the United Nations will spend to run all 16 of its current peacekeeping missions for a year. Therefore, the cost for one year of US operations in Iraq could approach the cost for all UN peacekeeping from 1945 to the present day. The United States pays only one-quarter

of the UN peacekeeping budget; thus, the annual US contribution for all UN peacekeeping is less than the cost of one week's operations in Iraq.

This is not to suggest that the United Nations could perform the US mission in Iraq more cheaply—or perform it at all—but simply to underline that there are 16 other places where the United States will probably not have to intervene because UN troops are already doing so at a tiny fraction of the cost.

Conclusion

The ultimate objective of any nation-building mission is to leave behind a society likely to remain at peace with itself and its neighbors once external security forces are removed and full sovereignty is restored. This will likely require some level of democratization and economic development. Neither endeavor, however, can assure peace, and either, if pushed injudiciously, can exacerbate rather than ameliorate the tendency toward renewed violence so prevalent in societies emerging from conflict. If peace is to be created, security is key. Only when a modicum of security has been restored do prospects for democracy and sustained economic growth brighten.

As a practical matter, full-scale peace enforcement actions are feasible only when the intervening authorities care a great deal about the outcome and, even then, only in relatively small societies. Thus, the effort needed to stabilize Bosnia and Kosovo has proved difficult to replicate in Afghanistan or Iraq, nations that are eight to 12 times more populous. It would be even more difficult to mount a peace enforcement mission in Iran, which is three times more populous than Iraq, and nearly impossible to do so in Pakistan, which is three times again more populous than Iran. Considerations of scale therefore suggest that the transformational objectives for intervention in larger societies need to be sharply restrained on account of the much more modest resources, relative to the population, likely to be available.

Nevertheless, the difficulties encountered and costs accrued in Iraq and Afghanistan should not lead Americans to conclude that the entire enterprise of rescuing failed states and reconstructing societies emerging from conflict is beyond them. Tens of millions of people are living in peace today, and mostly under freely elected governments, in places like Mozambique, El Salvador, Namibia, Cambodia, Bosnia, Kosovo, Macedonia, East Timor, Liberia, and Sierra Leone because US, or UN, or NATO

troops came in, separated the combatants, disarmed and demobilized the contending factions, secured economic growth, organized elections, and remained long enough to ensure government survival. It is important to recognize the true costs and risks associated with such exercises, but in most cases such a careful cost/benefit analysis will favor external intervention once the parties to conflict are ready to make peace. SSQ

Notes

1. The US and UN experiences in modern nation building are examined and compared in two RAND volumes: Dobbins et al., *America's Role in Nation Building: From Germany to Iraq* (Santa Monica, CA: RAND, 2003); and Dobbins et al., *The UN's Role in Nation Building: From the Congo to Iraq* (Santa Monica: RAND, 2005). The European experience is examined in Dobbins et al., *Europe's Role in Nation Building: From the Balkans to the Congo* (Santa Monica: RAND, 2008).

2. Paul Collier and Anke Hoeffler, *The Challenge of Reducing the Global Incidence of Civil War*, Copenhagen Challenge Paper (Oxford: Center for the Study of African Economies, Department of Economics, Oxford University, 23 April 2004).

3. Dobbins et al., *After the War: Nation Building from FDR to George W. Bush* (Santa Monica: RAND, 2008), examines the role of presidential personality, decision-making processes, and bureaucratic structure on the outcome of nation-building-type missions.

4. For a more extensive exploration of the necessary components for a successful nation-building mission, see Dobbins et al., *The Beginner's Guide to Nation Building* (Santa Monica: RAND, 2007).

5. The main criterion for success in any peacekeeping endeavor is whether, on departing, one is able to leave behind a society at peace with itself and its neighbors. The UN has achieved this objective over the past 20 years in a significant number of places, to include Namibia, El Salvador, Mozambique, Cambodia, East Timor, Liberia, and Sierra Leone. All of these once war-torn countries are today at peace, and all except Cambodia are ruled by freely elected governments.

6. In many low-income countries, the problem is not so much unemployment as poverty. In such societies people must work to survive. In consequence few are idle, but many make only a subsistence living by engaging in agriculture, manual day labor, or petty commerce. Employment in such societies is often equated with a government job, the only major source of a steady income. This definition leads to high unemployment statistics, which do not reflect the actual levels of gainful activity. In societies where the government is almost the only formal employer, it will not often be possible to fine long-term "employment" for large numbers of disbanded former combatants. It will be necessary in such circumstances to institute short- to medium-term programs to employ and retrain these individuals, while at the same time seeking to promote economic activity and reduce poverty in the society as a whole.

7. International police are uniformed police officers who monitor local police or enforce the law themselves. Civilian instructors in police training establishments, who may be former policemen, are not normally counted in this category.

8. For a fuller discussion of the sizing and costing of nation-building missions, see the relevant chapter in Dobbins et al., *Beginner's Guide to Nation Building*.

9. In three instances the projections differ substantially. The size, capability, and cost of the international military force that intervenes under the heavy peace enforcement operation are substantially more than in the light peacekeeping scenario, consistent with the international community's experience with these two types of operations. For the heavy peace enforcement scenario, we calculated the number of soldiers using the average number of international military personnel deployed in the first year of eight peace enforcement operations (East Timor, Eastern Slavonia, Japan, Somalia, Haiti, Bosnia, Kosovo, and Iraq; we excluded the two outliers—Germany on the high end and Afghanistan on the low end—from the average). For the light peacekeeping scenario, we used the average number of soldiers in the first year of six peacekeeping operations: Congo (in the 1960s), Namibia, Cambodia, Mozambique, Sierra Leone, and El Salvador.

Numbers of international police also differ. For the heavy peace enforcement scenario, we computed the number of police using the average number of international police deployed in the first year in three operations: Bosnia, East Timor, and Kosovo. (The average was 161 per 100,000 inhabitants; Afghanistan, Germany, and Japan were excluded from the average because no civilian international police were deployed to these three countries.) For the light peacekeeping scenario, we used the average number of police in the first year of eight less-ambitious operations with international police components: Congo (in the 1960s), Namibia, El Salvador, Cambodia, Somalia, Mozambique, Haiti, and Sierra Leone.

Finally, we assumed that the willingness of foreign donors to fund infrastructure development was less in the peacekeeping than in the peace enforcement scenarios. For the peacekeeping scenario, we assumed that the international community would fund reconstruction to the tune of 16 percent of GDP, the level funded in Bosnia the second year after the end of the conflict. For the peace enforcement scenario, we assumed that the international community would fund reconstruction at a high level: 30 percent of GDP, the level provided Bosnia the first year after the end of the conflict.

10. Collier and Hoeffler, *Challenge of Reducing the Global Incidence of Civil War*, 3; and Dobbins et al., *UN's Role in Nation Building*, 247.

11. "Human Security Report 2005," Human Security Center, University of British Colombia, and the "Human Security Briefs" for 2006 and 2007 from the same center, http://www.hsrgroup.org/human-security-reports/human-security-report.aspx.

How Terrorist Groups End

Studies of the Twentieth Century

Christopher C. Harmon

Terrorism studies are far too young to have their Arnold Toynbee. At this writing there remains a need for broad and searching inquiries into why and how terror groups have declined or ended. The project requires detailed knowledge of scores of important groups, extant and extinct, worldwide. It also demands originality. This article reluctantly sets aside the useful framework developed in 2003 and worked publicly for five years.[1] A fresh approach in this vital field will help with understanding what we expect in the twenty-first century. This article begins with a look at early forms of violence in the twentieth century and proceeds to specific examples in the American experience. Revolutionaries of the 1960s and terroristic religious groups are also addressed. Finally, the project presents a nine-part framework for understanding terrorist groups.

Early Forms of Violence

The twentieth century inherited several forms of violence that would dramatically influence politics and terrorism. Three important and very different ones were labor militancy, anarchism, and communism. Each of these schools of thought and action profited from liberalism and rationalism, was internationalist, and by degrees, each supported workers and the poor. The most honest and credible of the three was labor—the drive for the rights and wages of blue-collar working men,

---

Dr. Christopher C. Harmon taught strategy and policy at the Naval War College and held the Kim T. Adamson Chair of Insurgency and Terrorism (2005–2007) at the Command and Staff College, Marine Corps University. He is author of the graduate-level textbook, *Terrorism Today*, published by Frank Cass (2000) and Routledge (2007), and articles in such journals as *Vital Speeches*. From 2007 through 2010 he directed curricula for the George C. Marshall Center's Program on Terrorism and Security Studies. This article, edited for length, is reprinted from his new book, *Toward a Grand Strategy against Terrorism* (McGraw-Hill, 2010).

women, and children but a drive that sometimes assumed violent means and took innocent lives.

Labor Militancy and Violence

International labor organizations arose from, and sometimes parallel to, older national and more-local models. Their members were overwhelmingly partisans of a fair wage, decent hours, and protecting children from brutal factory work or endless hours. Some activists, however, stepped well over the lines of public pressure and civil opposition. Individual militants or groups of organized laborers undertook the beating or killing of bosses, night watchmen, or "big capitalists." Cities as different as Seattle and New York witnessed laborites' assaults on the innocent. A few representatives for a union of iron workers and bridge builders coordinated an ugly bombing campaign in the United States in the fall of 1910 that took two dozen lives, injured others, and massively damaged property.[2] The labor movements also produced theorists and public advocates (e.g., Georges Sorel in France). They advocated violence—usually accompanied by other political aims and strategies that might appeal to the sympathetic mind and to the average citizen.

American labor violence succeeded, in its way, according to the best US historian of terrorist movements, Walter Laqueur. "The daily wage of American iron workers (AFL) went up from $2.00 to $4.30 (for shorter hours) between 1905 and 1910 as the result of the bombing of some one hundred buildings and bridges."[3] To violence and that powerful display—the strike—labor militants added mediation, sweet reason, unions, and other factors. These combinations improved labor conditions and pay. There was steady growth and legitimization of unions. Over the decades, sporadic labor violence did not end, but it came to be seen in the American public mind as separate from political notions such as anarcho-syndicalism or communism. These are all reasons labor violence overturned so few economies and political orders of the early twentieth century.

Anarchism

Although it often lauded the poor man or hated the rich man, anarchism was never essentially and directly about conditions in the workplace or the economy. It was obsessed with the state itself more than the state of the working man. Anarchism despises political authority as inherently

repressive and antihuman; it thus drives to bring down government—all government. In the last third of the nineteenth century and the early twentieth, anarchism was distinctively international, for reasons that were philosophical, first, and operational, second. The revolutionary concepts were exported, and the colluders turned up to write, preach, and kill in the United States, Italy, Spain, Germany, and France. International anarchists believed they could win; they could at least kill and could reduce a city to general fear. Historian Barbara Tuchman depicts Paris at one time in the grip of "mad bombers"—streets deserted, shops shuttered, panic evident in the public.[4]

Why did this anarchist movement die? Indeed it did end; incidents of violence fell off dramatically in Italy and France after 1900. In the United States, the movement appeared to peak about 1908 and touched another summit in 1919, but one hears little of new lethal attacks after 1920. It is also important to recognize that it was a movement—not a freakish wave of public interest, or a political party, or a disciplined formation of cells. Anarchism was international, it was networked (to use a modern term), ideas drove the actors, there were clandestine levels as well as public faces, some adherents were lethal, and some were utterly fearless. For these reasons, the movement suggests parallels with the contemporary Salafist Islamic movement—best known for the much-narrower al-Qaeda organization—thus, how it perished is doubly important.

New studies of terrorists by Richard Bach Jensen and Ersel Aydinli demonstrate how state intelligence units, policing agencies, and other governmental offices and legislatures had profoundly important roles. Italy and Russia took leads in multistate action to coordinate border control and extradition. American cooperation with foreign states became a reality while creating the Federal Bureau of Investigation (FBI) at home to help develop a national register, allowing information exchange and coordination across hundreds of local, county, and state jurisdictional lines. Europeans adjusted internal laws, as in banning open anarchist meetings and enhancing court powers over conspiracy (i.e., revolutionary activities short of attacks). Russian services performed ruthlessly, locking up suspects and executing anarchists. In short, governments worldwide stiffly countered the anarchists.

Communism

The twentieth century lived with and endured communism. Witnesses, participants, and victims saw communism's stages of nascence, its rise to power, its dangerous status as deliberator over half the world during the Cold War and its sudden decline in authority by 1990. It is errant to assume, however, that late-twentieth-century communist terrorist groups all fell with the Soviet bloc in 1989–1990. First, many communist militants fought on, such as Revolutionary Organization 17 November (N17) in Greece. It was never touched by the Greek state and was indeed only broken by a bomber's accident in 2002, allowing a wave of arrests.[5] Second, some state-supported communist groups fought on and *live even now*: the National Liberation Army (ELN) in Colombia long ago became self-supporting, has outlasted the Soviet bloc by two decades, and keeps several thousand men and women in the field. Third, certain communist groups did not fall with the Kremlin but perished well *before*. This was true of the Belgian Communist Combatant Cells. Most Italian leftist terror groups disappeared before 1990. Law enforcement was the usual primary reason.

The German Red Army Faction (RAF), or Baader-Meinhof group, did not announce its dissolution and failure in a communiqué until April 1992, proximate to the world-shaking fall of the wall, but the group's real end was signaled as early as 18 October 1977. On that day, four of the imprisoned RAF leaders attempted suicide (three succeeded). The Lufthansa jet their comrades had hijacked to bargain for the freedom of the prisoners in Stammheim jail was recaptured by elite West German border guards (GSG-9), who shot all the hijackers. With only a handful of quarrelsome confreres still operating inside the Federal Republic, the RAF experienced despair. After eight years of terrorism, they had made astonishingly few allies among 60 million normal Germans—people whose lives were democratic, whose self-governance centered in Bonn and more local places, and whose economy was a shining success. The RAF thus tottered along after 1990, but few new members joined, and nearly all who did were uncovered by diligent police work.[6]

Similar diligence by security forces and governments in France, Belgium, and Italy undercut and effaced those countries' "fighting communist organizations."[7] Regional cooperation by authorities developed as well.[8] Proper extraditions of fugitives thus gradually trumped older presumptions of the "asylum rights" of political terrorists, which had made violent refugees challenging to find.

Today communism is exhausted in most locales, but it has not died. "Naxalites" dominate parts of central-eastern India. Counterparts of a Maoist calling have reached a peak of power in Nepal, entered parliament, and taken the prime ministry, shelving terrorist methods—at least in most places, at least for now. Their terrorism has been placed on "pause" while they share power. Colombia has badly damaged the ELN and Revolutionary Armed Forces of Colombia (FARC)[9] regions, but neither insurgency is at an end. Peru's Sendero Luminoso, or Shining Path, decapitated by 1992 arrests, cannot live up to reports of a "comeback" after a decade and a half of impotence. Most of these latter-twentieth-century communist organizations failed for two fundamental reasons. First, they could not successfully challenge the post–World War II success of capitalism and democracy. Second, as Lenin and Mao predicted, sporadic violence by small cells was unlikely to enjoy strategic success unless fully integrated with broader political and economic plans. In Europe, the United States, and some other regions, factors—including the collapse of the Soviet Union—have persuaded most that communism has little future and, thus, that its violent methods cannot be justified.

Ghosts in the American Experience

Unfortunately, racism and terrorism from the extreme right in America have never been limited to the Ku Klux Klan network. There is a lengthy and distressing chronicle of maiming, menacing, and, occasionally, even murder of the innocent by other US groups preaching narrow or eccentric forms of white power religion and politics. Tiny political minorities and "lone wolf" actors—militants, usually male—tend to imagine themselves as heroic defenders of the racial majority in the 50 states. In a testament to the significance of ideas—not just personalities—in terrorism, at least five acts of terrorism are linked to the ugly racist novel, *The Turner Diaries*.[10] What social and political forces contain and resist this modern-day terrorism from the racist right? One is leadership from Washington, be it in federal statutes or action against entrenched resistance in some states and localities.[11] Successive US presidents, the Justice Department, and other organs of federal power used law, administration, rhetoric, and, occasionally, the deployment of soldiers to check violence and dampen the resistance of white citizens and institutions opposed to racial equality.

Federal power has not ended the Klan or most related organizations, but it damages their prestige, discourages activists, and demonstrates their weaknesses.

Public opinion has been even more important. Evolution, not revolution, moved Americans toward fuller racial equality. Education, religion, and common sense played their parts. Overt public resistance has been common all across America as racism is despised.[12] A third factor in the "containment" of such terrorism in the United States is the private legal suit. In singular victories that have come in a slow and compelling parade, civil suits are now used by public interest groups—usually in federal courts—to break individual terrorist organizations and hate groups.

Outside the United States, racism, neofascism, and extreme nationalism have many homelands and occasionally spawn terrorism. The group Blood & Honour keeps alive the Nazi flame, with members or affiliates in a number of European Union countries and the United States.[13] Rightist extremism has by no means ended in Europe, although it does not regularly lead to terrorism, nor is it as dangerous now as certain other terrorist ideologies.

More from the Left: Revolutionaries of the 1960s and Beyond

Scores of Che Guevarist–type groups came and went, unsuccessfully and swiftly, especially on the Latin American scene. Two of the continent's most celebrated terrorist groups—in Uruguay and Argentina, respectively—enjoyed years of success until the military intervened and conducted systematic repression with all available assets; that is, powerful terrorists were defeated by greater powers. Uruguay's bout with the Tupamaros began in 1962. Uruguayan armed forces intervened in April 1972 and soon captured key revolutionary leaders, as well as hundreds of cadre, and killed many Tupamaro gunmen. This was decisive; after 1973 the movement was never able to reorganize, and after 1976 it had no serious presence at all. The Tupamaros had a successful run for about a decade and disappeared. Uruguay's armed forces defeated them and, years later, withdrew and handed government back over to civilian authorities. A once-flourishing democracy was thus returned to the democratic fold.[14] Some old Tupamaros are in pacific politics today.

Full-blooded state reaction also crushed the Montoneros in Argentina. Their terrorist ideology blended nationalism with Marxist-Leninism and

populism, finding a balance of motives that accorded well with political trends in that country. A series of spectacular actions occurred in 1974, but this marked the apex of success for the revolutionaries, as it led directly to a military decision for intervention. For several months, multiple and often ugly methods were deployed to exterminate this powerful underground.

The Latin world of the late 1960s and 1970s saw the rise and fall of many other groups, including the National Liberation Action (ALN) organization of Carlos Marighella. He turned from mainstream Brazilian communism to terrorist work and published the 1969 pamphlet *Minimanual of the Urban Guerrilla*. Then he perished almost immediately in a gun battle with police. His successor lasted only months, and ALN disappeared. The fall of many such short-lived groups makes clear the pattern. Force was met with force, be it legal, covert, or martial. Latin America saw some cases of state appeasement of terrorists but few instances of successful negotiation leading to satisfactory settlements. Most of the challengers to government were advocates of "absolute war;" they were serious revolutionaries in a hunt for state power, not compromise and not limited reforms in favor of the poor or the workers. Terrorist parties of this time were creative, exciting to some citizens, and often well led by charismatic figures or well-educated propagandists, or both, making them strong enemies. As such, Latin states tended to reply slowly but ultimately with great harshness. In Guatemala and Argentina, especially, the government offensive came with free use of torture and extrajudicial killing.[15] Attrition of the terrorists and victory for the state were normal outcomes. The pattern would remain during much of the 1980s and 1990s, as we shall see, but with two notable differences: efforts at negotiation would become more common; and in certain cases, numbers of Latin undergrounders would fold pacifically into overt political parties, shaping their ambitions in more legitimate fashions. The Colombian M-19 and Salvadoran Farabundo Marti National Liberation Front (FMLN) cadre would do so, following defeats in the fields.

Events in Latin America had strong parallels in Western Europe by 1968. Anarchism reappeared in major cities after decades of absence and to a degree not known in Latin America. Michael "Bommi" Baumann's June 2 Movement in Germany helped reopen wars of youth, radicalism, and criminality against order. His mindless book of those days, *Terror or Love?*, suggests the lack of strategy in his political circle in Berlin and thus anticipates the decline and failure of that dimension of the urban and student movement. Joschka Fischer and Daniel Cohn-Bendit did

not do notably better in Frankfurt. These self-declared *Sponti*, or spontaneous ones, unrestricted by Leninist ideas of planning and revolutionary organization, attracted attention and sympathy—and police brutality on occasion—but never persuaded the German people that they were all "latent fascists." A concentrated multiyear effort to infiltrate a large Opel car factory and bring about a workers' rebellion flopped due to immaturity of technique.[16] Anarchism failed in northern Europe in the 1960s and 1970s, unless a loosening of lifestyles and culture is taken as the only standard of success. Fischer's career shows one way terrorists end: folding into pacific life. He moved away from the violent underworld and sympathies for armed terrorism toward the Green Party and elections, even becoming the Federal Republic's foreign minister (1998–2005). Both Fischer and Cohn-Bendit appear regularly in the newspapers, but as personalities and politicos rather than street fighters.

Europe's communist terrorist groups were more successful, longer lived, and found more mainstream supporters than competing anarchist groups. Italy's communists make for remarkable study. Prima Linea, or Front Line, was a large terrorist organization and force of the underground. Trotskyite and Maoist parties abounded, inside and outside the law. Lotta Continua, or Permanent Struggle, boasted some 200,000 adherents. The Red Brigades had "columns" in Rome, Florence, Turin, and Milan, even if the last of those turned restless and broke away, taking money and guns with them. Incident levels in Italy rose to shocking heights in the 1970s; there was chaos—perceived and actual—through the early 1980s. Such power in terrorist hands is always to be judged in relation to other political power; in Italy, central government was weak after decades of tumultuous parliamentary politics, enhanced Communist Party strength, and voter disillusionment with such matters as organized crime. Instead of teaching the value of democracy and the mechanisms of rule of law, some social science faculty were poisoning students with contempt of country. A powerful press like the Milan-based Feltrinelli's was no bulwark of the establishment; its heir, Giangiacomo Feltrinelli, was a paymaster of terrorists.[17] Hard-working Italian politicians who labored to build working coalitions of disparate parties failed more often than succeeded, and when Christian Democrat Aldo Moro built a bridge to the legal communists left in 1978, the Red Brigades immediately murdered him for it.

In hindsight, Italian incident levels make it almost incredible that republican democracy survived. That it did, and without even one month

of tyranny, is a lesson for all times. No dazzling new computer software or police science was the key. No one leader from the political parties took the helm and showed the way. Security forces were key—but not the only answer. The country's response was a hesitating and disjointed one, but it did succeed. Legislators studied and improved the laws on terrorism in several key ways.[18] By law, police were given greater powers to investigate and to detain suspects. A new group of judges was created to specialize in prosecuting terrorists—as also occurred in France. Terrorism ceased to be considered an anomaly, or a quirky expression of libertines, and became a named offense in state codes. A new provision, however, pointed the terrorists toward a "golden bridge," even as it threatened longer years in jail and encircled their rear with policemen: this allowed those who confessed and aided police to dramatically reduce their own sentences. This last point capitalized on the very size of the underground by giving openings to weaker cadre. The terrorist movement contained not just hardened men and women but also softer adherents or comrades grown weary; some of these were willing to talk when captured. *Pentiti* testimony locked up comrades for decades, and the more they gave away, the more the rigor of the remaining terrorists generally dissolved. This phenomenon illustrated the vulnerabilities of terror groups that sought to become broad insurgencies; counterintelligence and discipline problems escalated with growth. Combinations of legal punches and law enforcement knocked down so many Italian leftist terrorists during the four years 1979 to 1982. Italy also deployed a specialized police unit, which in 1982 freed NATO's Gen James Dozier from a Padua apartment staffed by Brigadists. Incident chronicles then fell nearly silent for the Red Brigades columns; most notations were of arrests of undergrounders, not attacks.[19]

In North America the early 1970s were notable for their violence. This followed the rise in civil rights activism and included several hideous murders of these activists by right-wingers. Problems were illuminated by arson and rioting in major US cities. The Vietnam War was a second source of domestic violence for Americans and Canadians.

The Quebec Liberation Front (FLQ) operated from 1963 into 1972. This nationalist, separatist, and leftist group was among the first active in the northern hemisphere. It broke away from a larger leftist group and took aim at military establishments and US economic and political influence in Canada. Evading police, one young leader returned to his native Belgium, while Raymond Villeneuve made a pilgrimage to Cuba, helping

initiate a long relationship between that island state and North American leftists going underground or seeking to land airplanes they hijacked. The organization survived initial police reaction, found support in anti-Ottawa sentiment in the French-speaking region, published the journal *La Cognee* (*The Axe*), and engaged new members such as part-time journalist Pierre Vallieres to write propaganda.[20]

Robberies and kidnappings built toward a peak between the summers of 1968 and 1969; there were 100 bombings, including the Montreal Stock Exchange. These produced vigorous police action by a government long known as quiescent and liberal. In 1970, the FLQ overreached with an elaborate plot to seize a British trade commissioner and swap him for prisoners. As this fell into shambles, the FLQ also seized Vice Premier and Labor Minister Pierre Laporte—soon strangled. Quebecois separatism prompted the Canadian government to rediscover a World War I–era "War Measures Act" that now allowed a range of state actions. Authorities introduced, against fellow Canadian citizens, such methods as agent provocateurs, systematic intelligence work, countless arrests, and detention without trial. Hundreds of FLQ cadre or sympathizers were entrapped. Within months the cause had been stalled; the country had become silent. Separatism still watered the soil of Quebecoise nationalism but in legal and fruitful channels, yielding election of the socialist and former separatist Pierre Trudeau as prime minister in 1968. This victory by a leader that the FLQ's Vallieres had mocked as a slavish compromiser could just as well be said to show how the democratic path can be an effective path—that a forgiving and undisciplined political culture (such as that of Weimar Germany) need not invite the empowerment of thugs (such as Nazis). Quebec separatists won "half a loaf," and it seems difficult to deny that terrorism was one cause of the change.[21] Now the separatist cause seems satiated; polling gives few indications of support for violence to further set the region apart from Canada. Terrorism ended in a combination of intelligence work, harsh law enforcement, and political accommodation.

Puerto Rico offers a related case in which serious cultural, linguistic, and political differences may threaten division from a larger, multinational country in North America. United States control of the island in the Caribbean dates from its war with Spain; Puerto Rico was a sort of spoil of war. Advocates of total independence have never been able to capture more than a bare minimum of the island's votes, but their track record of violent provocations is lengthy, reaching back to 1950, when they

nearly assassinated Pres. Harry Truman, and 1954, when they shot up the US House of Representatives. Arrests ended these cells; however, the thoughts and resentments that sparked the cases smoldered as embers and produced new flames in 1974 when the Armed Forces of National Liberation (FALN) appeared. They stunned New York City with a tavern bombing; incendiaries were laid in department stores, and dozens of attacks followed. The action then jumped from the eastern United States to Puerto Rico itself, opening a fresh front. Arrests and convictions, as of 10 perpetrators in December 1980, squelched the drive. Some argue that the group ended in 1982; certainly after 1983 there was little to keep the FALN name in lights. Policing succeeded.

The FALN case reveals the difference between a campaign and a war. One militant Puerto Rican campaign was finished—but not the war. A very similar group had been founded in 1978 and proved well prepared to succeed the faltering FALN. They called themselves Los Macheteros. Mixing leftism and nationalism, the new group was an ally of the Marxist-Leninist Puerto Rican Socialist Party (PSP), which itself had connections to Cuba. In 1978 the Macheteros staged simultaneous incendiary attacks on nine US combat planes at a military base near Isla Verde International Airport. Five years later, having placed a member inside the workings of the Brinks armored car service in Hartford, Connecticut, they escaped with $7.2 million. Some of it emerged in Robin Hood–style giveaways in Puerto Rican communities; some of it doubtless bought weapons and supplies; much of it appears to have gone to Cuba in a vehicle driven over the US border with Mexico.

The FBI took apart Los Macheteros with the same patience and thoroughness it would show later against rightists and "militiamen" in the US "patriot movement" of the 1990s. With surveillance, wiretaps, and other efforts (not to mention the special energy of an organization whose office in San Juan had been rocketed by Macheteros), the FBI disassembled this organization, brought its people to trial, and exacted lengthy sentences. Women and men, activists and journalists, social workers, and a Harvard University man were convicted in the late 1980s. The effect on the group was nearly terminal. There did remain Filiberto Ojeda Rios, a longtime Machetero leader. In 2005 the FBI found him, armed, in a house on the island; he died in the subsequent gunfight.[22] Los Macheteros may be counted among the "deceased" of late-twentieth-century terrorist organs.

The proximate cause of their expiry was devoted work by law enforcement and successful trials.

After a century of using Vieques as a bombing and gunnery range, the US Navy ceased such practices, removing one cause of discontent in Puerto Rico. Perhaps a larger cause of the near-total containment of terrorism by the government has been inadequate support for it by other Puerto Ricans. The island of four million people,[23] as a whole, neither votes for nor supports bombings and killings for independence. There is no mass support, above or below the political ground level. On the other hand, Los Macheteros was a success for some years. Preceding it came other waves in this pool of ethnic and nationalist resentments, which may well be stirred by further storms.

As the twentieth century closed, another nationalist-separatist fighting force with long tenure and a solid level of performance and skill seemed in profound trouble. Basque Homeland and Freedom (ETA) in Spain still has fighters in the field and other operational capacities but is at an all-time point of weakness. It survives, but barely; it strikes against Spain, but rarely; it makes headlines, but usually for capture of ETA shooters or financiers by the more clever security forces of Madrid or Paris. The ETA is still standing but may be on its last legs. If the ETA ends, it would be significant to *world* terrorism: the group is a half century old, has killed nearly 900 Spanish in its operations, and has represented a model and been an occasional partner to other terror groups. Among its successes must be counted the attraction of foreign support—guns from Libya, perhaps advice from Soviet agents, certainly training grounds in Soviet bloc client-state South Yemen in the 1970s—without ever being soiled in its image as an indigenous and independent revolutionary force. This is a difficult balance to strike, but the ETA has done it well.

Formed at the end of the 1950s, the ETA focused on propaganda and political front activities, initiating systematic violence only years later. Principal Spanish political and security force personnel and *Guardia Civil* gendarmerie were the usual victims. Shooting was a preferred method; later would come the car bombs, with their far wider swathes of "collateral damage" to other Spaniards. Assigning a "revolutionary tax" to Basques who were, and were not, engaged in revolution was an innovative and successful financing means the group has never abandoned. But weaknesses were also present. Internecine quarreling over ideology plagued the early decades, with some leaders favoring pure nationalism, while another

strong wing wanted to rally behind declarations of communism and global revolution. Two larger problems were also political. First, Spain emerged as a strong democracy as the death of Francisco Franco in 1975 led to the benign monarchy of King Juan Carlos, who transferred some powers to the National Assembly. Second, in a move largely ignored by the outside world, the central government bestowed on the Basque lands a high degree of autonomy as to culture, local law, and language. The ETA reacted violently, probably sensing the subtle dangers (to a terrorist movement) in this prudent concession by Madrid. Over time the government reform had effect, helping to divide the ordinary Basque from his confrere in the terrorist underground.

Today the political fronts that were once so helpful to supporting ETA violence are gravely weakened. Several have been banned by Madrid, including Herri Batasuna (Popular Unity), which in the early 1980s was second in strength among Spanish political parties. Herri Batasuna changed its name to Batasuna, only to again be proscribed. In 2007–2009 the most noted spokesman for the front, Arnaldo Otegi, was under intense police pressure. The larger political challenge is that typical Basques no longer respond to ETA battle cries; indeed, the largest parade on the nationalist issue the country has seen in recent years occurred in January 2007, and it was *against* ETA terrorism.[24] A final problem is almost overwhelming for the dwindling ranks of ETA terrorists: Franco-Spanish cooperation is at all-time highs. The president of France and the prime minister of Spain met in Élysée Palace in January 2008 and have gone so far as to create a small binational policing unit.[25] This now continuous binational cooperation and other dimensions of good grand strategy are wrecking the ETA.

Two other famous and long-standing terrorist entities might have been comparatively studied until May 2009. Both were Marxist-Leninist; both had enjoyed protracted periods of leadership continuity; both were wealthy; they had been successful as insurgents and leaders of "shadow governments," protecting large swaths of territory, and were thus much more than "bite and flee" attackers of civilian and military targets. Mao Tse-tung's "phase two" warfare, combining guerrilla efforts with semi-conventional and positional warfare,[26] is the best descriptor of the nature of these two very important organizations. The FARC communists of Colombia and the LTTE (Liberation Tigers of Tamil Eelam) separatists and communists in Sri Lanka have been feared for their skills in varieties of fighting and terrorism. Now the latter appears finished, but the

Colombian government must be especially careful. One of the common sins of counterinsurgency is overestimating successes, of which there were many during 2007 and 2008. Bogota has more to do, and Colombia's president will soon complete his second and final term of office.

After 2001 the government and armed forces of Sri Lanka were seized with a profound determination that has resonated with their polity and allowed a concerted national effort against a powerful in-country enemy. The 1980s and 1990s had seen many ground battles, which together with LTTE terrorism had left over 65,000 dead. A negotiated peace made for a few quiet years but was overturned in 2006 and replaced by the most intense fighting. Advances by government ground forces and the recapture of key towns occurred in late 2008; the spring of 2009 brought the killing of leader Velupillai Prabhakaran. Leadership and fine armed forces wrecked the guerrillas and terrorists of the LTTE. After 35 indomitable years, Prabhakaran and many top officers are gone.

Some Groups of Religious Bent

Terrorism is always political. In the late twentieth century it also became more religious. The 1970s and 1980s offered several extreme versions of Christianity and Hinduism, which caught up "true believers" in militancy. Sikh sects were active—and killing—internationally in the mid 1980s.[27] There was long-running violence from the Jewish Defense League in the eastern United States. By 1988 one could discern newer groups of religious bent—or bent religion. A majority of the new groups founded since 1990 avow religious objectives—in front of, or parallel to, political ones.[28] Most such groups deserve to be taken at their word. Iran's officials supported (then and now) groups of both Sunni and Shia faiths. Beneficiaries include HAMAS, which in its well-crafted charter took an integrated approach to conceptual support for struggle and violence that combined ideas of Sunni Islamism in the realms of politics, culture, society, even the arts and the place of women. There are, newly in evidence, many more religion-inspired political movements in the traditional "arc of crisis" from North Africa through the greater Middle East into Afghanistan and Pakistan.

The 1990s also saw the crest of Aum Shinrikyo (Supreme Truth), strong in Japan and Russia. It offered an eccentric mix of worship of Shiva (Hindu goddess of destruction), certain precepts of Buddhism, fashionable mysti-

cism and self-help, and the claims to deity of its founder, Shoko Asahara. Among other innovations, Asahara expanded the Buddhist precept of *poa* into an excuse for mass killing for the "altruistic" purpose of releasing souls for reincarnation in higher forms and better status.[29]

Such perverse ideas amid a cult of personality led directly to some of the first uses of weapons of mass destruction (WMD) by a substate actor. Asahara had not always obsessed over WMDs, but his views darkened dramatically after efforts to compete in political elections to Japan's Diet in February 1990 brought in few votes. Humiliation set arrogance and self-interest together on the road to terrorism and, ultimately, mass murder. Asahara hastened his scientific programs, which came to include beam weapons, Ebola virus, and efforts to acquire uranium. Aum conducted its first WMD attack in April 1990—with botulism. Another dozen WMD attacks of varying type and considerable originality followed, including the use of botulinum toxin against the Imperial Palace in 1993, a killing with sarin in Matsumoto in June 1994, and a subway attack the next year with briefcases dispensing toxin (botulism, again) through built-in fans. More failed than succeeded, but all prepared the cult well for 20 March 1995 and success with sarin on subways. The world was amazed as Tokyo lay stunned. Maiming more than it killed, the gas traumatized the Japanese national psyche.[30]

Aum's strengths included fanaticism peculiarly combined with the high education levels and scientific training of many top cadres. There was also a fruitful collaboration with Russia. Thousands joined in that country, but more importantly, high-level military and government and scientific circles in Russia sold or gave Aum many valued prizes, from commando training by former KGB experts to a military helicopter to a formula for sarin.[31] Finally, there was the remarkable budget of the cult and its enormous infrastructure, especially in Japan; these were massive and doubtless helped with political influence and deterred punitive suits. But the most important of Aum's strengths, the one that most prolonged its life prior to 1995, was Japanese tolerance. A society long known to permit or indulge religious societies and cults, Japan is also a liberal democracy as hesitant as postwar Germany to display a heavy hand in domestic or foreign affairs. This religious, social, and political tolerance was stretched beyond all limits as Aum increasingly preyed upon wider circles of Japanese civilians in the early 1990s. There were kidnappings, druggings, shamelessly inept "medical treatments" in their clinics, disciplinary murders, illegal disposal

of corpses, and outright attacks on public figures such as a judge who had made anti-Aum rulings in property cases.

The cult's weaknesses, by contrast, were few. Aum required a relative minimum of members, being flamingly elitist in its practices and planning. If public support could not be mustered in elections, it was enough to have the public ignore most of the cult's actions. Even the visions of the apocalypse that darkened Asahara's mind were a source of certain strengths, forcing cohesion, permitting discipline, and eliciting tremendously long work hours from members. Only the excess of terrorist killing in the final, successful sarin attack brought about the group's end. Once government and police were confronted with the act of 20 March 1995, they snapped to attention and dismantled the decade-old organization. Japan arrested some 400 members; thousands quit on their own. The guru founder and many top leaders went to prison. Administrative proceedings immediately placed Aum in formal bankruptcy, although their legal charter to exist was not revoked, it seems. One can argue that Aum was decapitated by arrests.

Some Japanese security officials think Aum's successor "Aleph" bears watching. If thousands of original members left the group in 1995, several hundred did not or later returned, including several top officials complicit in the former violence. These include Fumihiro Joyu, who was jailed for three years only to return, gain control of Aleph, and direct it for a half decade—until a March 2007 schism. None of the capital sentences for murder have been carried out, and many lesser Aum criminals have left jail. The new group is also rebuilding physical infrastructure. The shell company that made computers never disbanded in official bankruptcy proceedings by the state and was soon prospering again, with tens of millions of dollars in sales by the late 1990s. In 2002, *Kyodo News* reported that such sales and the way Aleph "places the highest level of importance on developing cyber skills" and "identifies itself as a cyber cult" were reasons for US intelligence concern about a cyber attack by the group.[32] As of 2005, Aleph owned 26 facilities as well as another 120 residences, according to Japan's national police, and 650 members were living collectively in compounds. Canada, the United States, and the European Union all classify Aleph as a terrorist organization.

Other religious terrorist groups of the late twentieth century have not merely evaded arrest for their crimes; they have flourished. Hezbollah was born among Lebanese Shia in 1982, and HAMAS is a Palestinian Sunni counterpart begun some five years later. The trajectory of each helps explain

(1) how religion works with politics to produce successful terrorist organizations, and (2) how some terror groups end in success—both have achieved political power by degrees, even if their ultimate objects have not been won. Hezbollah and HAMAS are sophisticated and dangerous.

The so-called Party of God (Hezbollah) began by emphasizing a role as the "Organization of the Oppressed on Earth"—another of Hezbollah's many names. It prudently never abandoned this arm of activity. Human needs are abundant in Beirut's Shia slums, and Hezbollah's effective shadow government is at work nourishing, nursing, educating, and propagandizing among those people. Such labors have always helped to make people ignore the rank hubris in calling itself "The Party of God," on the one hand, and have helped to justify and excuse its terrorism, on the other. Indeed, the infamy of the 1980s' days of kidnapping, torturing, and killing hostages—including Germans, Frenchmen, and Americans—has all but passed out of today's parlance; it has been some time since Hezbollah acted in such ways against Westerners. Even after the death of intelligence chief Imad Mughniyah (in Syria in 2008), this remains an organization of capable terrorist operatives—but their emphasis is of other kinds: guerrilla war and politics.

Against any opponent, especially the Israeli Defense Force soldiers, the organization offers a sophisticated and developing array of methods and techniques, from well-disguised road bombs to antiship missiles to unmanned aerial vehicles (which may one day be armed). Several thousand men and women are armed by Hezbollah; many more thousands are trained or active supporters. Its discipline and ability has been recognizable to military analysts for a decade and a half and to the world after July 2006, when Hezbollah forces fired rockets into Israeli territory. Hezbollah has another arm, the political. Its skills well suit the freedoms of action offered in a relative vacuum of Lebanese life, where central government is weak and past official pronouncements about Hezbollah's existence and de facto rivalry to the state are permissive or even apologetic.[33] Finally there is the media arm of Hezbollah: outlets led by *Al Manar* television. When Israeli bombs destroy the antennas or studios, *Al Manar* resurrects—another proof of the way political infrastructure, religious motivation, and state sponsorship may enliven terror organizations under even the most intense pressure. Like the FARC in Colombia or the New People's Army in the Philippines, the Party of God can seemingly absorb any number of

hard hits, year upon year, and carry on, planning for an indefinite future. Conceivably, Hezbollah might one day lead a Lebanese coalition government.

HAMAS, the Islamic Resistance Movement, was formed in late 1987 amid the clatter of stones and bullets in the First Intifada. Like Hezbollah, it enjoys huge subsidies from Iranian coffers—even while declining to walk the Shiite line in religious affairs.[34] Individuals and groups of Palestinian expatriates worldwide supply other money and aid, as from the United States, Europe, and the South American "Tri-Border Area." Secular Syria gives fulsome support and always has, despite profound differences of political ideology. These Palestinian terrorists, politicos, and undergrounders began with the slingshot and the knife and graduated to an array of weapons, especially the vehicle bomb—yet another "lesson learned" by watching Hezbollah.

While HAMAS lacks its Lebanese counterpart's skills in complex guerrilla war, it is possessed of a smooth and practiced political touch. It campaigns and competes well at the polls and did so long before stunning Fatah (and outside observers) with a January 2006 electoral victory in Gaza. That led in turn to a June 2007 formal political regime in Gaza that rivaled Fatah's control of the West Bank and also allowed the periodic launching of rockets into Israeli towns.[35] "Owning" Gaza, HAMAS had the power to gather rockets, the ability to launch them, and the responsibility for the war they produced with Israel. The organization also defies decapitation efforts and continues its attacks on foreigners, especially Israelis, and its bloody rivalry with Fatah Palestinians. HAMAS has sums of both power and legitimacy—and grapples for more. In its charter, which lays down its views on society, religion, politics, the arts, and so forth, there is an absolute and oft-repeated proscription against compromise or any mediated solution to "the Palestinian problem," which surrenders any authority over any part of the land.[36] Negotiations, not to mention pathways out of violence, are never easy. It is most challenging to make inroads with a religiously motivated terrorist clan; negotiations will not make HAMAS quit, or even quit fighting Fatah. The group is a success.

Terrorism in Nine Parts

A sweep of the twentieth century proffers innumerable examples for the study of how terror groups end. There are hundreds of terrorist groups—too many to master, or even mention, in one article. And there are many different ways to approach this considerable analytical challenge. Ex-

cluded here are several notable false starts, such as the odd notion that terror groups have a natural lifespan. Arguing for the latter ignores the varied and important factors that limit or enable terrorism, ranging from governmental responses to the internal and strategic choices leaders make.

Terrorism can be classified by the leading ways most groups meet their demise; for example: defeat by security forces, defeat by decapitating the leadership; defeat by government's good grand strategy, folding into pacific political life, or terrorist success. The present, more chronologically oriented approach shows a different aspect of terrorist groups. It comes to conclusions about a given group under a pair of analytical rubrics: duration of the group's life, with emphasis on significant actions or years of "main violence"; and extent of successful results. Studied under the first rubric (I) are terror groups whose campaigns are of short duration (five years or less). Groups that ran for a medium length (8–15 years) are rubric II. Rubric III shows protracted terrorist campaigners whose efforts last from two to five decades. With crosscutting analysis, we identify first, organizations that end in defeat; second, those that achieved or are achieving limited success; and third, groups that have largely succeeded or appear to enjoy strategic successes now. (See charts on pages 75, 76, and 77).[37]

I. Short-Lived Organizations

Defeated. Scores of twentieth-century terrorist groups have had very brief life spans, as little as three to five years. This fact, and the swiftness with which the public forgets them, ought not to mean neglect of *how* they were defeated or brought into decline. Analysts and strategists have often declared that it is best if government can interrupt terrorism or insurgency in its incipient stages.

Among the first of these in post–World War II history was the Secret Army Organization, founded to save European settlers' status and French power in Algeria, but that totally failed within a year and a half—by mid 1962. Certain other European rightist groups were to have lifespans of similar brevity, or do only marginally better. In 1980, for example, there was the aforementioned neo-Nazi scare, a natural result of massive bombings in quick succession in Bologna, Munich, and Paris. The Paris assault, however, was by Palestinians using an invented French cover name, the Federation of National Action. In Germany the "Military Sports Group" of Karl Heinz Hoffman bombed the Oktoberfest in central Munich; a year later, this clan was on the ropes. Members went to the Near East

for Palestinian training and "were arrested on their return to the Federal Republic. . . . Hoffman was jailed in 1981, after which the group ceased to exist."[38]

American examples of total failure and precipitous decline are too numerous to chart. Illustrative are four groups of the 1970s and 1980s, at different ends of the ideological spectrum: the Symbionese Liberation Army, the United Freedom Front, the Order, and the Army of Aryan Resistance. The first two of these gun gangs were black-dominated leftists who held up banks and shot patrolmen while dreaming of status as a revolutionary vanguard. The other two were white-power groups on the political far right. None of these enjoyed even three good years of real power in their respective undergrounds. A common theme of such cases, in Europe and America, is good and aggressive police work and resultant attrition through both arrests and gun battles, sapping these secular, racist, and militant organizations.

Myriad fragments of militant life have burned briefly and expired shortly. Consider Latin America. In Bolivia, the endlessly romanticized Cuba veteran Che Guevara started a National Liberation Army that never exceeded 51 troops. It formed in 1966 only to see Che and another leader killed the next year. That drama inspired a successor in Brazil named the October 8 Revolutionary Movement, which was swiftly reduced to virtual invisibility by a wave of arrests in 1969. Later, as remnants folded back into Brazil's official Communist Party,[39] a further Brazilian spore failed to flower, let alone take root: the National Liberating Action existed from 1968 until 1971.[40] Europe experienced many such flickers and flights. In Holland, long-gone entities include the Free South Moluccan Youth Organization (1975–1979) and Red Youth and Red Help groups of the early 1970s. Italy's rightist Revolutionary Action Movement ran for only half a decade in the mid 1970s. There was the New Force, which lasted six years in Spain, passing from the scene in 1981, and Portugal's yet-shorter-lived New Order. Belgium's Communist Combatant Cells surely hold some form of European record for brevity. They operated only from October 1984 to December 1985, whereupon the arrest of all four members terminated their tactically effective campaign of two dozen nonlethal bombings of German, Belgian, and other NATO targets.[41] Belgium went quiet, as before, and remained so.

Thus, a range of twentieth-century groups have been stalled or stopped cold in a few years. These include many secular ones, most of them communist. There are also several good right-wing terrorist examples.

Limited Success. The known terror groups of short duration were not all total failures, however; some can claim limited achievements, if only when judged by their own lights or the praise of their own community or prestigious mainstream partisans. It is reasonable to study the US Black Panthers in this way.[42] Colombia offers its own case of a militant organization that began with claims of virtue, degenerated into crime and terrorism, and came to an end after a few short years: the United Self-Defense Forces of Colombia anti-leftist militias. The leader disappeared, mysteriously and permanently, and the group demobilized after successful negotiations on amnesty with the government. This examination of terror groups yields few that are *both* short-lived and successful in limited ways. One is a leftist revolutionary and single-race organization in the United States, while the other is a broad "preservationist" terrorist organization that flourished in Colombia.

Successful. There are still fewer clear examples of terrorist movements of short duration that came to enjoy total success. Communism did win a violent triumph in Cuba, with remarkable swiftness; but most judge that success came far more from guerrilla war and political work than from terrorism.[43] If one leaves aside the Cuban case, there may be no short-lived classic terror organizations that succeeded so completely, in so brief a time.

II. Midterm Lifespans

Defeated. The twentieth century's offerings under rubric II—medium-length terrorist campaigns—are numerous and varied. Some perish in exhaustion, be it physical, psychological, or organizational; an early post–World War II example was the fatigue of Luis Taruc's Huks in the Philippines. Their insurgency and flagrant terrorism[44] ran hard into many obstacles, especially defense secretary and later president Ramon Magsaysay. This government wore out its enemy with sophisticated grand strategy. Good political leadership inspirited the new democracy. Fine intelligence work captured a full politburo in Manila. A clever "free land" program seduced away some Huk cadres and demoralized others by answering their calls for "land for the landless." Well-trained, disciplined armed forces protected the Filipino people while hunting down terror cells. Eventually, the rural leadership under the labor activist turned communist Taruc capitulated.

The campaign ran from 1946 into 1955, a decade. Good leadership and good grand strategy defeated the Huks.[45]

Other forms of terrorism in the Latin world of the 1960s through the 1980s lasted eight to 15 years until totally defeated. Many important and compelling revolutionary terrorist organizations were crushed by governmental force. These included the Tupamaros of Uruguay,[46] who prompted a military coup, and the Montoneros of Argentina, whose cells were ground to pieces by government networks of intelligence, police, and soldiers. El Salvador offers a different kind of case study. The FMLN, a front group of some five guerrilla groups deeply engaged in nationwide terrorism and semi-conventional battles against the military, was finally brought to an end, but not because their demands were satisfied, as one strangely errant new study claims.[47] It was due to a combination of Salvadoran government and military resistance, enormous financial and intelligence help and military aid from the United States, the decline of Soviet bloc aid, and the close and skillful diplomatic engagement of neighboring and international states in a regional peace process. The latter included the United Nations and states such as the United States, but the most important actors were Mexico and Contadora countries.[48] This last factor was very important. Like the negotiated conclusion of IRA Provo violence in Northern Ireland, it suggests that at the right moment, negotiation may offer opportunities, even with terrorist enemies.

Western Europeans also grappled with terrorism from the 1960s through the 1980s. Another dozen campaigns of medium length by self-avowed "urban guerrillas" unfolded in cities and towns but were doomed to defeat. The far left's fascinating failures included the Turkish People's Liberation Army (TPLA, 1969–1980); Portuguese of Popular Forces (1980–1986); German anarchists of the 2nd of June Movement (1971–1980); the Baader-Meinhofs in Germany, whose main violence ran from about 1968 to 1977; Front Line, in Italy (1976–1981); [49] and Action Direct in France (1979–1987). The Italian left was torn apart by dissidents and *pentiti* (repentants) who, under prudent new laws, offered testaments against their former colleagues in exchange for light sentences for themselves.[50] In most cases, the European Marxist-Leninist organizations were slowly ground down by civilian law enforcement. The TPLA was different; it was among the Turkish clandestine political organizations forcibly suppressed by a 1980 military coup. The Army took power, defeated many terrorist groups, and ceeded control back to civilian authorities.

A few of these rubric II groups (8 to 15 years of major violence) have a longer, less-crisp profile: they rose, fell, and yet still defy eradication. Peru's Sendero Luminoso has existed since the early 1970s and determined upon armed resistance in 1977 but did not openly attack until 1980. Thirteen years later, the gravest of blows reversed its rise toward national power. In September 1992, a tiny police intelligence unit located leader Abimael Guzman and made an arrest; he has since been locked up on an island under Navy control. In practical terms, the Sendero Luminoso campaign ended there, but the insurgency had sunk roots, and a scattering of militants never left the field. As a hardened Maoist, Guzman would know the stories of the twentieth-century "comebacks" after jail or hardship—Adolf Hitler, "Long March" leader Mao Tse-tung, Mahatma Gandhi, Nelson Mandela, and others. So, while the self-described "Fourth Sword of Marxism" kept to his cell during the 1990s, a few remnants stumbled along the shining path of continuous revolution, enlivened by the obvious limitations of Peru's central government and unchallenged by rivals on the left. In 2007 and then 2008, a few reporters stretched to insist that Sendero is reviving.[51] More conservatively, we argue that its ideological convictions have allowed it to fail without disappearing. Meanwhile, Shining Path's former leftist nemesis, the Túpac Amaru Revolutionary Movement (MRTA), has totally disappeared. It was weakened in the mid 1990s and crushed by government security forces in 1997.

There are many "studies in defeat" for groups of midterm duration. All imaginable ideological categories are included: leftist, odd combinations of left and right, a religious cult, and others. Some of these groups are mostly urban in their focus, but the range includes many insurgencies as well.

Limited Success. There are also examples of terrorist groups that practiced violence for eight to 15 years and ceased operations with a feeling of considerable (but not total) success. Some of these existed in the Eastern Mediterranean as anti–British Empire organizations in Cyprus and the Jewish underground.

The National Organization of Cypriot Fighters (EOKA) was an unusual case of a post–World War II nationalist and ethnic Greek group that used terrorism and repudiated Marxism-Leninism. Remarkably independent, it lacked the kind of heavy external support and sanctuary to which some always ascribe insurgent success. The EOKA was founded in 1951 by George Grivas; he arrived on the island three years later; April 1955 saw the opening of guerrilla war; the violence combined with negotiations

to force British troops to abandon Cyprus; independence came in 1960. This was, however, but a partial success. Grivas and his sophisticated organization were of the 80 percent on the island whose blood was Greek, not Turkish, and the revolutionaries dreamed of full unity with Greece, not a separate state. A decade later, phase two of the struggle opened under the command of EOKA-B. Now the underground cells attacked indigenous Cypriots, took hostages, and raided armories in a renewed campaign to seize the whole island for unification with the mainland. George Grivas died of heart failure in 1974; attrition and jailing took further tolls on his organization. A December 1977 kidnapping of the Cypriot president's son in a plot to free colleagues from prison failed. The group announced dissolution in the next year.[52] Their legacy is thus mixed: a two-part campaign separated by a decade of peace left partial success—the expulsion of the British army and government but not a unification with Greece.

Several Jewish organizations fighting inside the British Mandate may also lay claim to a degree of success after mid-length campaigns. The achievement of an entirely new and free democratic state of Israel in 1948 appears to some people to justify the actions of Irgun Zvai Leumi, Lohame Herut Israel, and others. In fact, their terrorism is no more redeemable than that of African National Congress/Spear of the Nation bombers, burners, and assassins whose efforts contributed to destroying apartheid in South Africa. The model for Jewish liberation fighters is no terrorist organization but instead the Haganah, the mass organization that consistently and successfully resisted Arab, British, and Nazi rulers and deployed guerrilla attacks against their military assets. They were the militant Jews who most succeeded with war, but two further groups—both terrorist—helped destroy British authority over Palestine. The Irgun Zvai Leumi (IZL, or Etzel) was founded by David Raziel in 1937 and was led after his death in 1941 by Menachem Begin. The IZL used terror against the Arab population as well as British targets. The latter included the King David Hotel (1946), which had both civil and military administrative functions; that attack killed 91 people and was later detailed in Begin's autobiography *The Revolt*.[53] A fanatical group broke away from the IZL in 1940, damning its truce with the British during years of war with the German Reich; Abraham Stern's gang was formally known as Lohame Herut Israel (LHI, or Lehi, or Lechi).[54] Their attacks on Jewish rivals mirror the inter-ethnic slaughters of a hundred of the twentieth century's terror groups. The Stern Gang leadership moved to David Yassin in 1942, and the group continued

killing: Jews; the British, including Lord Moyne;[55] and, most revealingly, Sweden's Count Bernadotte, whose very purpose was to negotiate peace in Palestine. Here, too, was a revealing terrorist pattern: the explicit war upon peacemakers.[56]

Several other terrorist groups might claim limited success after a campaign of eight to 15 years' length. A marginal case is the Armenian Secret Army for the Liberation of Armenia (ASALA), which left many more bloody spots around Western Europe, hitting hard as late as 1986. Its leader perished two years later. Soon thereafter the Republic of Armenia came into being. This was primarily due to the disappearance of Soviet power, but it dramatically undercut the perceived need for terrorism and brought relief to militant nationalists who had earlier waved the flag and the gun.

Successful. The final parties to tier II are the more successful terrorists, whose mid-length campaigns brought them to power. The century's first success, the Bolsheviks, achieved the near-impossible between 1905 and 1917, taking total power and immediately using it to terrorize and destroy their innumerable enemies on the left and the right. History's next example might be the more moderate National Liberation Front (FLN) of Algeria. Fatigued with years of squabbling between militants and reformers, the FLN sprang to life in late 1954, published a short, powerful declaration to which they adhered closely, and took power in Algiers in 1962. These politicians, diplomats, guerrillas, and terrorists set the revolutionary standard for the post–World War II era. For example, their clever and violent methods of crushing Algerians opposed to them as "the sole legitimate voice" of nationalism would be aped by Palestinian militants under Yasser Arafat's leadership. They also exported the revolution to the Algerians in France, extracting funding, killing opponents, and undermining French desires to hold the Central Maghreb. The FLN shows how terrorism may end in success.

Central America offers the case the Nicaraguan Sandinista National Liberation Front (FSLN). While many neighboring revolutionaries failed or slipped into dormancy (e.g., Guatemala, Honduras, or Mexico), the Sandinistas won and won completely. Founded by 1961,[57] at a time when the Cuban and Algerian FLN examples were heated inspirations, the Sandinistas were revolutionary but enjoyed broad popularity among frustrated farmers and other reformers. Soviet bloc provisioning and Cuban direction were of great help in shaping the group. Their main period of

violence is of midterm duration: 1963 to 1979. They slowly discredited the Somoza dictatorship and rattled the regime with terror attacks and strikes on the National Guard. Not long after the United States nervously withdrew support to the sitting government, the Sandinistas marched into Managua (July 1979). The regime lasted 11 years; then the Sandinistas dared to risk elections and lost. But the turning screw of history kept on, and after years in the wilderness, they returned to power, winning elections in November 2006. Daniel Ortega is president again.

Asian insurgencies on the Maoist model also demand attention, especially the Khmer Rouge and Communist Party of Nepal (Maoist), or CPN(M). The former hacked its way into the capital in 1975 and ruled until expelled in late 1978 by the stronger army of Vietnam. Comrade Prachanda's Nepalese Maoists also began slowly and with protracted war, taking over swaths of countryside by combining overt politics, clandestine organization, terrorism, and guerrilla war. Then, as Nepal's monarchy tilted in impotence and reformists began calling out in Katmandu, the CPN(M) cut a remarkable political deal that put Prachanda into the prime minister's chair in 2006. His promises to demobilize his thugs have only been partially kept, which means that if overt politicking ceases to meet the party's needs, other options remain. No one need hurry in a protracted war.

Thus, a midterm lifespan does not signal defeat, necessarily. Religio-nationalist groups in this category have flourished and survived for many years and eked out demonstrable gains. Several secular leftist and revolutionary organizations using terrorism have similarly enjoyed limited success. Their will to survive and their gains over time indicate the truth in an old maxim about guerrilla war: that in some ways, merely to carry on fighting is to succeed.

III. Groups with Longevity

Defeated. The third and final tier is organizations with great longevity—protracted campaigns by terrorist groups. Some were ultimately and thoroughly beaten. The international anarchists, dramatic actors of the last two decades of the nineteenth century, all but ceased affecting the political world after 1920. Later an ideological opposite emerged with similar fate: the effort of Chin Peng and others of the Malayan Races Liberation Army to create a communist state ended formally with his surrender, after decades, in 1989.

One might reasonably take the long view of a "war"—rather than study a given group's shorter "campaign"—when examining nationalist militants in Ireland or in Puerto Rico. Puerto Rican nationalist attacks in the early 1950s, the latter 1970s, and the early 1980s all melted away, as tactical successes had no real strategic results. Successively, the Puerto Rican Nationalist Party, the FALN, and then Los Macheteros have won no important political change. The commonwealth remains a commonwealth; polling data still show revolution or total independence to be a far-fetched idea; new recruiting is miniscule; no foreign powers have stepped in to aid the militants other than Cuba—now largely inactive in this respect.

The Tamil Tigers of the LTTE lack roots so long, but they did begin as early as 1972.[58] They survived innumerable government campaigns and were only smashed in their "liberated zones" in early 2009. Another communist group of very different and urban character enjoyed almost as long a lifespan but was decidedly less lethal. The Revolutionary Organization 17 November was made up of a handful of Greek Marxist-Leninists who operated in Athens for a quarter century. They attacked Greeks, Americans, and NATO personnel—sometimes using the same Colt pistol—and also targeted multinational corporations. They managed to do so year after year, never even suffering a single arrest. But the small size which made this evasion possible[59] also flagged N17's unpopularity and failure to recruit. Lack of numbers likewise determined that if all operations might be secure from police, there would be very few operations. As the 2004 Athens Olympics approached, Greeks in government took a new attitude toward terrorists. A break for security forces came when an N17 man failed in a bombing, wounded himself, and then talked. Immediately, most of the small organization was arrested, and trials led to long sentences. N17 has come and gone.[60]

There are certain examples of fighting groups that devoted decades to their will to power and yet failed entirely. Those studied here are mostly internationalists of one sort or another, including anarchists and leftists. Two communist insurgent groups also manifest strong quotients of nationalism in their work. If one examined state terrorism sponsors, Libya's three-decade record would fit here—as a failure.[61] It is more common, however, for a well-organized fighting group to achieve more over time, to create "liberated zones," or otherwise make permanent effects, which brings us to the next rubric.

Limited Success. Terrorist groups of protracted duration that have achieved limited gains are many and richly varied. We may study the Provisional Irish Republican Army (PIRA) as a discrete entity, a guerrilla and terrorist organization with an intimate party affiliate. It began in a 1969 split with other nationalists and ended its violence against unsuspecting civilians with the 1998 Good Friday Accord. That Irish Republican Army (IRA), so delimited, is a clear case of limited success. Militancy had of course cropped up often before the twentieth century, as when Napoleonic France aided Wolf Tone and a few decades later when Americans began shipping weapons and money to insurrectionists in Ireland.[62] A periodically successful Irish fight began in 1916 and manifested guerrilla and/or terrorist variants. The IRA had some sleepy years in the twentieth century but came to life as the "Provos" in 1969 and 1970, fired with passion over civil rights as well as nationalism and a dash of Marxist-Leninism. A few British overreactions, and indeed the 1972 "Bloody Sunday" event, encouraged the hard men and drew in recruits. By the 1990s, many felt a kind of stasis; the Provos could neither win nor be beaten. Their leaders bent more to politics and sought to do less with terrorism. They negotiated with London, won limited concessions, and joined governance circles in the Stormont-based parliament in Ulster. There is no unification of Northern Ireland with the Eire republic, and the IRA Provos submitted to disarmament—or partially so. On the other hand, the Provos have seen comrades released from jails by the score; they operate openly, peaceably, and respectably; they have not surrendered their many foreign friends; and they can return to terrorism if they so decide. This could occur as a group effort, in theory, or more likely, scattered individuals may choose to join extant splinter groups such as the Real IRA.

The irony in this is that the Orangemen, too, can claim partial success from terrorist campaigns. And perhaps they should. The Ulster Volunteer Force (UVF), which declared war on the IRA in 1966, and the Ulster Freedom Fighters (UFF), begun in 1973, are as able as the PIRA/Provos' Gerry Adams and Martin McGuinness to see a "partial victory" in the status quo of the last decade. They fought below and above ground for decades, hurting as many Irish as English, and securing prestige and precious political space in that tormented island. Unlike smaller killing squads (e.g., the Red Hand Defenders), the UVF and UFF also work with political fronts, making them more significant and more morally credible. Now these major Loyalist groups have put down guns and taken up balloting; all their sup-

porters, in English and Irish politics, may see the former terrorists sharing banal administrative duties and profound political responsibilities in a new parliamentary structure in the Stormont parliamentary building just outside Belfast. The Orangemen of illegal bands are "preservationist"[63] terrorists who have arguably helped keep the six counties under the British Crown; at least, few would dare tell them otherwise.

Twentieth-century history is crowded with candidates for this rubric of protracted campaigns leading to limited success. American labor militants—a few of whom were terrorists—gradually won major concessions, first in wages and then organizational rights and later in benefits, and came to struggle pacifically and successfully in recent decades. The traditionalist and racist American Ku Klux Klans have atrophied drastically. Once a mass movement, now but numerous cells; they have never disappeared in 150 years of influence. In Colombia, the FARC and ELN are examples of rural insurgencies, widely using terror, that seem ineradicable and have endured for half a century. That mark may one day be met by India's Naxalites—Maoists who are, in effect, a shadow government in certain areas. Western Europe's ETA Basques have lasted exactly a half century. France remains bedeviled by the Corsican National Liberation Front, which still lights up strings of bombs to keep alive hopes of withdrawal from France and its system of district governance—as Algeria succeeded in doing in the insurgency ending in 1962. France is also troubled as the European home to the secular and ideologically vague People's Mujahedeen of Iran (PMOI), also known as the People's Mujahedeen al Khalq (MEK), which is still under veteran leaders' wings. Contained and disarmed on Iraqi territory and subject to US and Iraqi controls through 2008, the MEK still flourishes politically abroad. While this is especially true in France, the MEK also enjoys friends in the halls of US and European national parliaments.

Certain Middle Eastern groups are marginal but unrepressed; these include the Popular Front for the Liberation of Palestine–General Command, a Syrian-supported terror outfit that has operated for decades with no one to control it but Israeli forces. Hezbollah has turned covert and overt organization and violence into de facto political control over large swaths of Lebanon.[64] Its success in national politics in Lebanon has been immense, as indicated by its presence in political bodies and the national political life. The "mainstreaming" of such terrorists is a reproof to thinking that terrorism "has always failed and . . . will fail again," as one post–9/11 argument proclaimed. Much more narrowly, a think tank report of

2008 about the fate of terrorists concludes that "Religious groups rarely achieve their objectives."[65] Even that more careful view is misleading—given the impressive if incomplete successes of such religious-based groups as Hezbollah and HAMAS.

Analysts may find innumerable cases in the range of moderately successful groups engaged in protracted struggle and terrorism. From the radical rightist and preservationist terror groups, one may look to the left, and nationalist-leftist, and onward to religiously motivated politicos. The most successful have strategies that far exceed terrorist methods, combining these in a prudent and broad approach to power. Some may ultimately fail, but others appear likely to move to greater plateaus of success.

Successful. Earlier pages and rubrics explored terrorist successes—for example, the Bolsheviks, the Algerian FLN, Greek-Cypriot EOKA, some Jewish groups, and the Sandinistas—that achieved some or all of their strategic objectives after violent campaigns of medium duration. But there are also a few groups of longer life that did come to triumph and take state power.

In South Africa, 1961 saw the creation of The Spear of the Nation, forged to do bloody work for the African National Congress (founded 1912). This mid-century strategic choice followed years of indifferent political success; ANC militants now bombed energy companies, shopping centers, and other civilian targets. Later they commenced "necklacings"—victims were bound, seated, and then burned by means of placing an automobile tire around the torso, filling it with gasoline, and torching it. This was apparently done to murder black rivals or dissidents more often than white South Africans, an example of an old pattern—terrorism for discipline and control of "one's own." In retrospect, ANC terrorism led towards stunning electoral triumphs—not unlike the ways Palestinian terrorism has done so.

Yasser Arafat's Palestine Liberation Organization (PLO) was created in 1964. Like most revolutionaries, it aspired to match the fresh triumph of the FLN in Algeria. Fatah was the armed force created and shaped by the PLO; after it, innumerable subgroups and splinters appeared which achieved a certain advantage in deniability and deception. Except for Abu Nidal's gang,[66] which left the PLO only to hunt its former colleagues, the PLO splinter groups were generally helpful and useful to Arafat. He might support an Abu Abbas (of the PLO) in one season, then hold him at arm's length later, and welcome him back in a new springtime. Skillful as an organizer, adequate as an orator, immovable as the controller of PLO businesses

and income streams, Arafat won. It took three decades of his own blend of protracted war, yet he created a Palestinian homeland. It may today be divided in civil war, but it is a statelet; Israel has departed and hopes to avoid unpleasant returns; foreign governments jostle one another to lead in supplying humanitarian aid to Palestinians under the control of the Palestine Authority (PA); HAMAS terrorist acts all rebound in favor of PA legitimacy and give the older, more secular guard airs of empathy. Thus, the PLO and Fatah and the ANC's Spear of the Nation are among the few cases in which long-term efforts, including systematic terrorism, have led eventually to strategic success.

An Afterword: Wither al-Qaeda?

Al-Qaeda falls within our rubric of real longevity and limited success (III B). This innovative, international, and powerful organization has taken body-blows without going down. It lost in Afghanistan and still found cover. It absorbed members of Egypt's battered al-Jihad group at the end of the 1990s; in early 2007 it absorbed North Africans of the Salafist Group for Preaching and Combat; European converts and others have joined to offset losses. Many senior and mid-level leaders have been killed or captured, yet several of the newest leaders are from the ranks stupidly released from Guantanamo and other prisons.[67]

Certainly al-Qaeda and its allies will never achieve their "New Caliphate," but what matters is that they are fighting for it. No one should claim they have "failed" when top leaders with long experience and obvious charisma remain in the field (Osama bin Laden, Ayman al-Zawahiri, and Taliban partner Mullah Omar). Al-Qaeda's terrorism has made impressions on the politics, public opinion, or defense policies of a hundred countries worldwide, as in the US troop withdrawal from Saudi Arabia, bin Laden's birthplace. It accomplishes such things; holds up its intellectual, moral, political, and religious banners of attack; and protects many of its human and financial assets in the face of the largest manhunt in global history. To call al-Qaeda a "failure" would be the most desperate form of false hopes. It is apparent that states, and the international community, have much to do before al-Qaeda ends.

Editor's Epilogue

Terrorist groups in many forms have been around for many years and will be around for even more. Success or failure depends on a myriad of factors, both internally and externally controlled. Government intervention in the early stages of terrorist formation is most effective by employing a sophisticated grand strategy, solid political leadership, fine intelligence, effective civilian law enforcement, and a well-trained and disciplined military. As a terrorist group ages, different approaches may need to be initiated. For example, seduction of the terrorists' bases and co-opting membership becomes more important. Denying recruitment of new members and support from external sources is paramount. Once a terrorist organization becomes decades old, it may in fact resort to negotiations or even risk election and mainstream political action. Faced with these myriad scenarios, the challenge for modern-day strategists is to analyze the stage of the terrorist group and consider the most effective course of defeat. SSQ

EXTENT OF TERRORIST SUCCESS: DEFEATED

DURATION of MAIN VIOLENCE: SHORT *5 YRS OR LESS*		DURATION of MAIN VIOLENCE: MIDTERM *8–15 YEARS*		DURATION of MAIN VIOLENCE: *PROTRACTED, DECADES*	
OAS (Org. of Secret Army) 1960–1962, No. Africa & W. Eur.	61–62	Huks (Hukbalahap) 1946–1955, Luzon, Philippines	48–54	International Anarchists (lethal) 1866–1920s, Northern Hemisphere	1880–1920
ELN (National Lib. Army) 1966–1967, Bolivia (Che)	67	Tupamaros 1962–1976, Uruguay.	63–75	Malayan Races Liberation Army 1946–1988, Malaysia & Thai border & Chin Peng 70–77	46–60
ALN (National Liberating Action) 1968–1970, Sao Paulo, Brazil (Marighella)	68–70	JVP (Janatha Vimukthi Permuna) (People's Lib. Front) 1967–1989, Sri Lanka	67–75	JRA (Japanese Red Army) 1969–2001, Japan and Middle East	70–88
SLA (Symbionese Liberation Army) 1972–1975, California	73–75	RAF (Red Army Faction) 1968–1992, Germany	68–77	LTTE (Lib. Tigers of Tamil Eelam) 1972–2009, Sri Lanka	74–09
Front Line (Primea Linea) 1976–1982, Italy	76–81	The Weathermen 1969–1980, USA	69–75	ANO (Abu Nidal Org. or Black June) 1974–2002, Middle East and world	74–94
VZJ (Free South Malaccan Youth Org.) 1975–1979, Netherlands	75–78	Red Brigades 1970–1983, Italy	74–81	Revolutionary Organization 17 November 1975–2003, Greece	75–02
Hoffman Military Sports Group 1979–1981, Germany	80–81	Montoneros 1970–1984, Argentina	70–77		
The Order 1982–1984, Pacific N.W., USA	83–84	M-19 (19th of April Movement) 1970–1989, Colombia	74–86		
Communist Combatant Cells 1984–1985, Belgium	84–85	2nd of June Movement 1971–1980, Germany	71–78		
		Shining Path 1971–Peru	80–92		
		Aryan Nations 1974–2001, USA	84–99		
		FALN (Armed Forces of National Lib.) 1974–1985, Puerto Rico, US	75–83		
		MRTA (Tupac Amaru) 1975–1997, Peru	78–96		
		Los Macheteros (Machete Wielders) 1978–1986/88, Puerto Rico & USA	78–86		
		Action Direct 1979–1987, France	79–87		
		Popular Forces of 25 April 1980–1992, Portugal	80–86		
		FMLN 1980–El Salvador	80–90		
		The Order 1982–1985, USA .	83–84		
		Aum Shinrikyo 1984–1995, Japan & Russia	88–95		

EXTENT OF TERRORIST SUCCESS: LIMITED GAINS

DURATION of MAIN VIOLENCE: SHORT *5 YRS OR LESS*		**DURATION of MAIN VIOLENCE: MIDTERM** *8–15 YEARS*		**DURATION of MAIN VIOLENCE:** *PROTRACTED, DECADES*	
Black Panthers 1966–1972, USA	67–72	Irgun (Irgun Zvai Leumi) Israel	37–48	KKK (Ku Klux Klan) USA (& Canada early 20th cent.)	1866–
AUC (United Self-Def. Forces of Col.) 1997–2005, Colombia	97–02	Lehi (Lohame Herut Israel/Stern Gang) Israel	40–48	UVF (Ulster Volunteer Force) 1912– Northern Ireland	66–early 70s
		EOKA (National Org. of Cypriot Fighters) 1951–1960, Cyprus	54–59	ETA (Basque Homeland & Liberty) 1959– Spain (& French borderland)	62–
		FLQ (Quebecois Liberation Front) 1963–1972, Canada	66–70	ELN (National Lib. Army) 1964–Colombia	81–98
		ASALA (Secret Army for Lib. Armenia) 1975–1988, Lebanon & Europe	75–86	FARC (Revy. Armed Forces of Col.) 1966–Colombia	66–
		HAMAS (Islamic Resistance Movement) 1987–Palestinian Territories & Israel	88–	IRA Provisionals 1916/69–UK and the Continent	70–98
		Taliban 1994–Pakistan & Afghanistan	94–01	NPA (New People's Army) 1969–Philippines	69–
				MEK / PMOI (People's Muj. Al Khalq) Iranians in exile	71–1966/67–
				PFLP-GC (Pop. Front for Lib. of Palestine) General Command 1967–Middle East & W. Europe	68–88
				Naxalites (Comm. Party of India/Maoist) 1969–India	75–
				UFF (Ulster Freedom Fighters) 1973–Northern Ireland	73–
				FLNC (Corsican National Lib. Front) 1976–Corsica & mainland France	73–
				Hezbollah (The Party of God) 1983–Lebanon	82/83–
				al Qaeda 1988–SW Asia & the world	98–

EXTENT OF TERRORIST SUCCESS: STRATEGIC SUCCESS

DURATION of MAIN VIOLENCE: SHORT *5 YRS OR LESS*	**DURATION of MAIN VIOLENCE: MIDTERM** *8–15 YEARS*	**DURATION of MAIN VIOLENCE:** *PROTRACTED, DECADES*
None—with possible exception of M-26-7 (26th of July Movement) 58–59 Cuba, 1952/55–1959	Bolsheviks 05–17 1903–1917, Russia FLN (National Lib. Front) 54–62 1954– Algeria, No. Africa, & France Khmer Rouge 62–78 1951/61–1978, Cambodia Communist Party of Nepal (Maoist) 96–05 1990s–	ANC (African National Congress, Spear of the Nation, etc.) 61–88 1912/1961– FSLN (Sandinistas) 63–79 1961–Nicaragua PLO: Fatah, Black Sept., etc. 65– 1964–Palestinian Territories

Notes

1. Scholars must recognize certain intellectual debts, and good scholars enjoy doing so. My debts are happily paid in this and earlier places, especially to Martha Crenshaw. One begins with her essay "How Terrorism Declines," in Terrorism and Political Violence 3, no. 1 (Spring 1991): 69–87, and its admirable chart. There was a distinctive direction to my body of earlier work on this subject (e.g., many public presentations in 2004, a speech on Capitol Hill, a Webcast from the Woodrow Wilson Center in Washington, DC, on 20 March 2006, a book chapter with Cambridge University Press earlier that year, etc.). It was to retrace researches I'd made over a previous quarter century, present a half dozen leading reasons for terrorist group decline, and then detail examples within each rubric. The present essay's approach is new, guided more by chronology, and my analysis profits from continued study of individual-named terror groups. Endnotes for chap. 7 of my book *Terrorism Today*, 2nd ed. (London & New York: Routledge, 2007) indicate other resources I found worthy.

2. Joseph T. McCann, *Terrorism on American Soil: A Concise History of Plots and Perpetrators from the Famous to the Forgotten* (Boulder, CO: Sentient Publications, 2006), 33–40.

3. Labor histories by L. Adamic and G. W. Meaker are cited in Walter Laqueur, *The Age of Terrorism*, 2d ed. (Boston: Little, Brown & Co., 1987), 75.

4. Barbara Tuchman, *The Proud Tower: A Portrait of the World before the War, 1890–1914* (New York: Scribner/Macmillan, 1966).

5. There are two good English-language accounts (known to me) of the precipitous fall of N17. A gifted student at the Institute of World Politics in Washington, DC, aviation security expert Mr. Paris Michaels, wrote an unpublished 2003 paper for our course. George Kassimeris of the University of Wolverhampton, England, published a detailed article, "Last Act in a Violent Drama? The Trial of Greece's Revolutionary Organization 17 November," *Terrorism and Political Violence* 18, no. 1 (March 2006): 137–57. The group's head of operations is quoted saying the group was finished as a terrorist organization yet could return in some other form, "perhaps, in 10–15 years' time, a new generation of fighters for the people might relaunch the struggle" (p. 153). It may be relevant that several Greek cities faced protracted rioting in late 2008 following a police shooting, and that since 2003 a terrorist group called Revolutionary Struggle has emerged.

6. I have often spoken in lectures of the roles of Horst Herold and German police in the attrition of the RAF cadre. Introducing "computer profiling" and diligence with detail allowed federal authorities to find, one by one, the RAF militants. As there were never more than a few dozen weapons-carrying members; arrests reduced the group to nothing. In recent years, nearly all members have been released from jail. The unrepentant Hans Christian Klar, guilty of 20 murders or attempted murders, won early release in late 2008, prompting debate in Germany and this comment by Bavarian justice minister Joachim Hermann: "Klar deserves no sympathy as long as he continues to show none for his victims." *Christian Science Monitor*, 22 December 2008; and *BBC News*, 19 December 2008.

7. This appellation, often self-applied by the terrorists, was taken up by two scholars as a subtitle for their fine book, *Europe's Red Terrorists: The Fighting Communist Organizations,* by Yonah Alexander and Dennis Pluchinsky (London: Frank Cass, 1992). They include several post-1990 RAF documents, such as the aforementioned confession of failure dated 15 April 1992. In 1998 came yet another confession of failure from an RAF hand, so that year, too, appears in print sometimes as "the end of the Baader-Meinhof organization."

8. One careful listing of relevant regional and subregional offices and organizations is by Florina Cristiana (Cris) Matei, "Combating Terrorism and Organized Crime: South Eastern

Europe Collective Approaches," in *Bilten Slovenske Vojske*, the journal of the Slovenian Armed Forces (September 2008), 37–58.

9. Teaching case studies of counterinsurgency success long ago convinced me that defections are a superior metric for decline. When Colombia's vice-minister of defense Sergio Jaramillo wrote "Pourquot le Temps Joue Contre les FARC" for *Le Figaro*, 23 January 2008, he reported that 1,454 FARC members had quit in 2007, double of the previous year. As this occurred in the context of much-enhanced skills and professionalism by the Colombian armed forces, I took it to be highly significant. A few months later, the Ingrid Betancourt hostage party was rescued in a Colombian special forces operation—another case in which years of negotiations failed but surgical force worked brilliantly.

10. *The Turner Diaries*, a 1978 novel by William L. Pierce (writing under the pseudonym Andrew MacDonald), is linked to at least five killings or nonlethal terrorist incidents of 1995–2006; see the 2d edition of my book *Terrorism Today*, 18–19. Other incidents in the present text are documented by Department of Justice/FBI publication *Terrorism in the United States: 1999—30 years of Terrorism, A Special Retrospective Edition* (Montgomery, AL: Southern Poverty Law Center Publications, 2001) and by media reports.

11. This answer reveals the difference between "pro-state" terrorism and right-wing terrorism. The former is exercised by agents or partisans of state power, but in the US case it was precisely federal power that was most active against the racists. Right-wing terrorism of the KKK sort was by substate actors who hated the federal government's intervention in southern American affairs.

12. This also happened in Cologne, Germany. In September 2008, a few dozen rightists appeared to rally against "Islamisation and immigration invasion." Forty thousand counterprotestors swamped the scene, and the initial marchers literally fled. See Jess Smee, " 'Anti-Islamisation' Event Abandoned after Protests," *Irish Times*, 20 September 2008, http://www.irishtimes.com/newspaper/world/2008/0920/1221835126595.html.

13. Europol, *EU Terrorism Situation and Trend Report, March 2007*, www.europol.europa.eu.

14. When freed from jail in the mid 1980s, Tupamaros leader Raul Sendic refounded his movement as a legitimate political party—the Movement of Popular Participation—and that, too, is part of how some terror groups end. On such groups as the Tupamaros, the best single source is Michael Radu and Vladimir Tismaneanu, *Latin American Revolutionaries: Groups, Goals, Methods* (Washington: Pergamon-Brassey's, 1990).

15. One thorough English account of the chronicles of torture in Argentina is Paul H. Lewis, *Guerrillas and Generals: The "Dirty War" in Argentina* (Westport, CT: Praeger, 2002), e.g., 150–59. The book was given to me by a gifted and humane military officer of that country who wished that others avoid his country's mistakes while waging the "global war on terror."

16. Paul Hockenos, *Joschka Fisher and the Making of the Berlin Republic* (Oxford: Oxford University Press, 2007).

17. Claire Sterling, *The Terror Network: The Secret War of International Terrorism* (New York: Henry Holt & Co., 1981), chap. 2.

18. The impressive and deliberative way Italian democracy brought an end to terrorism has been remarkably understudied despite bales of publications on that country's violence. A recent exception is the well-done Leonard Weinberg chapter, "The Red Brigades." It does note that the antiterrorist police DIGOS probably used torture in a very few cases during the attempt to find kidnapped NATO general James Dozier and in its aftermath. *Democracy and Counterterrorism: Lessons from the Past*, eds. Robert Art and Louise Richardson (Washington: US Institute of Peace Press, 2007), 49–56, are relevant.

19. No Italian leftist killings of the 1980s (after 1981) make the 31-page chronicle of international terror incidents 1920–2007 by Ann E. Robertson, *Terrorism and Global Security* (New

York: Facts on File, 2007). My main source is the detailed research in Donnatella della Porta, "Left Wing Terrorism in Italy," in *Terrorism in Context*, ed. Martha Crenshaw (University Park: Pennsylvania State University Press, 1995). Certainly there have been leftist terrorist actions in Italy in the last 10 years; two murders in 2002 and 2003 were claimed by a group calling itself "Red Brigades," prompting newspaper reports of a revival.

20. I have yet to study Pierre Vallieres' introduction to the movement, *Qu'est-ce que le FLQ?* but read with profit his 1967/1968 aggressively titled prison memoir *White N------ of America: The Precocious Autobiography of a Quebec "Terrorist"* (New York: Monthly Review, 1968).

21. One contribution to this Canadian case is Ted Robert Gurr, "Terrorism in Democracies," chap. 6, in *Origins of Terrorism*, a superb book edited by Walter Reich (Washington: Woodrow Wilson Center Press, 1998).

22. It is not surprising that Filiberto Ojeda Rios declined to "walk away" from terrorism when discovered in September 2005 or that the FBI had to use its weapons. In a previous arrest, this same terrorist had begun burning documents when agents knocked at his door; he then opened fire with a machine gun, blinding an FBI agent in the eye. Ojeda Rios was disarmed. Later he jumped bail.

23. If some four million live on the island of Puerto Rico, more than two million more now live in the rest of the United States—which helps explain the disparate locations of these terrorist attacks.

24. See "Timeline: ETA Attacks," *BBC News*, last updated 6 August 2009, http://news.bbc.co.uk/2/hi/europe/545452.stm.

25. "Paris and Madrid United against Terrorism," *Le Figaro*, 11 January 2008 (trans. CCH).

26. American writers, even in military journals, sometimes misrepresent Mao's concepts. From his writings of the 1920s and 1930s and the historical work of Samuel Griffith, I see "phase one" warfare as the strategic defensive—characterized by political organization and guerrilla war (as well as terrorism, which Mao usually declines to mention). "Phase two" warfare is a strategic equilibrium in which the insurgency is strong enough to hold its ground, and in which guerrilla war continues, supplemented by positional and even conventional war elements. In "phase three," the insurgency has developed well politically and is battle-tested militarily, and commanders can use all manners of fighting that are appropriate, especially conventional positional war. Mao's theory is too often treated skeptically, even by scholars; it well accounts for the progress and successful resolution of wars in China (1949) and Vietnam (1975). The FARC and LTTE are thus groups that for many years have been locked into "phase two" war with their respective enemies. For an effective use of Mao's theory to illuminate modern Islamist fighting, see Dr. Norman Cigar's introduction to Abd al-Aziz al-Muqrin, *A Practical Course for Guerrilla War: Al Qaida's Doctrine for Insurgency* (Dulles, VA: Potomac Books, 2008).

27. One Sikh group took down an Air Canada flight, killing 329 passengers, in June 1985. Perhaps a scholar interested in how terror groups end, a regional expert such as K. P. S. Gill, will one day detail how it was that international Sikh terror had so short a lifespan.

28. Ami Pedahzur, William Eubank, and Leonard Weinberg, "The War on Terrorism and the Decline of Terrorist Group Formation: A Research Note," *Terrorism and Political Violence* 14, no. 3 (Autumn 2002): 141–47.

29. Of the several English-language books on Aum, the best may be Ian Reader, *Religious Violence in Contemporary Japan: The Case of Aum Shinrikyo* (Richmond, UK: Curzon, 2000), e.g., 193–95.

30. Haruki Murakami, trans. A. Birnbaum and P. Gabriel, *Underground: The Tokyo Gas Attack and the Japanese Psyche* (New York: Vintage Books, 2001).

31. David E. Kaplan and Andrew Marshall, *The Cult at the End of the World: The Terrifying Story of the Aum Doomsday Cult, from the Subways of Tokyo to the Nuclear Arsenals of Russia* (New York: Crown Publishers, 1996), 108–12.

32. Lt Col John Kane, USMC, has been of good help in tracking the cyber side of Aum and of Aleph.

33. While events in 2008 seemed to instruct the national government in the dangers Hezbollah poses inside Lebanon, it has been striking to hear how apologetic many previous official statements have been. Twice I heard radio interviews in which the Lebanese ambassador to the United States said nothing but good about Hezbollah and blamed the group's violence on the "Israeli occupation"—which, with the exception of a couple of farms, had ended *years before*. Government spokesmen were ignoring as well the policy ends of Hezbollah, which are contrary to those of democratic, multiconfessional Lebanon, and the meddling of Iran, which Hezbollah itself counts as its mentor.

34. According to A. N. Pratt, posted to a Middle East diplomatic mission during early 2008, Iran gives HAMAS some $120 million a year. Other estimates of Iranian aid to Hezbollah have been as high.

35. See Department of State, *Country Reports on Terrorism—2007* (Washington: Government Printing Office, April 2008), and past versions of this State Department annual, which has appeared for three decades. In certain recent years the report suffered from flaws in its statistics, which required correction in some cases, but I do not accept the implications suggested by resultant newspaper articles. I find the report in general an admirable compilation and a sound record of most events, highly useful to scholars, and less flawed than the terrorism coverage of many books and periodicals.

36. "The Covenant of the Islamic Resistance Movement," offered up to the "Name of the Most Merciful Allah," is dated 18 August 1988 and may be found on the website of the Avalon Project at Yale Law School, http://avalon.law.yale.edu/subject_menus/mideast.asp.

37. When speaking of a group's lifespan, I refer to its participation in violence of consequence to the state; therefore, some periods of several years or even a decade (e.g., Sendero in the 1970s) spent in preparation and planning may be excluded. So, too, might one exclude years of quiet after violence (as when members of the Symbionese Liberation Army, having failed, hid underground, 1976–1999). My chart shows dates for the group's existence, but others for the years of "main violence." Consistent with the PTSS approach, I include discussion of appropriate *insurgent* groups that systematically employ terror; this article is not merely focused on small terrorist cells.

38. Peter Janke, *Guerrilla and Terrorist Organizations: A World Directory and Bibliography* (New York: Simon & Schuster, 1983), 23. The Hoffman group is so lost to history that even the US National Counterterrorism Center's annual desk diaries say nothing of the bombing on 26 September 1980. Yet, its significance recurred in 2009 when the famous fall festival in Munich was again directly threatened by terrorists—of al-Qaeda.

39. Radu and Tismaneanu, *Latin American Revolutionaries*, 115–23.

40. Ibid.; and Janke, *Guerrilla and Terrorist Organizations,* 431–40.

41. Yonah Alexander and Dennis Pluchinsky, *Europe's Red Terrorists: The Fighting Communist Organizations* (London: Frank Cass, 1992), 148–50. Marine Corps University was honored to have both these scholars in its colloquium on "Terrorist Group Vulnerabilities" in Quantico, VA, 30 April 2007.

42. Are the Black Panthers a case of limited success? They emerged in 1966 and 1967 with aspirations to be a sort of armed wing of the civil rights movement. They expected status as a virtuous self-defense force and carried weapons openly amidst claims to protect their communities and their race from the diffidence of a white majority and the aggressions of its white

government. Their quotidian work included "survival activities" such as providing food and medical aid and schools in impoverished areas. Their other side was to be found in brutalizing critics, open calls to "Kill the Pigs" (police), and physical attacks on the establishment. The Panthers found themselves very much out-gunned by police; many died at police hands, and their supporters often claimed assassination. More (including "defense minister" Huey Newton) died committing crimes or in battles with other black militants. Dozens were arrested and jailed for rape, drug-dealing, assault, and other crimes, illustrating the criminality often typical of a political terror group. A few Panther notables fled abroad, to return years later, usually disillusioned by life in Cuba or Algeria. Their organized political violence lasted but a half decade, ending in 1971/1972. Some Panthers spent the next years folding peaceably into American political and social life, winning community and city elections, or devoting themselves to education. Some wrote memoirs. They had not fallen into indiscriminate killing of normal citizens; this set them apart and helped make them a limited success in America. Panthers would doubtless claim to have helped the civil rights movement by using publicity, psychological shock, and the spectacle of openly bearing arms; they would say they advanced with force while other black activists advanced related causes in more pacific, less controversial ways. There are many published memoires on these times—some by Panthers themselves—as well as Peter Collier and David Horowitz, *Destructive Generation: Second Thoughts about the '60s* (New York: Summit Books, 1990), 149 ff; and Crenshaw, "How Terrorism Declines," 81.

43. Dr. David Tucker is one of the very few American authors in recent years to document and discuss Castroite terrorism during the rise to power, which ended in 1959—something older reports and US congressional hearings used to cover. Tucker details several incidents of hostage taking and so forth in a book drawing well on both his DoD and academic work, *Skirmishes at the Edge of Empire: The United States and International Terrorism* (Westport, CT: Praeger, 1997). My point that guerrilla war was far more important than terrorism is also why this essay does not attempt to include so massive a movement as the Chinese Communist Party's rise to state power in 1949.

44. One notable Huk attack devastated a military hospital and featured widespread murder of patients. That is a tactic even the most nihilistic terrorist groups avoid—although certain Chechens savaged a hospital.

45. By contrast, Malaysian communists were pushed out without surrendering. Chin Peng and some remnants held out for decades in Thai border areas, quitting only with a treaty signed 2 December 1989.

46. The Tupamaros became fashionable; their kidnapping and political theater tactics excited widespread admiration on the militant left. One testament to this is Russell Little's words in a documentary film about his group, the Symbionese Liberation Army (SLA) of California. He discusses their fascination with the group and the film "State of Siege" ("*État de Siège*") and says his own SLA literally took form from a discussion group on political films running in Berkeley. Robert Stone's "Guerrilla: The Taking of Patty Hearst" (Magnolia Pictures, 2005).

47. Seth G. Jones and Martin C. Libicki, *How Terrorist Groups End: Lessons for Countering al Qa'ida* (Santa Monica, CA: RAND, 2008), chap. 4, "Politics and the FMLN in El Salvador." The notion that this Cuban-organized group of communists and self-proclaimed armed forces was mainly pushing for "reforms" and "for the transition to a democratic political regime" is comically naïve (ibid., 64). After its defeats at phase-two-style fighting and disarmament under various national and international pressures, the FMLN did morph into a political party and compete in elections, often with a measure of success. A similar error occurs in table A.1 in which the "goal" of the 2nd of June Movement in Germany is declared to be "policy change." They were anarchists, and later some joined the communist RAF.

48. Phil Peters (Lexington Institute, Arlington, VA), interview by author, 2006. Peters worked on Central American issues for many years in the office of Rep. James A. Courter (R-NJ) on the House Armed Services Committee, where I also had the honor of employment.

49. Donatella della Porta, "Left-Wing Terrorism in Italy," in *Terrorism in Context*, ed. Martha Crenshaw (University Park: Pennsylvania State University Press, 1995), 121.

50. See Richard Drake, *The Aldo Moro Murder Case* (Cambridge, MA: Harvard University Press, 1995), 259, ff.

51. See, for example, Frank Hyland, "Peru's Sendero Luminoso: From Maoism to Narco-Terrorism," *Jamestown Foundation Terrorism Monitor* 6, no. 23 (8 December 2008), http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=34237&tx_ttnews[backPid]=167&no_cache=1. The article states that "SL's apparent resurgence may be viewed fairly as an integral part of a burgeoning wave of leftist ideology in Latin America . . . Concern over an SL comeback is well founded." I think these reports are overblown. As a November 2009 briefing at the Marshall Center by a Peruvian lieutenant colonel indicates, the actual area of operations of Sendero today is miniscule and very isolated.

52. Janke, *Guerrilla and Terrorist Organizations,* 7–10.

53. Menachem Begin, trans. Samuel Katz, *The Revolt: Story of the Ergun*, 5th ed. (Jerusalem: Steimatzky, 1972); and Doris Katz, *The Lady was a Terrorist: During Israel's War of Liberation* (New York: Shiloni Publishers, 1953).

54. Janke, *Guerrilla and Terrorist Organizations,* 245–47; and the Jewish Virtual Library, http://www.jewishvirtuallibrary.org/.

55. Lord Moyne was a friend of Winston Churchill. After the 1944 murder, the prime minister made a scorching speech in the House of Commons, describing Jewish "terrorism" as evil and risking comparison to acts by Nazi terrorists. This was a principled political posture, the right one, however difficult it must have been for Churchill, well known to be a friend to the Jews since his earliest years in parliament.

56. There have been innumerable terrorist attacks upon those who would ameliorate social and economic problems, and often this is a strategy by the violent. Some of these are a pattern of anti–United Nations terrorism—e.g., today's visible al-Qaeda hatreds of the United Nations. I have written on other such attacks in "The Assault on Aid Workers: A New Pattern in Terrorism," *Security Insights* (January 2008), the first of a new series of policy papers from the Marshall Center.

57. Authorities date the origin of the FMLN differently—1958, 1960, 1961, etc.

58. A more common date of origin for the Tigers is 1976. This author chooses to begin when Velupillai Prabhakaran founded the Tamil New Tigers, 1972. An active terrorist and guerrilla in the next years, he refounded the Tigers as the LTTE in 1976.

59. N17 prospered so long that some began to whisper that the socialist governments of Greece did not care to arrest the terrorists, given the targets they were choosing. Keith Weston, once part of an official British contingent in Greece, disagrees. He believes the extremely small size of the group and the blood connections many had as well ensured secrecy.

60. The Kurdish PKK, the most beguiling of cases, may or may not deserve a place here in section III A. Once easily classified, this protracted insurgency has become an analytical challenge. Founded by Abdullah Ocalan in the mid 1970s and ruled continuously by this charismatic leader, it was decapitated in February 1999 with his arrest and rendition. Kurdish violence all but disappeared for some four years. Ocalan's announcements from jail appeared to dissuade loyalists from terrorism, and no clear successor has appeared. The PKK appeared defeated. Then a shadow came over Turkey's accomplishment; violence by Kurdish militants of unclear loyalty slowly reappeared. The leader's son is an active militant, and new organizations that may or may not be well linked to the old have appeared and are fighting—in Turkey and from Iraq. There is,

for example, the Kurdish Freedom Falcons, which the US State Department initially reported on neutrally and years later began referring to as a militant wing of the PKK. Today one must speak of a phoenix of Kurdish militancy. The US State Department and the government of Turkey see a new chapter in a long PKK life. Either of these different views may be defensible; a historian might well prefer the latter.

61. Ken Duncan, the Marshall Center's Program on Terrorism and Security Studies (PTSS) expert on Middle Eastern states' sponsorship of terrorism, adds that Syria has been successful—a contrast with Libya.

62. Jack Holland, *The American Connection: US Guns, Money, and Influence in Northern Ireland* (New York: Viking, 1987).

63. This unique term *preservationist* is from Bard O'Neill. The term *pro-state terrorist* is inferior because it is less exact; some right-wing groups want to preserve the cultural or political status quo, not necessarily the sitting government, with whose police they often quarrel.

64. Stephen Morris, an Australian scholar and former colleague at the Naval War College, propounded a very useful scheme for beginning study of an insurgent group—analyzing its performance in the overt political, the covert political, and the military realms. If we group terrorist violence in with the third category, the approach has much value for study of organizations such as Hezbollah and HAMAS, and to lesser degrees al-Qaeda.

65. The second source, described as more careful, is the aforementioned Jones/Libicki study dated 2008, which declares on page xiv, "No religious group that has ended achieved victory since 1968." A student of history inclined to think terrorism fails will be most content with the views of and best instructed in studying the works of Walter Laqueur. His decades of fine work, based on many primary sources and varied languages, have set high standards for writing the history of terrorism.

66. The Abu Nidal Organization flourished for a quarter century and killed some 900 people before expiring from combined causes. These culminated in the shooting of the leader in Iraq but included internecine violence in the ANO, repudiation by other Palestinians, and a clever US effort in counterterrorism thus far described by almost no one in print; see the chapter on "History" in Tucker, *Skirmishes at the Edge of Empire*.

67. ABC Radio News on 24 January 2009 named a released terrorist who rejoined al-Qaeda. These incidents have occurred perhaps once a year, during the very same years of popular European and American agitation for closure of the detention facility at Guantanamo Bay, on US–controlled land in Cuba.

Unit Cohesion and the Impact of DADT

Gary Schaub Jr.

"This year, I will work with Congress and our military to finally repeal the law that denies gay Americans the right to serve the country they love because of who they are."[1] So said president of the United States and commander-in-chief of the armed forces, Barack Obama, before a joint session of Congress on 27 January 2010. The president referred to the 1993 law and associated policy commonly known as "Don't Ask, Don't Tell" (DADT), that codified homosexual conduct, including declarations of sexual orientation that indicate a propensity to engage in homosexual acts, as grounds for discharge from the military.[2]

The following week, Secretary of Defense Robert Gates and chairman of the Joint Chiefs of Staff ADM Michael Mullen testified before the Senate Armed Services Committee. "No matter how I look at the issue, I cannot escape being troubled by the fact that we have in place a policy which forces young men and women to lie about who they are in order to defend their fellow citizens," said Admiral Mullen, who further stated that it was his personal belief that "allowing gays and lesbians to serve openly would be the right thing to do."[3] Secretary Gates announced that his office was undertaking a study "to thoroughly, objectively, and methodically examine all aspects of this question and produce its finding and recommendations in the form of an implementation plan by the end of this calendar year," that he had contracted the RAND Corporation to update a 1993 study on the issue,[4] and that his office would seek ways to implement the policy "in a fairer manner" in the interim—changes that have since been implemented.[5] The policy preferences enunciated suggest that it is a question not of *if* homosexuals will be permitted to serve openly in the military, but *when*.[6]

Gary Schaub Jr., PhD, is an assistant professor in the Leadership and Strategy Department, Air War College, Maxwell AFB, Alabama. He previously taught at the USAF School of Advanced Air & Space Studies, the University of Pittsburgh, and Chatham College. Dr. Schaub has published in the journals *Parameters, International Studies Review*, *Political Psychology*, and *Refuge* and book chapters in volumes published by Oxford University Press and St. Martin's Press. He has written on military coersion, nuclear weapons issues, European security, and research methodology.

The issue of cohesion is at the center of most debates about repealing DADT. Hence, I focus on the impact this change in policy may have on the cohesion of military units. The arguments underlying Title 10, § 654's prohibition on openly homosexual members in the military, the concerns of Secretary Gates and the JCS, and the views of many military personnel rest on the premise that their presence would undermine the cohesion of military units, thereby making service more difficult and performance less effective.[7] Critics discount these concerns. Aaron Belkin and Melissa Embser-Herbert argued in 2002 that a "growing body of scholarly evidence has undermined the validity of the unit cohesion rationale . . . [and] show that whether a unit's members like each other has no impact on its performance."[8] In 2010, Bonnie Moradi and Laura Miller found in an analysis of Iraq and Afghanistan war veterans that knowing that a member of a unit is gay or lesbian had no effect on their judgments of unit cohesion.[9] Thus, the argument hinges on whether repealing DADT will negatively impact unit cohesion.

I argue the critics are wrong. Whether members of a unit cohere socially does matter and has an independent effect on performance. The latest literature on the cohesion-effectiveness link indicates that both task and social cohesion affect performance and outcomes. Evidence shows that liking one's teammates affects cohesion and performance almost as much as devotion to getting the job done. Policies that discount social cohesion will underestimate the degradation in performance that will occur if it is diminished by repealing DADT. Social cohesion depends heavily upon shared values and attitudes, and if a significant proportion of members opposes the presence of gays and lesbians in their unit, then social cohesion will suffer tremendously. Available evidence suggests that attitudes of US service members vary toward homosexuals, both in general and in the context of DADT. They vary more by service, sex, race, and party identification than by unit type (combat, combat support, and combat service support) or rank. These characteristics are not isolated, so disruption is likely to occur in some units more than others.[10] Therefore, changing the policy with regard to gays and lesbians serving openly in the military will unevenly affect unit performance—at least until attitudes shift. It is therefore important that ongoing studies include measures of social cohesion and that they be applied to the force on a regular basis so any shifts can be tracked and their implications managed effectively.

Cohesion

There is strong belief that cohesion is related to performance in the military and more generally in small groups and organizations. Title 10, § 654 argues that "[o]ne of the most critical elements in combat capability is unit cohesion, that is, the bonds of trust among individual service members that make the combat effectiveness of a military unit greater than the sum of the combat effectiveness of the individual unit members." These beliefs within the military are largely based upon studies dating from World War II[11] and anecdotal evidence, but substantial literature exists on the nature of cohesion and its relationship to performance. Cohesion is defined as "the resultant forces which are acting on the members to stay in a group."[12] Guy Siebold asserts that "the essence of strong primary group cohesion . . . is trust among group members (e.g., to watch each other's back) together with the capacity for teamwork (e.g., pulling together to get the task or job done)."[13]

Indeed, the impact of cohesion on "pulling together to get the task or job done" has been one of the primary motivators in this study. How does group cohesion affect group performance? "Presumably," write Daniel Beal et al., "when cohesion is strong, the group is motivated to perform well and is better able to coordinate activities for successful performance."[14] In essence, the literature posits that cohesion is causally linked to performance in two ways. First, it induces individuals in the group to value group-produced outcomes more than the cost of their relative level of effort.[15] Second, it reduces the transaction costs associated with the cooperation and coordination required in any group effort.[16] The degree of communication and coordination necessary to achieve the group's goal would be mediated by the pattern of their work flow. Outputs that are merely pooled individual efforts require little cooperation, coordination, or cohesion to be effective, while those that were produced in a sequential or reciprocal process would require more, and those that require collaboration would require the most. These theoretical conceptions of how group cohesion affects performance help us to understand the logic behind the persistent belief that the two are positively related—particularly in a military setting.[17]

The social psychological literature on cohesion focuses on its motivators and distinguishes between two types: social and task. Social cohesion has been defined as "the nature and quality of the emotional bonds of friendship, liking, caring, and closeness among group members. A group

is socially cohesive to the extent that its members like each other, prefer to spend their social time together, enjoy each other's company, and feel emotionally close to one another."[18] Task cohesion is described as "the shared commitment among members to achieve a goal that requires the collective efforts of the group. A group with high task cohesion is composed of members who share a common goal and who are motivated to coordinate their efforts as a team to achieve that goal."[19]

Clearly, these two forms of cohesion are related but distinct. A group that is socially cohesive is more likely to have task cohesion, but this need not be the case. Indeed, the literature on small-group decision making suggests that building and maintaining high social cohesion may undermine the group's ability to perform tasks, such as making sound decisions, if maintaining cohesion displaces the group's instrumental purpose.[20] Likewise, social cohesion is not necessary for task cohesion; people who do not like one another may work well together nonetheless. Yet both forms of cohesion are related, and both affect unit performance and quality of life for service members. Or do they?

There has been a consensus in the literature that task cohesion is related to performance but social cohesion is not. This consensus is primarily based upon the analysis of 49 studies of group cohesion by Brian Mullen and Carolyn Copper.[21] Mullen and Copper aggregated measures used in these previous studies into two measures of social cohesion—interpersonal attraction and group pride—and one measure of task cohesion: task commitment. They then determined the average independent relationship that each had to group task outcomes.[22] They concluded that the measures of social cohesion were not independently related to measures of performance; task commitment, however, was.[23] "The results of these analyses demonstrate commitment to the task to be the most important component of cohesiveness in the cohesiveness-performance effect . . . Practically, these results indicate that efforts to enhance group performance by fostering interpersonal attraction or 'pumping up' group pride are not likely to be effective."[24]

This finding was accepted in the study of military cohesion because it not only reflected a sound empirical conclusion but it was also consonant with the military's inculcation of a group identity over that of the individual,[25] its honing of (nearly) arbitrarily assigned individuals into task-oriented teams,[26] and its meritocratic culture that focused on job performance as opposed to personalities.[27] Thus it should not be surprising that

arguments that attempt to gauge the effect of allowing homosexuals to openly serve in the military have emphasized the importance of task cohesion over social cohesion. Robert MacCoun, who oversaw the cohesion section of the 1993 RAND study on the issue, argued that

> the established principles of cohesion suggest that the presence of acknowledged homosexuals has an effect, [and] it is most likely to involve social cohesion rather than task cohesion . . . [S]imilarity of social attitudes and beliefs is not associated with task cohesion, although it is sometimes associated with social cohesion. Task cohesion involves . . . a commitment to the group's purposes and objectives. There seems little reason to expect acknowledged homosexuality to influence this commitment . . . [Indeed], Commitment to these values seems particularly likely, given that homosexuals in the military are a self-selected group and enlist despite numerous obstacles and personal and professional risks.[28]

Col Om Prakash, USAF, echoed this argument in his award-winning essay in *Joint Force Quarterly*: the "integration of open homosexuals might degrade social cohesion because of the lack of homogeneity; however, the effects can be mitigated with leadership and will further dissipate with familiarity. More importantly, task cohesion should not be affected and is in fact the determinant in group success."[29] RAND sociologist Laura Miller and Loyola University professor CAPT John Williams, USNR, retired, wrote that "these literature reviews argue that social homogeneity is inconsequential for the work outcomes, and that achieving specific goals creates commonality among otherwise different people and forges productive social bonds."[30] Finally, Bonnie Moradi and Laura Miller analyzed the views of 545 Iraq and Afghanistan war veterans to determine the effect on unit cohesion of knowing that a unit member was gay or lesbian, defined in terms of task cohesion, and after controlling for the effects of NCO and officer leadership, equipment quality, and unit training, found "near 0 percent" effect.[31] This is consistent with the previous literature, which found that social attitudes had no effect on task cohesion but says little about social cohesion.

The problem is that Mullen and Copper's work is no longer the most recent or authoritative integration of the empirical research on cohesion and performance.[32] Beal et al. reconsidered the literature and conclusions reached by Mullen and Copper and expanded upon their work by including more-recent literature.[33] Beal et al. advanced what is known about cohesion by differentiating between outcomes and performance behaviors, between effectiveness and efficiency, accounting for different types of group work flows, and improving upon Mullen and Copper's coding of studies and statistical

procedures.[34] They hypothesized that cohesion would be more important to determining the quality of performance rather than the achievement of outcomes, that it would affect efficiency more than effectiveness, and that cohesion would increase as the collaborative nature of the flow of work within the group increased.

Their findings suggest that the two primary components of social cohesion—interpersonal attraction and group pride—are positively related to group performance, albeit slightly less so than commitment to the task.[35] Still, social cohesion matters to performance, however measured. This is contrary to the previous findings of Mullen and Copper. The data indicate that a one-unit increase in interpersonal attraction is related to an increase in overall performance of almost 20 percent, compared to a 26-percent increase for group pride and a 28-percent increase for task commitment. These relationships are independent of one another. They also differ across the type of performance considered—commitment to task had a stronger relationship than interpersonal attraction when it came to outcomes (27 vs. 14 percent increases, respectively), effectiveness[36] (23 vs. 15 percent), and even efficiency (34 vs. 28 percent). But interpersonal attraction was related to performance behaviors within the group more than task cohesion (31.5 vs. 30 percent). Thus, while commitment to task has a larger relationship than interpersonal attraction and group pride to most measures of performance, the important point is that measures of social cohesion have a large and positive relationship to performance independently of commitment to task.

This new set of conclusions means that social cohesion matters to performance and cannot be ignored in favor of measures of task cohesion when considering changes in personnel policy. To do so would underestimate the negative effects that disruptions to social cohesion can cause as well as underestimate the positive performance effects of efforts to enhance social cohesion.[37] Therefore, most of what constitutes the scholarly consensus on the likely effect of repealing DADT on unit cohesion is outdated and underestimates the probable disruptive impact.

Bringing Social Cohesion Back In

These conclusions bring social cohesion and its determinants back into relevance, in particular those that affect interpersonal attraction and group pride. Beyond the generic effects of propinquity (i.e., mere membership in

a group), group size, quality of leadership, shared threats, and shared successful experiences that should remain constant in the event that DADT is repealed, the determinants of cohesion that have been considered are demographics (sex, race, ethnicity), and homogeneity of attitudes, values, and interests.

Broader studies of demographic diversity and organizational dynamics have found that "the preponderance of the empirical literature suggests that diversity is most likely to impede group functioning."[38] On the other hand, the military sociology literature suggests that racial and ethnic differences do not affect unit cohesion today (although they may have in the past),[39] while gender differences have been found to affect unit cohesion marginally, with effects far smaller than those of rank, work group, generation, or leadership.[40] Still, a recent study of Soldiers' views of civilian contractors (yet another distinctive group) associated with their unit found that "Soldiers' social comparisons with civilian contractors have a significant total effect on cohesion" based upon a perception of relative deprivation.[41]

Given these studies, it is argued that although "superficial" homogeneity based upon racial, ethnic, or gender similarity facilitates initial cohesion, it is underlying values, attitudes, and interests that motivate social cohesion over the long term.[42] These can be shaped by the institution itself.[43] But what values, attitudes, and interests? It is commonly argued that the attitudes, values, and interests of military personnel are more homogenous and circumscribed than those of the American public.[44] Morris Janowitz, for instance, argued that "military ideology has maintained a disapproval of the lack of order and respect for authority which it feels characterizes civilian society. The military believe that the materialism and hedonism of American culture is blocking the essential military virtues of patriotism, duty, and self-sacrifice."[45] The massive influx of conscripts during and after World War II moderated these views by continually introducing citizen-soldiers into the professional and social realm of career military members and providing for more diversity of thought.[46] Janowitz wrote in 1960 that "the social values of the military are probably less at variance with civilian society than they have been at any period of American history."[47]

With the end of conscription, the all-volunteer force has become a self-selected population whose political and social values have become increasingly differentiated from American society as a whole.[48] The work of Ole Hosti, Peter Feaver, and Richard Kohn bear this trend out. Party

identification among military elites shifted from 33 to 64 percent Republican and 12 to 8 percent Democrat from 1976 to 1999, while among civilian elites the shifts were 25 to 30 percent and 42 to 43 percent, respectively.[49] Ideological identification shifted from 16.0 to 4.4 percent liberal and from 61.0 to 66.6 percent conservative among military elites, while among civilian elites the comparable shifts were from 42.0 to 37.5 percent liberal and 30.0 to 31.5 percent conservative from 1976 to 1999.[50] The "gap" between military and civilian views has spawned a large literature analyzing its implications.[51]

Attitude Homogeneity about Homosexuality?

Perhaps what matters most is not the gap in political views but rather views about sexual orientation. Tarak Barkawi and Christopher Dandeker argue that militaries necessarily inculcate "a definite set of values that can be understood in ideal terms as 'warrior masculinity' . . . a specifically masculine and heterosexist soldierly identity . . . [that is] crucial to the competitiveness, the aggressiveness, and the willingness to kill and die required of effective combat formations."[52] The identity encompassed in these attitudes is part of what separates military culture from that of the society at large, they argue. Yet, as they wrote in 1999, only 41.2 percent of military elites agreed that "even though women can serve in the military, the military should remain basically masculine, dominated by male values and characteristics," and only 5.3 percent of military elites indicated that it "greatly hurts" if "the military becom[es] less male-dominated."[53] It would seem that even as they wrote, only a minority of the elite officers that shape the military's culture agreed with Barkawi and Dandeker.

Perhaps these broad conceptual questions about masculinity did not tap the attitudes of military officers with regard to homosexuality in the way that the researchers had hoped. Perhaps it is best to directly address the issue: what is known about the attitudes of military members with regard to homosexuality and its relationship to unit cohesion in particular?

Such data are difficult to acquire. Efforts by the author to survey military personnel on this subject have been repeatedly denied. The best data available are those in a poll conducted by Zogby International of 545 US military personnel who had served in Iraq, Afghanistan, or in combat support roles for personnel in those theaters.[54] The poll was conducted in

October 2006, and its respondents were "fully representative of the US and military population."[55]

The poll asked respondents about their views of homosexuals as well as various performance indicators of their current (or, in the case of veterans, last) unit. The following table presents a summary of the sample's characteristics and breaks out the percentage of agreement/disagreement with the proposition where these data were indicated in the Zogby report, which is when it deviated significantly from the overall sample's response. This average response is indicated by (x) in this table for comparison.[56]

Responses to the question "Do you agree or disagree with allowing gays and lesbians to serve openly in the military?" were as follows: 26 percent agreed, 37 percent disagreed, and 32 percent were neutral.[57] The level of opposition to allowing gays and lesbians to serve openly in different subgroups of the sample, as shown in the table, are 39 percent of active duty, 40 percent of Air Force, 37 percent of Army, 33 percent of Navy, and 32 percent of Marines oppose repealing DADT. Differences also appear when the force is broken down according to sex and race: 40 percent of males, 27 percent of females, 43 percent of Whites, 28 percent of Blacks, and 17 percent of Hispanics oppose repealing DADT. Perhaps predictable as well, differences in opposition also correspond to party identification; 28 percent of Democrats, 41 percent of Republicans, and 45 percent of independents oppose repeal. Views across other sample characteristics, such as rank and unit type, did not deviate substantially from the group average of 37 percent in opposition.[58] This is substantial opposition, yet in no subset of the sample does a majority oppose changing the policy, topping out at 45 percent among self-identified political independents. Still, the opposition outweighs those that agree with lifting the ban. This is true for every subset of the sample—except for females (44 percent vs. 27) and self-identified Democrats (35 percent vs. 28).

Two less-formal measures of acceptance of gays and lesbians in the military tapped by the poll were level of comfort "in the presence of gays and lesbians" generally and whether they were known to be serving in the unit of the respondent. Although 45 percent of respondents indicated that they "suspected" that a member of their unit was gay or a lesbian, only 23 percent indicated that they knew "for certain," and among those respondents 59 percent knew because they were told by the individual. Given the sample's size of 545, that is 125 military members who knew and 74 who were told—in clear violation of DADT. Furthermore, 55 percent of

The Zogby sample and selected responses

Characteristic	Sample #	Sample %	% Agree Allow	% Disagree Allow	% Comfort-able	% Uncomfort-able	% Know
Overall responses			26	37	73	19	23
Duty Status							
Active duty	353	65	23	39	70	(19)	(23)
Reserve/Guard activated	35	6	(26)	(37)	(73)	(19)	(23)
Reserve/Guard not activated	69	13	(26)	(37)	(73)	(19)	(23)
Veteran	88	16	35	(37)	81	(19)	(23)
Service							
Air Force	160	29	29	40	73	23	13
Army	251	46	23	37	69	(19)	25
Marines	35	7	25	32	82	(19)	26
Navy	92	17	31	33	79	(19)	31
Coast Guard	5	1	(26)	(37)	(73)	(19)	(23)
Rank							
Enlisted	—	66	(26)	(37)	(73)	(19)	27
Officer	—	31	23	(37)	(73)	(19)	12
Warrant	—	3	(26)	(37)	(73)	(19)	(23)
Unit Type							
Combat	—	29	(26)	(37)	(73)	(19)	(23)
Combat support	—	32	(26)	(37)	(73)	(19)	(23)
Combat service support	—	18	(26)	(37)	(73)	(19)	(23)
Other/Unsure	—	21	(26)	(37)	(73)	(19)	(23)
Sex							
Male	451	85	24	40	71	22	22
Female	80	15	44	27	88	6	29
Race/Ethnicity							
White	375	73	26	43	(73)	(19)	(23)
Black	62	12	37	28	71	(19)	(23)
Hispanic	47	9	26	17	(73)	(19)	(23)
Asian	13	3	(26)	(37)	(73)	(19)	(23)
Native American	5	1	(26)	(37)	(73)	(19)	(23)
Hawaiian/Pacific Islander	5	1	(26)	(37)	(73)	(19)	(23)
Other	10	2	(26)	(37)	(73)	(19)	(23)
No response	20	—	—	—	—	—	—
Party ID							
Democrat	101	21	35	28	73	(19)	(23)
Republican	241	51	22	41	72	24	(23)
Independent	103	22	36	45	81	(19)	(23)
Not sure	100	7	—	—	—	—	—
No answer	68	—	—	—	—	—	—

Demographic information from Rodgers, *Opinions of Military Personnel*, 3–4. "Veterans" had left the service within the previous five years (p. 9, question 3). "Rank" and "Unit Type" from p. 10. Percentages indicate those that responded, not for the sample as a whole. Reported data reflect this. Response to the allowing service question from pp. 14–15.

all respondents indicated that "the presence of gays or lesbians in the unit [was] well-known by others."[59] Although it is possible that all of these instances were acted upon, it seems unlikely. Perhaps this is because a large majority of respondents (73 percent) reported that they were comfortable in the presence of gays and lesbians, while only 19 percent reported that they were uncomfortable.[60]

The Zogby poll also asked about the effect that the presence of gays and lesbians could have, and has had, on unit morale. When asked about the strongest argument against repealing DADT, 40 percent of respondents indicated that "open gays and lesbians would undermine unit cohesion," and this was the most popular response.[61] This suggests that many respondents were aware of the basis for the DADT policy. Turning to unit morale, the analysis provided by Rodgers differentiated between those who were not certain that their unit had homosexual members and those who knew. For those who were not certain, 58 percent estimated that their presence would negatively impact unit morale, 2 percent thought it would increase morale, and 26 percent forecast no impact. When considering only the respondents who indicated that they were certain that their unit had gay or lesbian members, 27 percent said that this presence negatively affected morale, 3 percent said that it was positive, and 64 percent indicated that it had no impact.[62] It is striking that the knowledge of a gay or lesbian unit member reduced those indicating a negative impact from 58 to 27 percent and increased those indicating no impact from 26 to 64 percent.

It is also clear that some hypothesized concerns may not be borne out. For instance, it has been argued that the members of units more likely to be deployed to Spartan positions where amenities and privacy are scarce would be less likely to accept homosexuals in their midst. The data suggest that the views of personnel in combat units, combat support units, and combat service support units do not differ appreciably from each other or the overall sample, however. Nor is the hypothesis that enlisted members are less likely to be comfortable around homosexuals than officers borne out—indeed they are slightly more accepting of repealing DADT. The data also suggest that members of minority groups, Blacks and women in particular, are less opposed and more willing to repeal DADT.

What does this data reveal about the likely effects of repealing DADT on social cohesion within military units? Clearly, more members oppose changing the policy than favor doing so. Responses to individual questions by the sample and certain subsets are informative as well, in particular the

difference in estimated and actual impact on morale of having a known lesbian or gay unit member. The overall conclusion to be drawn is that military members do not necessarily all share the same attitudes, values, and interests when it comes to DADT. While substantial subsets of the military share general attitudes toward homosexuals and homosexual conduct—negative, as well as tolerant, if not accepting—the attitudes of the entire force are not homogeneous. This suggests there may be difficulties as substantial minorities of military members disagree on the issue.[63] The impact on social cohesion within units will be mixed because the characteristics that most likely define those who disagree are not isolated to particular types of units. Where disruption is likely to occur cannot be determined with the data currently available. We can conclude, however, that changing the policy with regard to gays and lesbians serving openly in the military will negatively if unevenly affect unit performance—at least until attitudes within the force shift sufficiently across the board.[64]

Conclusions

Will social cohesion, and therefore military effectiveness, suffer if DADT is repealed? The Zogby poll of attitudes of US service members toward homosexuals, both generally and in the military, suggests that there is a substantial minority opposed to allowing homosexuals to serve openly in the military, and views on the issue are far from homogenous. The lack of homogeneity in views suggests that allowing gays and lesbians to serve openly may provide a basis for these disagreements to become salient. Given this situation, repealing DADT is likely to have a negative impact on the social cohesion of many units. For these units, social cohesion will likely decrease and have a negative effect on unit performance.

This is an unsatisfying answer for those engaged in the heat of the debate over DADT today, since the size of the disruption and where it is most likely to appear cannot be predicted with what is currently known. Data will soon be available to evaluate, monitor, and forecast the effect that allowing homosexuals to serve openly in the armed forces will have on all components of unit cohesion: commitment to task, interpersonal attraction, and group pride. The 2010 DoD Comprehensive Review Survey of Uniformed Active Duty and Reserve Service Members currently underway includes questions that tap all three forms of cohesion.[65] The original RAND study developed a conceptual position within the context

of DADT that discounted social cohesion and so shaped the subsequent debate. If the update to the RAND study also discounts social cohesion, it is likely to miss a key determinant of unit cohesion and underestimate negative impacts.

Those who are making assessments must take social cohesion into account. Contrary to almost all previous studies of unit cohesion considered in the DADT debate, commitment to task is not the only determinant of cohesion; whether service members like their coworkers matters and whether they have pride in their unit matters. These forms of cohesion are independently and significantly related to performance. Policies that undermine the social cohesion of units in the mistaken belief that only commitment to the task matters will have larger negative effects than anticipated. Formal measurements of unit cohesion should be initiated and continued as a gauge to readiness of the force. In the end, ongoing studies that will determine the policy of the United States with regard to who can serve in the military must take social cohesion into account. SSQ

Notes

1. Barack Obama, "Remarks by the President in State of the Union Address," 27 January 2010, http://www.whitehouse.gov/the-press-office/remarks-president-state-union-address.

2. See David F. Burelli, "*Don't Ask, Don't Tell:" The Law and Military Policy on Same-Sex Behavior,* CRS Report for Congress (Washington: Congressional Research Service, 25 March 2010), 1–7.

3. Elisabeth Bumiller, "Top Defense Officials Seek to End 'Don't Ask, Don't Tell'," *New York Times*, 3 February 2010, A-1, http://www.nytimes.com/2010/02/03/us/politics/03military.html.

4. Bernard D. Rostker and Scott A. Harris (study directors), *Sexual Orientation and U.S. Military Personnel Policy: Options and Assessment*, MR-323-OSD (Santa Monica, CA: RAND, 1993).

5. Quoted in Bumiller, "Top Defense Officials." See Craig Whitlock, "Pentagon Restricts Evidence that can be Used against Gays," *Washington Post*, 26 March 2010, 3, for details of the policy shift.

6. The individual service chiefs supported Secretary Gates' plan to study the issue but expressed trepidation, if not opposition, about changing the policy. See Thom Shanker, "2 Generals Wary About Repealing Gay Policy," *New York Times*, 24 February 2010; and Shanker, "More Calls for Review of Gay Policy," *New York Times*, 25 February 2010.

7. Specifically, Title 10, § 654 asserts, in part, that:

> (6) Success in combat requires military units that are characterized by high morale, good order and discipline, and unit cohesion.
>
> (7) One of the most critical elements in combat capability is unit cohesion, that is, the bonds of trust among individual service members that make the combat effectiveness of a military unit greater than the sum of the combat effectiveness of the individual unit members. . . .
>
> (14) The armed forces must maintain personnel policies that exclude persons whose presence in the armed forces would create an unacceptable risk to the armed forces' high standards of morale, good order and discipline, and unit cohesion that are the essence of military capability.

> (15) The presence in the armed forces of persons who demonstrate a propensity or intent to engage in homosexual acts would create an unacceptable risk to the high standards of morale, good order and discipline, and unit cohesion that are the essence of military capability.

8. Aaron Belkin and Melissa Sheridan Embser-Herbert, "A Modest Proposal: Privacy as a Flawed Rationale for the Exclusion of Gays and Lesbians from the U.S. Military," *International Security* 27, no. 2 (Fall 2002).

9. Bonnie Moradi and Laura Miller, "Attitudes of Iraq and Afghanistan War Veterans toward Gay and Lesbian Service Members," *Armed Forces & Society* 36, no. 3 (April 2010): 412.

10. The survey of 400,000 military personnel (1 in 5) being conducted by Westat on behalf of the OSD will provide excellent data to make such assessments. See Andrea Stone, "Pollsters: Pentagon's Policy Survey May be 'Overkill'," *AOL News*, 13 July 2010, http://ebird.osd.mil/ebfiles/e20110071476358 4.html.

11. S. L. A. Marshall, *Men Against Fire* (New York: William Morrow and Co., 1947); Samuel A. Stouffer et al., *The American Soldier, Volume 2, Combat and Its Aftermath* (Princeton: Princeton University Press, 1949); and Edward A. Shils and Morris O. Janowitz, "Cohesion and Disintegration in the Wehrmacht in World War II," *Public Opinion Quarterly* 12, no. 2 (Summer 1948).

12. Leon Festinger, "Informal Social Communication," *Psychological Review* 57, no. 5 (September 1950): 274.

13. Guy L. Siebold, "The Essence of Military Group Cohesion," *Armed Forces & Society* 33, no. 2 (January 2007): 288.

14. Daniel J. Beal et al., "Cohesion and Performance in Groups: A Meta-Analytic Clarification of Construct Relations," *Journal of Applied Psychology* 88, no. 6 (December 2003): 989. See also Dorwin Cartwright, "The Nature of Group Cohesiveness," in Dorwin Cartwright and Alvin Zander, eds., *Group Dynamics: Research and Theory*, 3d ed. (New York: Harper and Row, 1968); and James H. Davis, *Group Performance* (Reading: Addison-Wesley, 1969).

15. Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge: Harvard University Press, 1965).

16. Herbert A. Simon, *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*, 3d ed. (New York: The Free Press, 1945, 1976), 160–64.

17. Contrary to the argument of Kier, who oddly claimed that "[q]uantitative, experimental, historical, and sociological studies have not found a causal link leading from cohesion to performance. Indeed, group cohesion can diminish an organization's performance." Elizabeth Kier, "Homosexuals in the U.S. Military: Open Integration and Combat Effectiveness," *International Security* 2, no. 23 (Fall 1998): 8. If there is no link, then cohesion should have no impact on performance, good or ill.

18. Robert MacCoun, Andrew Cornell, and John D. Winkler, "Unit Cohesion and Performance," in Rostker and Harris, *Sexual Orientation and U.S. Military Personnel Policy*, 291.

19. Ibid.

20. Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes* (Boston: Houghton Mifflin, 1982); and Marlene E. Turner and Anthony R. Pratkanis, "Theoretical Perspectives on Groupthink: A Twenty-Fifth Anniversary Appraisal," *Organizational Behavior and Human Decision Processes* 73, no. 2/3 (February/March 1998). Whether these effects "may be as likely to undermine performance as enhance it," as claimed by Kier ("Homosexuals in the U.S. Military," 15), is an empirical question that has yet to be addressed.

21. Brian Mullen and Carolyn Copper, "The Relation between Group Cohesiveness and Performance: An Integration," *Psychological Bulletin* 115, no. 2 (March 1994).

22. These factors follow Festinger's seminal formulation. Leon Festinger, "Informal Social Communication," *Psychological Review* 57, no. 5 (September 1950).

23. Accounting for almost 20 percent of the variance in performance in the nonexperimental studies analyzed. Mullen and Copper, "The Relation between Group Cohesiveness and Performance," 222.

24. Ibid., 224.

25. Roy R. Grinker and J. P. Spiegel, *Men Under Stress* (New York: McGraw-Hill, 1945); Shils and Janowitz, "Cohesion and Disintegration in the Wehrmacht in World War II"; Michael A. Hogg, *The Social Psychology of Group Cohesiveness: From Attraction to Social Identity* (New York: New York University Press, 1992); and Michael A. Hogg and Sarah C. Haines, "Intergroup Relations and Group Solidarity: Effects of Group Identification and Social Beliefs on Depersonalized Attraction," *Journal of Personality and Social Psychology* 70, no. 2 (February 1996).

26. As Siebold and Lindsay put it, "A central tenet of current [1999] personnel policy is that the Army can recruit 17-to-21-year-old men (who are capable of meeting certain educational, aptitude, and character standards) from different demographic backgrounds, train them, and assign them to groups with leaders, who also have different demographic backgrounds, to form cohesive, motivated, and competent combat units." Guy L. Siebold and Twila J. Lindsay, "The Relation between Demographic Descriptors and Soldier-Perceived Cohesion and Motivation," *Military Psychology* 11, no. 1 (March 1999): 110.

27. See James Griffith and Mark Vaitkus, "Relating Cohesion to Stress, Strain, Disintegration, and Performance: An Organizing Framework," *Military Psychology* 11, no. 1 (1999); James Griffith, "Multilevel Analysis of Cohesion's Relation to Stress, Well-Being, Identification, Disintegration, and Perceived Combat Readiness," *Military Psychology* 14, no. 3 (2002); Robert J. MacCoun, Elizabeth Kier, and Aaron Belkin, "Does Social Cohesion Determine Motivation in Combat? An Old Question with an Old Answer," *Armed Forces & Society* 32, no. 4 (July 2006); Anthony King, "The Existence of Group Cohesion in the Armed Forces: A Response to Guy Siebold," *Armed Forces & Society* 33, no. 4 (July 2007); Arni Ahronson and James E. Cameron, "The Nature and Consequences of Group Cohesion in a Military Sample," *Military Psychology* 19, no. 1 (2007); and Martha McSally, "Women in Combat: Is the Current Policy Obsolete?" *Duke Journal of Gender Policy and Law* 14 (2007): 1035. For an alternative view that disputes the relevance of the distinction between social and task cohesion for "Army policy," see Leonard Wong, Thomas A. Kolditz, Raymond A. Millen, and Terrence M. Potter, *Why They Fight: Combat Motivation in the Iraq War* (Carlisle Barracks: Strategic Studies Institute, July 2003).

28. Robert J. MacCoun, "Sexual Orientation and Military Cohesion," in Gregory M. Herek, Jared B. Jobe, and Ralph M. Carney, eds., *Out in Force: Sexual Orientation and the Military* (Chicago: University of Chicago Press, 1996), 166.

29. Om Prakash, "The Efficacy of 'Don't Ask, Don't Tell'," *Joint Force Quarterly* 55 (4th Quarter, 2009): 91.

30. Laura L. Miller and John Allen Williams, "Do Military Policies on Gender and Sexuality Undermine Combat Effectiveness?" in Peter D. Feaver and Richard Kohn, eds., *Soldiers* and *Civilians: The Civil-Military Gap and American National Security* (Cambridge: MIT Press, 2001), 394.

31. The question that operationalized cohesion in the questionnaire was, "There is a lot of teamwork and cooperation in my unit." See Moradi and Miller, "Attitudes of Iraq and Afghanistan War Veterans," 412–13, table 6.

32. James Griffith, "Further Considerations Concerning the Cohesion-Performance Relation in Military Setting," *Armed Forces & Society* 34, no. 1 (October 2007): 143.

33. Beal et al., "Cohesion and Performance in Groups."

34. Differentiating task outcomes in terms of performance and achievement allowed them to analyze studies in which external factors could affect the group's performance from those in which they could not. Differentiating between measures of effectiveness and efficiency allowed them to analyze studies in which the level of effort necessary to achieve outcomes was accounted for and those in which it was not.

35. Presenting the mean corrected correlations from table 2, page 997. All studies that examined the effect of group pride on outcomes utilized measures of effectiveness rather than efficiency and outcome rather than performance; therefore, its corrected mean correlation does not vary across these categories.

Mean corrected correlations between cohesion type and performance

Cohesion / Factor	Overall Performance	Performance Behavior	Outcome	Efficiency	Effectiveness
Interpersonal Attraction	.199	.315	.139	.284	.148
Group Pride	.261	—	.261	—	.261
Task Commitment	.278	.302	.273	.343	.232

36. Effectiveness measures outcomes without regard to inputs.

37. Contrary to the conclusion of Mullen and Copper, "The Relation between Group Cohesiveness and Performance," 224.

38. Katherine Y. Williams and Charles A. O'Reilly III, "Demography and Diversity in Organizations: A Review of 40 Years of Research," *Research in Organizational Behavior* 20 (1998): 120; and David A. Harrison, Kenneth H. Price, and Myrtle P. Bell, "Beyond Relational Demography: Time and the Effects of Surface- and Deep-Level Diversity on Work Group Cohesion," *Academy of Management Journal* 41, no. 1 (February 1998).

39. Siebold and Lindsay, "The Relation between Demographic Descriptors." For analyses of the racial integration prior to and during its implementation, see Ulysses Lee, *The Employment of Negro Troops* (Washington: Office of the Chief of Military History, 1966); Leo Bogart, ed., *Social Research and the Desegregation of the U.S. Army* (Chicago: Markham, 1969); Morris J. MacGregor, *Integration of the Armed Forces, 1940–1965* (Washington: Center of Military History, 1981); and Sherie Mershon and Steven Schlossman, *Foxholes and Color Lines: Desegregating the U.S. Armed Forces* (Baltimore: Johns Hopkins University Press, 1998).

40. Indeed, "[p]eople whose unit cohesion appeared to be low were most likely to mention gender as an issue, although gender was only one of several characteristics that separated people—and was often not the primary rift. Moreover, gender separations were often attributed to or thought to have been reinforced by structural components or leadership practices." Margaret C. Harrell and Laura L. Miller, *New Opportunities for Military Women: Effects upon Readiness, Cohesion, and Morale*, MR-896 (Santa Monica: RAND, 1997), 61. Also see Leora N. Rosen et al., "Gender Composition and Group Cohesion in U.S. Army Units: A Comparison across Five Studies," *Armed Forces & Society* 25, no. 3 (April 1999).

41. Ryan Kelty, "Citizen Soldiers and Civilian Contractors: Soldiers' Unit Cohesion and Retention Attitudes in the 'Total Force'," *Journal of Political and Military Sociology* 37, no. 2 (Winter 2009): 147.

42. Miller and Williams, "Do Military Policies on Gender and Sexuality Undermine Combat Effectiveness?" 392.

43. Omer Bartov, *Hitler's Army: Soldiers, Nazis, and War in the Third Reich* (New York: Oxford University Press, 1992).

44. Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge: Belknap Press of Harvard University Press, 1957); Feaver and Kohn, eds., *Soldiers and Civilians*; and Adam B. Lowther, "The Post–9/11 American Serviceman," *Joint Force Quarterly* 58 (July 2010).

45. Morris O. Janowitz, *The Professional Soldier: A Social and Political Portrait* (New York: Free Press, 1960), 248.

46. Ibid., 242, 249.

47. Ibid., 249.

48. As feared by Janowitz, ibid., iii.

49. 1976 figures from Ole R. Holsti, "A Widening Gap between the U.S. Military and Civilian Society? Some Evidence, 1976–96," *International Security* 23, no. 3 (Winter 1998/99): 11, table 1. 1999 figures from Ole R. Holsti, "Of Chasms and Convergences: Attitudes and Beliefs of Civilians and Military Elites at the Start of a New Millennium," in Feaver and Kohn, eds., *Soldiers and Civilians*, 28, table 1.3, utilizing the figure for civilian nonveteran leaders.

50. 1976 figures from Holsti, "A Widening Gap," 13, table 2.

51. Including Jason K. Dempsey, *Our Army: Soldiers, Politics, and American Civil-Military Relations* (Princeton: Princeton University Press, 2009); and Kathy Roth-Douquet and Frank Schaeffer, *AWOL: The Unexcused Absence of America's Upper Classes from Military Service—and How it Hurts Our Country* (New York: HarperCollins, 2005).

52. Tarak Barkawi and Christopher Dandeker, "Rights and Fights: Sexual Orientation and Military Effectiveness," *International Security* 24, no. 1 (Summer 1999): 184.

53. Holsti, "Of Chasms and Convergences," 76, table 1.24; 78, table 1.25.

54. Sam Rodgers, *Opinions of Military Personnel on Sexual Minorities in the Military* (New York: Zogby International, December 2006). This is the data analyzed by Moradi and Miller, "Attitudes of Iraq and Afghanistan War Veterans."

55. Rodgers, *Opinions of Military Personnel*, 2. For further details on the sample, see Moradi and Miller, "Attitudes of Iraq and Afghanistan War Veterans," 402.

56. The margin of error for these estimates when generalizing to the population of US military members is +/– 4.3 percent.

57. Only the overall neutral response was indicated in Rodgers, *Opinions of Military Personnel*. Therefore, it is not included for the subsets in this table.

58. In addition, 41 percent of Baptists opposed allowing homosexuals to serve in the military—the only religious group meriting mention in the report. Rodgers, *Opinions of Military Personnel*, 14.

59. Ibid., 15–18.

60. Interestingly, USAF members were less comfortable than the average, and fewer "certainly" knew of the presence of homosexuals in their unit than the average. Among the religious subset, Catholics displayed the highest comfort rate (78 percent) and Baptists the highest rate of discomfort (26 percent).

61. Rodgers, *Opinions of Military Personnel*, 24.

62. Ibid., 18–19.

63. On the impact that diversity of attitudes has on social cohesion, see Elizabeth Mannix and Margaret A. Neale, "What Differences Make a Difference? The Promise and Reality of Diverse Teams in Organizations," *Psychological Science in the Public Interest* 6, no. 2 (October 2005).

64. Attitudinal shift can occur in two ways: through changes within individuals and through attrition. Attitudes of individuals within groups tend to become more positive as initial differences are shaped through interaction over time. See Harrison, Price, and Bell, "Beyond Relational Demography." With regard to attrition, surveys of the American public, from which the military recruits personnel, suggest a substantial shift in views with regard to homosexuals and homosexuality. These views, however, "tend to be relatively stable [amongst individuals], implying that changes in public opinion largely result from generational differences—i.e., as older generations are replaced with younger generations." Robert Andersen and Tina Fetner, "Cohort Differences in Tolerance of Homosexuality: Attitudinal Change in Canada and the United States, 1981–2000," *Public Opinion Quarterly* 72, no. 2 (Summer 2008): 314. Also see Chelsea E. Schafer and Greg M. Shaw, "The Polls—Trends: Tolerance in the United States," *Public Opinion Quarterly* 73, no. 2 (Summer 2009).

65. The survey was available at https://dadt.csd.disa.mil/ (accessed 16 July 2010).

Cyber Deterrence

Tougher in Theory than in Practice?

Will Goodman

> *In theory, there's no difference between theory and practice. In practice, there is.*
>
> —Yogi Berra

How difficult is cyber deterrence? Some theorists argue that it is quite difficult.[1] These skeptics make valid points; the domain of cyberspace does pose unique challenges for an effective deterrence strategy. But treating cyber deterrence only theoretically—that is, ignoring the geopolitical context in which cyber attacks occur—unintentionally exaggerates its difficulty. Cyber deterrence proves easier in practice than it seems to be in theory because cyber attacks are ultimately inseparable from the physical domain, where deterrence has a long-demonstrated record of success.

Why Yet Another Article (Chapter, Book) on Cyber Deterrence?

Security scholars have recently given more attention to cyberspace because it has evolved into an important domain of interstate conflict. In 2007 Estonia experienced a campaign of cyber attacks that temporarily damaged its economy. Georgia experienced a similar cyber attack campaign in 2008 as an element of its war with Russia. In 2009 the United States and South Korea endured a series of cyber attacks that some suspect originated in North Korea (or Florida, or perhaps elsewhere).[2] Some

The author thanks Alex T. J. Lennon, Diego Chojkier, Lit Kilpatrick, Sergiy Chemezov, Derek Grossman, Rishi Kapoor, and Stephen Abott for their thorough review and helpful comments on earlier drafts of this article. Thanks also to Rain Ottis and Kenneth Geers of the Cooperative Cyber Defense Centre of Excellence for their assistance with research materials.

Will Goodman presently serves as an adviser on defense and veterans issues to Senator Patrick Leahy. As the assistant for plans to the assistant secretary of defense for homeland defense and America's security affairs, he oversaw operational and contingency plans, participated in national-level exercises, and managed several counterterrorism portfolios. Mr. Goodman is a graduate of Georgetown University and the University of Florida.

major powers, such as China, have adapted their military strategies to the characteristics of the cyber environment.[3] Real cases of "cyber war" and overt strategizing by government and military analysts around the world have attracted more scholars to the subject of conflict in cyberspace.

As theorists have questioned how to prevent or defend against cyber attacks in the future, they have included deterrence as a possible approach. Deterrence strategy goes back at least to Thucydides and the Peloponnesian War,[4] and the subject had a major renaissance during the Cold War as the United States and the Soviet Union sought to avoid a nuclear exchange. Since that conceptual high-water mark,[5] analysts have applied deterrence concepts to contemporary security problems, like terrorism, with at least some success.[6] Authors have asked if deterrence could prove useful in cyberspace, too.

In addition to its potential effectiveness, deterrence is cheaper than its alternative, continuous conflict. Cyber warfare like the 2007 attack on Estonia can inflict substantial economic costs on the victim.[7] When states combine cyber attacks with conventional operations, cyber attacks can cost lives.[8] Although cyber deterrence requires expenditures on new capabilities, these costs seem minor compared to an even temporary loss of networked marketplaces or vital financial information. Conflict imposes human and material costs, and deterrence, as conflict avoidance, offers a way to escape those costs. The possibility of securing cyberspace without the costs of conflict keeps scholars interested in cyber deterrence.[9]

These three factors—a future potentially filled with cyber wars, the past efficacy of deterrence in other domains, and its relatively low cost—have made cyber deterrence a popular subject for articles, chapters, and books. When Prof. James Der Derian coined the term *cyber deterrence* in a 1994 issue of *Wired Magazine*, he considered the deterrent effect that network technologies might have on the physical battlefield.[10] Scholar Richard Harknett focused the subject on conflict taking place in cyberspace itself in a 1996 article.[11] Since Harknett, at least 20 other authors have made varying contributions to the study of cyber deterrence. All this work has laid a solid theoretical foundation.

Despite the theoretical scholarship, a critical lack of case studies has created debate over the efficacy of cyber deterrence. Articles on the subject offer theories but nothing to test those theories. Theorists agree that cyberspace poses new challenges for deterrence not found in other domains, but they do not agree on whether those challenges can be overcome.[12] With

the literature consisting of nothing but theories, scholars can offer only educated opinions.

This study aims to augment the existing literature by evaluating the generally agreed-upon challenges of cyber deterrence using cases where cyber deterrence failed. The cases will demonstrate whether in fact those difficulties played an actual role in several cases of cyber conflict. Although different analysts may draw different conclusions from the evidence, using cases as the grounds for debate should give theorists more to discuss than pure theory.

Method and Findings

The analysis begins with the basics of deterrence theory, advances a brief specific theory of cyber deterrence, describes several cases of cyber conflict to illuminate and evaluate the problems of cyber deterrence, and concludes with the implications of its findings for future cyber deterrence strategies. The cases each address deterrence failures because a deterrence failure results in conflict, a phenomenon which can be studied. On the other hand, deterrence success results in the absence of conflict—in other words, the absence of an identifiable political phenomenon—so it cannot be conclusively studied. Unfortunately, evaluating why some conflicts occur cannot fully or satisfyingly explain why conflict does not occur in other cases. This method does get the conversation started, however, and analysts may presume that future cyber deterrence strategies must address at least those factors which led to cyber conflict in the cases addressed here.

Each case highlights a different aspect of cyber conflict. The 2007 Estonia case exemplifies a "pure" cyber war, where conflict took place only in cyberspace. It provides the best opportunity to evaluate the "contestability" of cyber deterrence and the potential for assigned responsibility. The 2008 Georgia case exemplifies cyber attack as one of several combined arms in an ongoing war and offers an example of the adverse effects of scalability and temporality in cyberspace as well as the potentially positive effects of futility as an element of cyber deterrence. Cases OP 1, OP 2, and OP 3[13] exemplify why cyber espionage deserves a distinct category in cyber deterrence strategies. Although these supposed cases of cyber espionage against the United States evoked anger in Americans and a desire to retaliate,[14] the refusal of the United States to reassure its potential adversaries that it will also forgo spying in cyberspace kept the government from hitting back aggressively. Among these cases, OP 3 in particular reinforces the

need for thorough investigation to avoid convicting innocent parties in cyber attacks.

This study evaluates only cases of suspected state-instigated cyber attack because states are the preeminent actors in cyberspace. States are the most capable and highly funded potential adversaries, so deterring state-based attacks will yield the greatest benefit to overall security. Moreover, if malicious state-based cyber activity decreases, states can focus their resources on defending against and prosecuting malicious nonstate and criminal activities in cyberspace. Finally, a clear articulation of what is acceptable behavior for states in cyberspace should help create norms for everyone.

The cases have major implications for future cyber deterrence strategies. The Estonia and Georgia cases reveal that attribution is not the insurmountable challenge that theoretical models suggest. While an unambiguous *strategic* cyber threat has yet to materialize, some of today's attacks may be harbingers of much worse attacks to come. While futility, interdependence, and counterproductivity are potent in the cyber domain, they have yet to prove themselves as potent as retaliation. The cyber espionage (OP 1–3) and the Estonia cases demonstrate that while reassurance cannot enforce deterrence, its absence certainly can detract from an otherwise effective deterrence posture. The Estonia and Georgia cases also prove that escalation dominance is a key component of cyber deterrence. Finally, the cases imply that the United States and other countries must be clearer about how they will respond to certain types of cyber attacks. While deterrence in cyberspace does pose challenges, the cases evaluated in this study prove that deterrence in cyberspace remains inextricably linked to the geopolitics of the physical world. As a consequence, cyber deterrence turns out to be simpler in real life than it appears to be in many theoretical models.

Deterrence Basics

While "no single theory of deterrence exists,"[15] authors offer mostly similar lists of deterrence components. For the purposes of this study, deterrence has eight elements: an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost-benefit calculation.

A state employs a deterrence strategy to protect an interest.[16] To keep adversaries from attacking the interest, a state makes a deterrent declaration,[17] "Do not do *this*, or else *that* will happen." *This* is any adversary action that would threaten the interest. *That* includes either denial

measures,[18] penalty measures,[19] or both. For other states to take a deterrent declaration seriously, the declaration must be credible and reassuring. Credibility means that the deterrent declaration is believable,[20] and reassurance means that if a state does not attack the interest, it can rest assured that it will not face penalties.[21] Fear also plays a role.[22] If a potential adversary fears the denial or penalty measures, that actor is less likely to take an undesirable action. These elements all factor into an adversary cost-benefit calculation: what are the benefits and costs of action versus the benefits and costs of restraint?[23] While these basic definitions may suffice, denial, penalty, credibility, and reassurance each deserve some further explanation.

Denial is the defensive aspect of deterrence and consists of prevention and futility. Deterrence by prevention means that if an attack is launched, defensive measures will disrupt the attack to keep it from succeeding. Deterrence by futility means that even if an attack breaches defenses, it will not have its desired effect on the target.[24] Effective prevention and futility both signify that attacks will inevitably fail and thus serve to deter even the attempt to attack.

Penalty is the offensive aspect of deterrence and consists of retaliation, interdependency, and counterproductivity. Retaliation is a familiar concept: during or after an attack, the defender launches a counterstrike that imposes costs on the attacker that outweigh the benefits gained from the initial attack. Interdependency and counterproductivity are less familiar. Interdependency means both the attacker and the defender hold the interest in common.[25] The more both parties agree on the commonality of the interest, the more costly an attack becomes for the attacker and defender alike. Counterproductivity relates an attacker's tactical goals to its strategic goals. If a defender can convince potential attackers that a tactically successful attack will frustrate larger strategic or normative goals, that may keep the attackers at bay. For example, if the United States punished the families of suicide bombers, terrorists might be deterred from suicide bombing; however, such an approach would be morally repugnant to the United States (normatively counterproductive) and would have adverse effects on broader US goals (strategically counterproductive). Retaliation, interdependency, and counterproductivity together comprise deterrence by penalty.

Credibility is the attacker's calculation of the defender's capability and intent to carry out the deterrent declaration[26] and whether the deterrent measures can be contested. Capabilities are a defender's tools of denial or

penalty: can those tools be used as described by the deterrent declaration? For example, no one would find a threat of nuclear retaliation credible if it came from a state that has only conventional capabilities. To be credible, a defender must also have the intent to use the capabilities to carry out the deterrent declaration. An attacker would not question whether the United States has nuclear weapons, for example, but an attacker might question whether or not the United States would use them to retaliate against a conventional attack. The concept of contestability is more complex. To be incontestable, deterrent measures (either denial or penalty) must be certain, severe, and immediate.[27] The less certain, severe, or immediate a deterrent measure, the less credible potential adversaries will find deterrence declarations, and the more potential adversaries will seek to test them. Capability, intent, and incontestability together define the credibility of a deterrent declaration.

Last, reassurance means giving a potential adversary a reason not to attack the interest. Reassurance most often comes in the form of reciprocal security guarantees—one state promises to forgo an activity if others do so as well. In some cases, however, it may mean other linked benefits such as foreign aid or a special trading status. While deterrence increases the potential costs and lowers the potential benefits of acting against an interest, reassurance lowers the costs and increases the benefits of inaction.

All of these components (an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost-benefit calculation) together form a strong and effective deterrence strategy.

A Theory of Cyber Deterrence

Cyber deterrence, like all other deterrence, succeeds when an adversary decides not to act aggressively. This decision follows two separate assessments: whether the costs of cyber aggression outweigh its benefits and whether the benefits of restraint in cyberspace outweigh its costs. These assessments are made partly rationally, partly irrationally. To be completely rational, a decision maker would need both perfect information about the scenario of potential conflict and the willingness to make a decision only on the basis of its strategic implications. In real life, decision makers have incomplete information, which is rife with inaccuracies, and consider many factors (personal emotions and interests, domestic politics, etc.) when making decisions. Therefore, continual dialogue, in the form of a regular exchange of deterrent messages, is the first necessary condi-

tion to deter cyber aggression. During the Cold War, the United States and the Soviet Union famously created channels for crisis and noncrisis communications (for example, "the Hotline") to engender this exchange of deterrent messages. If states currently exchange cyber deterrence messages, they do so quietly and with little fanfare—likely contributing to the prevalence of cyber attacks.

Both denial and penalty measures feed into an adversary's calculation of whether or not the costs of cyber aggression outweigh the benefits. By taking cyber attack targets offline, by making them impenetrably secure, or by making attacks impossibly futile, denial measures diminish the benefits of a possible cyber attack. Denial, however, is not in itself sufficient to deter aggression in cyberspace. Adversaries must also face some threat of penalty—which raises the costs of cyber attack—for deterrent messages to take effect. If adversaries do not face penalties, they will continue to mount unsuccessful cyber attacks until they find an effective approach. While denial admittedly cannot stand alone, strong denial measures coupled with a reasonable expectation of penalty will go a long way toward deterring cyber aggression.

In addition to strong denial measures, classical deterrence theory demands that penalty measures be certain, severe, and immediate; however, cyber deterrence emphasizes certainty more so than severity or immediacy. Because of the dire consequences involved, nuclear deterrence necessitated that mutually deterring states be able to quickly and overwhelmingly counterattack. But cyber attacks typically involve less-serious consequences, less-identifiable attackers, and a wider variety of tools for counterattack. With less-serious consequences, counterattacks do not need to involve overwhelmingly severe (and disproportionate) retaliation. Neither does the counterattack need to come immediately, for unlike a surprise nuclear first strike, few, if any, cyber attacks can render a victim state completely impotent to respond. For these reasons, neither severity nor immediacy is ultimately necessary for cyber deterrence penalty measures—only certainty.

For a cyber counterattack to be certain, the deterring state must first know who to counterattack. Gathering this information in the cyber domain is trickier than in the physical domain. It takes thorough investigation enabled by international cooperation. States that will not assist in cyber investigations can prevent the identification of the culprits behind cyber attacks. However, in such instances, victim states can, based on mutual legal aid agreements or the inherent right to self-defense, assign

responsibility for the attack to the non-cooperating state. In such cases, assigned responsibility obviates the need for further investigation and incentivizes future cooperation.

Besides knowing who to counterattack, states must also have the means and the will to counterattack to deter cyber aggression. Because cyber attacks can disable networks used to command and control military technologies, and because more and more military technologies are enabled by linkages to cyberspace, states must either inure their weapon systems to cyber attack or remove them from the grid entirely. Otherwise, in some extreme cases, a victim state may find much of its counterattack weaponry preemptively disabled. A victim state must also have the will to counterattack to convincingly threaten retaliation. In this area, cyber deterrence greatly resembles conventional deterrence. A victim state must count the cost before retaliating—if it cannot match its adversary in an escalating series of retaliations, then it should forgo retaliation in the first place. The state with escalation dominance, the coup de grâce, will eventually win. So to have an effective cyber deterrent, a state must have at least geopolitical symmetry with its adversary, if not a favorable asymmetry, to protect itself as the conflict in cyberspace escalates and spills over into the physical domain.

Last, while reassurance does not necessarily bolster cyber deterrence, its absence certainly encourages conflict. States should consider reassurance the "velvet glove" of cyber deterrence—without an iron fist of interlocking denial and penalty measures giving force to reassurance, promises to give up certain types of cyber attacks are an invitation to be victimized. Yet without some reassurances overlaying denial and penalty measures, states will never cease to probe for and exploit minor weaknesses in each others' cyber networks.

Combined, these conditions and variables add up to cyber deterrence. States must continually communicate on matters of cyber conflict to ensure that deterrent messages are projected, received, and understood. States must maintain effective denial measures and threaten credible penalties. If attacked, victim states must be able to correctly identify the responsible state or states to counterattack, either through effective investigation or assigned responsibility. States must ensure that at least some of their counterattack capabilities cannot be disabled by an overwhelming cyber first strike. Most importantly, the deterring state must have geopolitical symmetry, if not a favorable asymmetry, with potential adversaries to deter

them from cyber aggression. Last, the absence of reassuring promises can hinder states wishing to reach a stable cyber deterrence relationship. In each of the cases that follow, the absence of one or more of these variables led to a breakdown in mutual cyber deterrence.

Cyber Deterrence Failure Cases

Estonia, 2007

The cyber attacks began shortly after a decision by the Estonian government to move a WWII–era statue that memorializes the sacrifice of Soviet troops who fought against the Nazis. Since 1947, the Bronze Soldier stood at a busy intersection in central Tallinn, the capital of Estonia, but the government decision relocated it to a nearby military cemetery. Although such a change might seem minor to outsiders, moving the statue heightened tension between ethnic Estonians, ethnic Russians living in Estonia, and the governments of Russia and Estonia. According to at least one commentator, the statue symbolized that Estonia remained in the Russian sphere of influence.

This cyber barrage on Estonian government, banking, and media websites began on 27 April 2007 and lasted for 22 days. The attacks mostly consisted of huge numbers of privately owned computers jamming Estonian government and business websites with meaningless or malicious information. These "distributed denial of service" (DDOS) attacks flooded their targets with data to prevent the processing of legitimate Internet traffic.[28] Hackers also defaced websites, but these attacks seemed minor in comparison to the DDOS attacks that froze web servers, e-mail servers, and the Estonian network infrastructure. The DDOS attacks used "bot nets," or networks of infected "zombie" computers owned by potentially unwitting and innocent bystanders. The mass attacks lasted until 18 May, although isolated and easily mitigated attacks continued thereafter.[29] While police were able to quickly quell a real-world riot over the Bronze Soldier, the cyber attacks on Estonia continued for weeks.[30]

Because Estonia depends heavily on its cyber infrastructure, the attacks could have been devastating. Commentators call Estonia "a primitive cyber society" because of how integral the Internet has become for commercial, government, and interpersonal transactions. For example, Estonians vote online, 98 percent of all bank transactions occur online, doctors store

medical records online, and Estonian police and courts use an online case management system.[31]

Estonia's response to the attacks proved effective. It initially closed off parts of its network to some international traffic. States with numerous clients but few attackers were slowly permitted back onto Estonian networks. While the attacks targeted sectors of Estonian cyber society that were especially critical, the attacks did not cause serious damage because of the highly capable members of Estonia's computer emergency response team.[32]

Analysts debated and continue to debate whether or not the Russian government ordered the attacks. Only one person, an Estonian of Russian descent, was actually charged and convicted; however, Estonian officials claimed to have also identified responsible individuals in Russia.[33] Russian-language forums and websites posted instructions on when and how to execute the DDOS attacks. Some evidence has implicated Russian criminal networks as "bot net herders," or those responsible for controlling personal computers infected with bot net viruses.[34] Estonian officials claim that Internet protocol (IP) addresses belonging to members of Putin's cabinet were used in the attacks.[35] Although Russia and Estonia have a mutual legal assistance treaty which Estonia invoked after the attacks, Russia refused to assist Estonian investigation efforts. That refusal made in-depth investigation of the attacks impossible and cast a shadow of Russian culpability, or at least complicity, over the attacks.[36] During the period of the computer attacks, the Russian government also banned heavy commercial traffic with Estonia across the border bridge at Narva, seeming to provide an official sanction for anti-Estonian behavior.[37] However, none of this circumstantial evidence constitutes a conclusive "smoking gun" that proves the Russian government authorized the attack.

Disadvantages of Cyber Deterrence: Contestability. The 2007 cyber attacks on Estonia showcase a major problem for cyber deterrence strategies, contestability. Cyber deterrence messages seem contestable because of three mutually reinforcing factors: anonymity, asymmetry, and superempowerment.

Without a doubt, anonymity poses great difficulty for cyber deterrence. Because Internet protocols were not developed with identity authentication in mind, investigators must battle the anonymity inherent to the Internet every time they look for clues about who executed a cyber attack.[38] Although it may appear that a cyber attack originated in a certain computer system, that system may have served only as a transit point. In fact,

some actors may use transit points to stage "false flag operations" with the objective of fomenting strife between two other parties (e.g., Russia and Estonia).[39] Even if an investigator can verify an attacker's identity, the investigator cannot know the attacker's motive—did the attacker freelance, act on orders, or attack by accident?[40] A thorough investigation may take quite some time; some so long that the counterattack seems more like aggression than retaliation.[41] Combined, these factors lessen the likelihood that the defending state will retaliate, or if it does, that it will correctly target the responsible entities. The anonymity of cyberspace causes big problems for cyber deterrence.

The 2007 Estonia case also exemplifies the asymmetry of cyberspace. Even if investigators could attribute the attack to an actor (say, Russia), that actor may not offer Estonia any target in cyberspace worthy of retaliation. Estonia depends much more on the Internet than Russia—any Estonian counterattack on Russian networks would not have nearly the impact of a Russian attack on Estonian networks. On the other hand, states face a challenge trying to create proportional effects in the physical world. If one state has more to lose in cyberspace than another, the defending state must find other interests to hold hostage.[42] But can states really "kill people who kill bits?"[43] At the very least, cyberspace asymmetry will cause defenders to think twice before retaliating asymmetrically or disproportionately, which weakens deterrence.

Finally, the 2007 cyber attacks on Estonia illustrate how the Internet creates super-empowered actors. Although Estonia insists that others were involved, only one individual has faced criminal charges for the attacks. If an individual using a personal computer can execute an attack on major national or international targets, then individuals become the equals of states in cyberspace.[44] This poses obvious problems as states attempt to develop an effective cyber deterrence strategy. The deterring of states poses enough of a challenge; deterring super-empowered individuals seems almost impossible.

Advantages of Cyber Deterrence: Assigned Responsibility. The 2007 Estonia case does not offer only bad news. While contestability does pose challenges for cyber deterrence, cyberspace also allows for assigned responsibility. Although cyberspace may be a stateless domain, the individuals that manipulate information in cyberspace do so sitting in the real world—where states are supreme. International law and domestic criminal laws could be updated and improved to hold states responsible, make them

liable, or at least encourage mutual assistance in fighting cyber attacks that originate in their territory (like the treaty shared by Estonia and Russia that Russia failed to honor).[45] Moreover, information travels the World Wide Web along technology owned by a handful of private network infrastructure firms.[46] Although states would not retaliate against businesses for third-party traffic on their networks, states could establish agreements under which these companies would provide key information to investigators seeking to attribute malicious activity in cyberspace.[47] Cyber attacks offer the possibility of assigning responsibility to states or infrastructure providers if they refuse to help attribute cyber attacks to the guilty parties.

Why Did Cyber Deterrence Fail? Although many attackers clearly got away with participating in the 2007 attack, Estonia had the opportunity to assign responsibility to Russia—an opportunity it could not exploit because of the geopolitical imbalance between the two states. Anonymity and super-empowerment did play a role. Investigators still disagree among themselves over whether or not the evidence proves Russian culpability. They cannot conclude that Russia officially ordered the attacks, partly because super-empowered individuals could have hijacked the network addresses of Russian officials and others to make the attacks appear state sponsored. Attackers probably considered these advantages before deciding to attack.

On the other hand, Estonia could have assigned responsibility for the attacks to Russia. International law provides a basis for assigning the culpability of the attacks to Russia even if Russia did not officially direct them.[48] Setting matters of attribution aside,[49] Russia reneged on a standing mutual legal aid agreement with Estonia that required its investigation assistance. Russia's refusal to honor its international agreements meant that the perpetrators escaped justice. Attribution poses no challenge at all in the 2007 cyber attack on Estonia because Russia accepted responsibility for the attack on behalf of the guilty parties.

As a counterargument to assigning responsibility to Russia, some might question whether Russia had a legitimate reason to refuse to support Estonia's investigation—but most reasons seem strained. According to Estonian cyber investigator Rain Ottis, Estonia made "a formal investigation assistance request" to Russia that Russia refused despite "the fact that this type of cooperation is specifically 'enumerated in the Mutual Legal Assistance Treaty' between Estonia and Russia."[50] If Russia considered such investigation assistance unwise in principle, its leaders probably would not have agreed to the mutual legal aid treaty in the first place. Moreover, Russia

should have no fear of Estonian investigators exploiting its networks, since Russian investigators could observe, manage, and control the investigation assistance they provided. The facts of the case do not seem to offer Russia a good reason to refuse legal assistance to Estonia other than that further investigation might have revealed official Russian involvement.

Asymmetry also played a role in the attack on Estonia, but physical asymmetry more so than cyber asymmetry. Russia—or groups sympathetic to Russia—had cyber-bullied tiny Estonia. Certainly, Russia did not offer to Estonia the broad selection of cyberspace targets that Estonia offered to Russia. More importantly, Estonia could not have retaliated in any manner without risking further unwanted Russian escalations. Had the two states shared a more reasonable geopolitical balance, Estonia might have looked to the effects of Russia's attack—on Estonia's economy, business transactions, media, and the like—to determine a course of retaliatory action that might yield similar effects (whether the counterattacks targeted Russian cyberspace or not).[51] Instead, Russia's substantial power compared to its relatively powerless neighbor deterred Estonian retaliation. Physical asymmetry between Estonia and Russia, more so than cyber asymmetry, facilitated the 2007 cyber attack.

Estonia's cyber deterrence posture did prove as contestable as theorists have predicted but not to the degree that they have predicted. Although attribution efforts proved inconclusive, this was a consequence of Russia's refusal to honor its standing legal agreements with Estonia. That refusal gave Estonia the option of assigning responsibility for the attack to Russia. However, even if Estonia had assigned responsibility to Russia, the geopolitical asymmetry between the two states would have left it with few retaliatory options. Instead, Estonia sought to rebalance its relationship with Russia by appealing to its NATO allies to add cyber defense to the NATO charter.[52] By seeking NATO involvement in combined cyber defense, Estonia passed over retaliation in favor of improving its geopolitical parity with Russia and increasing its chances at deterring future cyber attacks through the threat of combined NATO response.

Georgia, 2008

In the summer of 2008, many days prior to Russia's military invasion of Georgia, cyber attacks began on its websites and network infrastructure.[53] These attacks effectively disabled Georgia's web-based communication with the outside world and made it very difficult to offer the global

media its perspective on the conflict. According to reports, attacks were "well-coordinated with what Russian troops were doing on the ground"[54] and lasted through the duration of the 2008 Russian-Georgian conflict.[55]

The attacks share remarkable similarities with the cyber attacks on Estonia the previous year.[56] Government, bank, business, and media websites suffered worst. To raise international awareness about the attack, Georgia had to work around its Internet blackout to plead for international support and assistance.[57] The attacks mostly consisted of DDOS, again with some limited attempts at network intrusions. Attackers even targeted Russian media outlets that provided a more balanced, occasionally pro-Georgian take on the war. Based on subsequent network activities, analysts now speculate that some intruders left malware "time-bombs" to create havoc even after the shooting war concluded.[58]

Unlike the Estonian attacks, the cyber attacks on Georgia had "a strategic economic impact." In addition to sowing general confusion, combined physical and cyber attacks diverted business from Georgian fuel pipelines over to Russian infrastructure offering a similar service at twice the expense. The attacks reinforced Russian military operations by limiting access to secondary sources of power after physical attacks disabled Georgian electrical power grids. To execute such coordinated assaults, attackers used social networking services like Twitter and Facebook.[59] According to at least one Russian media source, Georgian hackers mounted an ineffective counterattack.[60]

Georgia was less prepared than Estonia to confront the cyber assault, but its international partners and private industry jumped to assist. Estonia, Lithuania, and Poland offered to host some Georgian government websites on their better-defended systems.[61] Google also provided assistance to some of Georgia's private business websites, hosting them on higher-bandwidth Blogspot accounts.[62] Russia prevailed over Georgia in cyberspace, although at the time Georgia probably feared Russia's physical attack more than its cyber attack.[63]

Although the strategic context strongly indicates official Russian involvement, like the 2007 attacks on Estonia, investigations have not revealed a smoking gun. The Russian government may have directed the attacks, but some other organization, like the Russian Business Network (RBN), probably coordinated them. The RBN is a "cyber mafia" that traffics in child pornography, identity theft, and other web-based crime and rents its expertise, including DDOS attacks, out to the highest bidder.[64]

Computers belonging to Russian, Ukrainian, and Latvian civilians with no connections to the Russian government or military actually carried out the attacks.[65]

Disadvantages of Cyber Deterrence: Scalability and Temporality. The 2008 Russian operation against Georgia highlights a couple of additional cyber deterrence problems: scalability and temporality. Scalability refers to the wide variety of effects that a single capability can achieve in cyberspace. In the physical world, capabilities have a limited set of purposes, and "both the modalities for attack and the severity of outcomes generally scale predictably."[66] A tank, a nuclear weapon, and a balled fist all have certain predictable effects. In cyberspace, a single tool can achieve a wide spectrum of effects, making it much harder to predict the scale of an attack from attack indications and warnings. For example, during the attack on Georgia, hackers defaced government websites, causing some mild inconvenience but no long-term disruption. They also left hidden, time-sensitive viruses on government systems that unpredictably wreaked havoc on Georgian networks after the intrusions had concluded. Since the same platform and similar techniques were used for both immediate and long-term attacks, defenders were challenged to define beforehand how they would respond to certain adversary actions.

Scalability thus creates problems for establishing deterrence thresholds.[67] Because a single capability can produce a variety of outcomes, deterrence messages must address effects, not actions. A formerly simple message, "You cannot do *this*," becomes much more complicated, "You cannot do *anything* that has *these effects*." This "effects-based" approach must also account for potential effects—such as those caused by time-delayed malware. Not knowing the scale or purpose of a potential adversary's cyber activities makes it difficult to craft an effective and incontestable deterrent declaration.

Temporality refers to the instantaneous nature of cyber attacks.[68] The physical world, hampered as it is by friction, gives defenders early warning of attacks: aircraft or missile radar signatures, satellite photographs of launch preparations, massed tanks on the border. Some activities in cyberspace, like bot net viruses, "packet sniffing," and network reconnaissance,[69] indicate some kind of future malice. But these digital signals do not signify when, how, against whom, and for what purpose network intrusions or other cyber attacks might occur, whereas physical signals provide most or all of that information. Cyberspace provides no unambiguous attack signatures like those offered by the physical world.

Advantages of Cyber Deterrence: Futility. On the other hand, futility offers defenders some major deterrence advantages in cyberspace. Digital information can be replicated endlessly.[70] Redundancy and recovery—very expensive in the physical domain—cost almost nothing in cyberspace.[71] As the Georgia case proved, even if a defender has not taken precautions against cyber attack, outside assistance (like that offered by Georgia's neighbors and Google) can still quickly create redundant systems to help in recovery. Although attackers may corrupt or destroy data saved in one location, that data can have numerous copies elsewhere, rendering many cyber attacks futile and eliminating the motive to execute them.

Defenders can also render cyber attacks futile by disconnecting systems from public networks or removing known vulnerabilities. As analyst Martin Libicki points out, there is "no forced entry in cyberspace."[72] Attackers can only attack where a vulnerability in the network already exists. Removing vulnerability or taking equipment offline means any attempt to attack that equipment through cyberspace will be futile. For example, Georgian advanced air defense systems proved resilient in the face of Russian attack and shot down several highly capable Russian aircraft. Some suggest that Georgian air defenses proved less vulnerable to Russian blackout because the Georgians had not networked them.[73] Taking some critical systems off of the network may at times prove a better option than attempting to secure critical systems from cyber attack.

Why Did Cyber Deterrence Fail? The cyber attack on Georgia occurred in the context of an ongoing war with Russia in another case where geopolitical factors trumped the theoretical difficulties of cyber deterrence. Although anonymity and super-empowerment did play a role in the 2008 cyber conflict, most observers assume a connection between the Russian military attacks on Georgia and concurrent "anonymous" cyber attacks. Super-empowered private citizens did appear to play a role in the cyber attacks,[74] but Russia led the overall war effort.

Scalability also played a role rendered moot by the two countries' conventional asymmetry. As noted earlier, hackers placed malware time bombs in Georgian network systems. Deterring less-obvious cyber attack tactics like this one will prove challenging in the future. Georgia probably had more concerns about the physical bombs falling on its territory than any digital "bombs" hidden in its networks.

Cyber asymmetry, temporality, assigned responsibility, and futility also pale in importance to the geopolitical asymmetry between Russia and

Georgia. How, if it could not deter Russia's full-scale kinetic attack, could Georgia possibly hope to deter its cyber attack? Although temporality, under other circumstances, might have made it more difficult to deter a Russian cyber attack, Georgia might have also had the opportunity to invoke assigned responsibility if Russia proved unwilling to help in Georgia's investigation (creating circumstances similar to those in Estonia in 2007). However, even under those circumstances, Georgia would have had few options. To what end would it assign responsibility to Russia? It could not strike back against its behemoth neighbor. In every aspect, the geopolitical relationship between Russia and Georgia trumped the advantages and disadvantages of cyber deterrence identified by theorists.

In the case of the 2008 Russo-Georgian war, cyber deterrence did prove very difficult but not for the reasons identified by the theorists. With cyber attacks used as one of several combined arms, cyber deterrence became a lesser included subset of conventional deterrence. Between more balanced states (such as the United States and Russia), factors like mutual legal aid or, alternatively, assigned responsibility probably would have kept cyber attacks from commencing. In seeming recognition of this point, Georgia has long pushed to gain membership in NATO. While analysts interpret this desire in different ways, at least some suggest that Georgia seeks parity with Russia through combined defense.[75] As in the case of Estonian cyber conflict, geopolitics played a greater role than the challenges of cyber deterrence.

Cyber Espionage

OP 1

The US government purportedly first discovered OP 1 in March 1998, and the attacks continued through at least 2001. No apparent international crises or behaviors precipitated this series of intrusions; they consisted purely of attempts to collect information through cyber espionage. OP 1 intrusions targeted government and military cyber networks, with attackers penetrating systems by "tunneling" through routine programs and scripts, making it difficult for security analysts to detect the intrusions. According to an FBI source, OP 1 intrusions stole "unclassified but still sensitive information" about technical research, contracts, encryption, and war planning.[76]

Although investigators have not publicly identified a culprit, the OP 1 attacks appear to have come from Russian Internet addresses.[77] Some analysts outside the government conjecture that the sophistication of OP 1 suggests Russian state direction. Others consider "direction" an overstatement, but even some of these believe the attacks must be, at a minimum, "state allowed."[78] "The hackers have built 'back doors' through which they can re-enter the infiltrated systems at will and steal further data; they have also left behind tools that reroute specific network traffic through Russia."[79] While confusion about authorship lingers, circumstantial evidence again points to Russia.

The United States has pursued a few response options. First, the US government lodged a formal diplomatic complaint with Russia. Media reports state that although "hack-backs" (intruding on the systems used to launch attacks on US networks) would provide better information about the source of the attacks, investigators have relied on passive detection due to concerns about legality and the risk of creating an international incident.[80] Although OP 1 led to "the largest cyber-intelligence investigation" ever conducted by the US intelligence community prior to 2001, that investigation yielded "disturbingly few clues" about the perpetrators.[81]

OP 2

Like OP 1, OP 2 consists of attempts to collect US secrets through cyber espionage. In OP 2, hackers exploited NASA, the Sandia National Labs, and other government and military networks that contained unclassified but sensitive and proprietary information.[82] The attacks had a broad scope and collected a substantial volume of information. Regardless, officials report that OP 2 is "not the biggest thing going on out there" in the world of cyber espionage.[83]

The OP 2 attackers' methods exhibited a high level of professionalism. The attacks extracted sensitive information quickly and deliberately wiped away evidence of transiting the networks in an attempt to keep the attacks clandestine. Outside observers note that only highly skilled and experienced hackers tend to use such tactics.[84] The attackers targeted export-controlled information with substantial value to foreign governments and businesses. The OP 2 attacks pose the latent threat that hackers could shut down Pentagon or other government networks should they choose to do so.[85]

According to *Time*, the FBI and other law enforcement agencies were not up to the challenge posed by OP 2. Instead, American cyber vigilantes

got involved. One of them, supposedly with US government knowledge, hacked into Chinese routers to detect and characterize the OP 2 intrusions, gain information as to their origins, and provide a detailed report of stolen information.[86] Subsequently, the Defense Department's Joint Task Force—Global Network Operations also investigated OP 2.[87]

The US government has not openly identified suspects in OP 2. In response to media questions, Chinese government officials call claims that China backs the intrusions "totally groundless, irresponsible, and unworthy of refute." However, China has refused to cooperate with FBI investigation.[88] The *Washington Post* reports one US official as stating, "Is this an orchestrated campaign by [China] or just a bunch of disconnected hackers? We just can't say at this point."[89]

OP 3

In February 1998, Israeli hacker Ehud Tenenbaum and two California teens intruded on unclassified DoD networks.[90] According to media reports, the teens hacked the systems just for fun.[91] Their attacks followed a predictable process. First, the intruders would reconnoiter network systems to determine if a vulnerability existed. Then, if they found one, they would exploit it to gain unauthorized access to the network. Once they had network access, they would emplace a packet sniffer to gather data then return later to download the sniffer-collected data.[92]

Officials initially suspected that the attacks originated in Iraq.[93] Coming during a period of heightened tension in the Persian Gulf and as "the most organized and systematic attack to date" on Pentagon networks, according to then–deputy secretary of defense John Hamre, observers jumped to the conclusion of Iraqi responsibility based on the circumstantial evidence. A team of investigators led by the FBI eventually used technical means to track the attacks, not to Iraq but back to the three teenagers.[94]

Disadvantages of Cyber Deterrence: Lack of Reassurance. Cyber espionage highlights one more problem plaguing cyber deterrence: the lack of reassurance. Presently, few international laws or norms define acceptable and unacceptable behavior in cyberspace,[95] meaning that states cannot rest assured that they will not be targeted by cyber attacks if they refrain from targeting others. The United States may have only recently begun to consider legal restrictions on its cyberspace freedom of action,[96] but laws will help all state actors, including the United States, be assured that certain types of egregious cyber attacks will not occur.[97] The difficulty

in attributing cyber attacks to certain actors may explain why some states choose not to agree to legal restrictions on their Internet behavior. If a state considers it likely that it might be framed in a "false flag" operation, that state has little incentive to forgo attacks (since it will be blamed anyway). The absence of reassurance incentivizes hitting first in cyberspace so states can victimize others before they become victims themselves.

Advantages of Cyber Deterrence: Information Quantity and Interdependence. Cyber spies also face some difficulties. The huge amount of low-quality information in cyberspace bolsters deterrence by denial. Because individuals can generate information with so little expense, "noise" can overcome "signal."[98] To mount effective cyber espionage, spies must know the cyber terrain well. What information is worthwhile, and what is junk? Understanding, reconnoitering, and mapping networks take time; while some reconnaissance can be automated, targeted reconnaissance to steal, corrupt, or destroy the *right* information often takes human reasoning. The quantity of worthless information makes cyber espionage more difficult.

In addition to the volume of information in cyberspace, interdependency might help to deter states from cyber espionage. The nature of cyberspace is connection, and interconnectedness enforces deterrence by interdependency.[99] Part creator, part beneficiary of globalization, cyberspace allows states to "embrace" each other through electronic connections.[100] This interdependency increases the value of accurate information to all actors and increases the harm caused by inaccurate information.[101] As states connect further, the incentives of attack will gradually decrease, and disincentives will increase. This theory resembles those offered by advocates of economic interdependence.[102] Although interdependence will not lead states to ignore their vital interests in favor of economic or information benefits, they will forgo lesser interests if they see the loss of those interests as less valuable than interconnection. The more states pursue the "friendly conquest" of interconnectedness in cyberspace,[103] the more interdependency will deter cyber attacks.

Why Did Cyber Deterrence Fail? Observers cannot really know to what extent attribution difficulties played a role in cyber deterrence breaking down in these cases. Understandably, the US government is very circumspect about how much or how little it knows about cases of cyber espionage, but media reports suggest some very strong leads. In the instance of OP 3, the United States identified its attackers and brought them to justice, demonstrating that thorough and effective investigations are possible in at

least some cases of cyber espionage. Without more evidence, the innuendo surrounding the cases makes attribution seem possible.

Asymmetry did not pose that much of a challenge. In the absence of evidence, one can assume that while states like China and Russia may have less confidential information stored on networked systems than the United States, they probably do generate and store at least some confidential information on networked computer systems. If true, that symmetry makes proportional retaliation possible. For the criminals discovered in the OP 3 case, the Israeli and US governments pursued legal action. Asymmetry thus did not cause the breakdown in cyber deterrence.

More so than anonymity and asymmetry, a lack of reassurance caused deterrence to fail in the OP 1 and OP 2 cyber espionage cases. Although news reports do not mention the possibility, presumably the United States also uses cyberspace to spy. If not, it is high time to start. Although commentators and analysts alike express outrage and frustration when others penetrate sensitive US networks, the US government may be sinning as much as sinned against in cyberspace.

That lack of reassurance keeps the United States from retaliating against cyber spies. Although some columnists seem to suggest that retaliation could keep adversaries from stealing military technology secrets,[104] most retaliatory measures would seem disproportionate to espionage. If the United States demands that other states allow the FBI to investigate intrusions into US cyber networks, it must grant the law enforcement agencies of those states similar access to its own intelligence community.

The scalability of cyber attacks creates further incentives for cyber espionage and might have caused deterrence to break down. The theft of information from confidential networks may be a harbinger of much worse things to come. As the Georgians found out after the 2008 war, hackers may leave hidden code in computer systems that network administrators do not detect until after that code has done its damage. Intrusions onto US networks suggest that hackers could harm or even disable those networks if they were able to retain access to them. Such attacks would lie dormant while states are at peace but could cripple military, intelligence, and command and control networks if activated during times of war. If intrusions involve nuclear command and control networks, cyber espionage becomes an existential threat. "Precisely because [cyber attacks are] counter [command and control] warfare par excellence, the resort to [cyber attacks] almost compels a WMD-armed opponent to strike first and pre-

emptively."[105] Cyber espionage poses a much more serious *potential* threat because hackers could graduate from stealing information to harming the network itself. To deter these types of scalable attacks, states must maintain at least some retaliatory capabilities that are impervious to cyber attack.

The sheer volume of information in cyberspace has the potential to bolster cyber deterrence in the future, but it does not appear to have mattered much in these cases. Certainly, adversaries will face a diminishing return on their cyber espionage investments if the United States can hide its "signal" in the midst of an overwhelming supply of "noise." The United States could, for example, load existing networks with meaningless files and disinformation. Or, the United States could create huge numbers of fake networks with automated, human-simulated packet traffic to deceive cyber spies into wasting time with decoys. Although these strategies seem plausible, states would never reveal whether or not they employ them to avoid compromising their defenses.

Likewise, interdependence seems promising but does not appear to have strengthened deterrence in these cases of cyber espionage. If the United States could convince Russia, China, and other states that they depend equally on the confidentiality of US classified information, interdependence might diminish anticipated gains from spying. Prof. Peter Feaver makes a very strong case for the deterrent effect of information interdependence. Because intelligence operations are often compartmented, Russia, China, and other states risk confusing their own intelligence communities if they alter or corrupt secret information on US networks.[106] OP 1, OP 2, and OP 3 involve only stolen information, so interdependence has had no effect.

Although states should include cyber espionage in their cyber deterrence strategies, cyber espionage deserves distinction from other types of cyber attack. Information security consists of confidentiality, integrity, and availability.[107] Cyber espionage involving only intelligence collection harms confidentiality, but not integrity or availability. And, as scholar and professor Martin Libicki notes, "The law of war rarely recognizes [information collection] as a *casus belli*, and a good case for changing this has yet to be made."[108] So states probably could not justifiably retaliate against other states for cyber attacks involving only the collection of confidential information; however, DDOS attacks or varieties of cyber espionage, such as deception operations that harm the integrity or availability of information, could involve retaliatory measures (depending on their effects). In sum, while cyber deterrence strategies should address cyber espionage,

most forms of cyber espionage deserve separate treatment from more aggressive and harmful types of cyber attack.

The lack of mutually reassuring treaties also keeps states from retaliating against each other. In its simplest form, deterrence is reciprocity: if you do something to me, I will do it back to you, and if you forgo doing something to me, then I will forgo doing that thing back to you. If the United States does cyber spy, it will have a very tough time justifiably retaliating against other states for following its lead.

With retaliation off the table, decision makers may want to seriously consider deterrence strategies for cyber espionage based on futility, interdependence, and counterproductivity. In addition to the futility strategies discussed earlier, the United States might be able to link economic or trade benefits to restraint in cyberspace. As information gains further value, the interconnectedness of the World Wide Web might itself become a benefit the United States could use to its advantage by threatening to take it away. The United States may also have an opportunity to make successful cyber spying strategically counterproductive for other states. The legitimacy of the Chinese government, for example, largely depends on China's economic growth.[109] If cyber spying causes US businesses to purchase fewer Chinese goods or in some other way harms that growth, those effects might deter China from using cyberspace to spy.

Last, OP 3 proves that states need more than context clues to attribute cyber attacks to specific actors. Some theorists argue that investigations need not find a smoking gun because circumstantial evidence is sufficient.[110] OP 3 proves conclusively that this argument does not hold water. Had the United States proceeded with only the available context clues, it would have targeted Iraq without cause. Moreover, OP 3 demonstrates that investigators can positively attribute cyber attacks, at least in some cases, further lessening the rationale for states to shoot first and ask questions afterwards. The United States should investigate all cyber attacks to the fullest extent possible before declaring any suspect guilty.

Implications for a US Cyber Deterrence Strategy

How Difficult is Attribution?

Attribution surely poses difficulties, but the evidence suggests that it is possible in many cases. Under some circumstances, attribution may not even be necessary for deterrence.

OP 3 demonstrates that attribution is not always the impossible challenge that some commentators make it out to be. The United States clearly has the ability to link at least some cyber attacks to their perpetrators. As more and more actors recognize the need to further secure cyberspace, and as identity authentication in cyberspace improves,[111] attribution should gradually become easier.

The 2007 cyber war in Estonia also shows that definite attribution may not be necessary in every case. In some circumstances, third parties may, by shielding the guilty from investigation, make themselves a legitimate target of retaliation. If victim states do begin to assign responsibility to obstructionist third parties, those states or infrastructure providers may be deterred from protecting the culprits. Those culprits, once exposed to investigation and judicial punishment, may themselves be deterred from conducting cyber attacks in the first place.

In instances of cyber attack as a combined arm, attribution may be reasonably inferred regardless of whether private citizens or states conduct attacks. Since these attacks occur in the midst of a physical war, attribution does not pose its typical challenges.

How Much of a Problem is Scalability?

Experts bombard the public with warnings about the "strategic" cyber threat. They describe threats to US digital banking and financial information and networked critical infrastructure. The Department of Homeland Security (DHS) has even run tests to demonstrate how power generators could be remotely damaged by a cyber attack.[112] But do these threats exist outside of our collective imagination?

The attack on Estonia did not represent a strategic cyber threat. The attack did not even force Estonia to return the Bronze Soldier to its original location. Estonia responded effectively and seemed to recover quickly.

The attack on Georgia is somewhat different. Coming as it did alongside a Russian invasion of Georgian territory, this cyber attack did have strategic implications. However, if one disaggregates the effects of the cyber attacks from the physical invasion, that clarity dissipates. Would a cyber attack alone have accomplished Russia's strategic goals without the tanks and soldiers? Probably not.

The thorniest of the cases for cyber deterrence strategists are undoubtedly OP 1, OP 2, and OP 3. Although these instances of cyber espionage have not yet had a strategic effect on our national security, they might in the

future. Foreign states could, for example, penetrate critical US networks during times of peace and then lay dormant, retaining access without drawing the attention of network administrators. Then, if the foreign state and the United States ever entered into conflict, the foreign state could scale those attacks drastically upward to cripple military command and control systems at a decisive moment. Such scalable cyber attacks, coupled with physical attacks, could lead to strategic defeat for the United States. The US government must tailor its cyber deterrence messages—and its retaliatory capabilities—to prevent such a scenario from ever occurring.

Is Defense More Compelling than Retaliation?

The cases do not offer a conclusive answer to this question. Defense, especially futility, seems to have great potential in cyber deterrence strategies, but only time will tell if the defensive strategies that states employ live up to their potential.

Estonia's defensive measures offer reason for hope. At least one subsequent DDOS attack on Estonia since the 2007 case has not yielded any significant success for the attacker.[113] This kind of successful defense deters attackers from similar attacks in the future and leads them to search for new vulnerabilities. The more that defending states prove they can capably handle many varieties of cyber attack, the less attractive the cyber domain will seem as an avenue of attack.

Are Interdependence and Counterproductivety More Compelling than Retaliation?

Perhaps so, but again, the evidence lags behind the theory. In none of the cases did interdependence have a major deterrent effect. Closing the bridge at Narva to commercial traffic demonstrates that Russia does not depend on trade exchanges with Estonia, and its military domination of Georgia suggests a similar imbalance between those two states. Presumably interdependence with the United States has not kept Russia and China from cyber spying, or vice versa.

Interdependence in the cyber world seems to follow rules similar to economic interdependence, a topic addressed more completely by other studies.[114] Suffice it to say, interdependence between great powers and near-peer neighbors may have positive implications for cyber deterrence in the future, but they have not yet played a discernable role in cases of cyber attack.

The same goes for counterproductivity. Concerns that aggressive actions in cyberspace would prove politically counterproductive did not keep Russia from its role in the cyber attacks on Estonia and Georgia (whatever that role may have been). Political "fair play" does not prepossess states like Russia or China in the way that it concerns the United States and our European allies. However, because Russia and China rely on economic strength for domestic political legitimacy, the United States and other countries might find counterproductivity strategies targeting economic growth more effective than strategies focused on international political legitimacy.

Whither Reassurance?

The cases demonstrate that while reassurance might not help, its absence will certainly harm otherwise effective cyber deterrence. A lack of reassurance certainly did not prompt the attack on Estonia, since Western democratic states that strongly value the rule of law (like Estonia) are not likely to execute surreptitious DDOS attacks on other states. Likewise in the Georgia case, reassurance was not at issue. However, the cyber espionage cases show that an otherwise effective cyber deterrence posture requires reassurance. States face an uphill battle trying to deter activities in which they themselves indulge. In view of this, the United States and other countries should seek to reassure others by limiting their own aggressive behaviors in cyberspace. Without reassurance based on international and domestic law, cyber deterrence cannot reliably succeed.

How Important is Escalation Dominance?

The cases show escalation dominance comprises a critical component of cyber deterrence. Without it, Estonia and Georgia could not respond to Russia. If the United States deters strategic cyber attacks in the future, it must maintain strategic escalation dominance. If, in OP 1, OP 2, or other cyber intrusions, the United States fears command and control attacks on its nuclear weapons or other military capabilities, it should clearly indicate how it will respond to and escalate conflict in the instance that its survival appears to be at stake. Without escalation dominance, the United States will be left with no recourse in the aftermath of an attack.

Clearer and More Prevalent Deterrent Messages

US cyber deterrence languishes because other states do not understand what interests are off limits from attack and the consequences they face

for attacking those interests. If the United States considers certain types of intrusions on command and control systems harbingers of strategic attack, the government should indicate how it will overwhelmingly and justifiably respond to such attacks. Because cyber attacks have a broad spectrum of severity, the United States need not open itself up to salami tactics[115] by providing a menu-style list of punishments for various crimes. However, higher-level strategic attacks and threats should have specific and clearly delineated consequences. Last, the United States should create new channels of communication for cyber deterrence messages. While cyber deterrence may not require the level or extent of messaging necessitated by nuclear deterrence in the Cold War, senior leaders are mistaken if they believe a casual statement from time to time to domestic media outlets will suffice to deter foreign states.

Conclusion

While cyberspace does pose unique challenges for deterrence strategists, real-world cases demonstrate that those challenges can be overcome.

The 2007 Estonia case demonstrates that attribution and asymmetry in cyberspace may not be as challenging as many authors argue. Instead, assigned responsibility can alleviate the need for attribution, and asymmetry in the physical domains proves more consequential than cyber asymmetry.

The 2008 Georgia case reinforces the conclusions of the Estonia case. Although Russia might deny a role in the cyber attacks, attribution becomes a moot issue as Russian tanks roll across the Georgian border. Again, geopolitics trumped the difficulties unique to cyber deterrence.

The cases of cyber espionage demonstrate several more key points. First, without reassuring potential adversaries of reciprocal restraint, the United States will continue being the victim of cyber espionage (just as it may victimize other states). Moreover, without offering reassurance, the United States cannot legitimately retaliate against cyber spies—it must instead seek to deter these attacks through strategies of futility, interdependence, and counterproductivity. Although these areas have theoretical promise, the cases show they have not lived up to their potential.

Together, these cases have implications for cyber deterrence strategies. Attribution may be difficult, but it is not impossible. Strategic cyber attacks may not have materialized yet, but cyber deterrence strategies must account for the scalability of surreptitious cyber attacks. While futility,

interdependence, and counterproductivity have promise, they have not yet yielded the desired results. Reassurance is an important and as yet unaccounted for component of a reliable cyber deterrence strategy. Escalation dominance remains a key component of effective deterrence, including cyber deterrence. Even if the United States remains ambiguous about less-dangerous cyber threats, it must be painstakingly clear about what activities it will not tolerate in cyberspace and the consequences of those activities.

The cases and their implications demonstrate that cyber deterrence is challenging, but with a measured and realistic strategy, cyber deterrence can accomplish most of its desired effects. Yogi Berra was right. Despite theorists' predictions, cyber deterrence remains connected to the physical and political worlds and seems tougher in theory than it will turn out to be in practice. SSQ

Notes

1. Although much of the literature conveys this message, some good examples include Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica, CA: RAND, 2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf; Richard Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (Autumn 1996); and Stephen Blank, "Can Information Warfare be Deterred?" in *Information Age Anthology, Volume III: The Information Age Military*, eds. David S. Alberts and Daniel S. Papp (Washington: Command and Control Research Program, 2001), 125–57, http://www.dodccrp.org/files/Alberts_Anthology_III.pdf.

2. "US Eyes N. Korea for 'Massive' Cyber Attacks," *MSNBC.com*, 9 July 2009, http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security; and Jack Goldsmith, "The New Vulnerability," *New Republic* 241, no. 4885 (24 June 2010): 23.

3. Chris Wu, "An Overview of the Research and Development of Information Warfare in China," in *Cyberwar, Netwar, and the Revolution in Military Affairs*, eds. Edward Halpin et al. (New York: Palgrave MacMillan, 2006), 192–93.

4. Austin Long, *Deterrence: From Cold War to Long War* (Santa Monica: RAND, 2008), 5, http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf.

5. Although Cold War–era studies on deterrence are too numerous to count, Thomas Schelling offers a paramount example in *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

6. For example, Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on al-Qaeda* (Santa Monica: RAND, 2002), http://www.rand.org/pubs/monograph_reports/MR1619/MR1619.pdf.

7. In Mark Landler and John Markoff, "Digital Fears Emerge after Data Siege in Estonia," *New York Times*, 29 May 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html, the authors report that many of the attacks on Estonia targeted its banks. In Peeter Lorents, Rain Ottis, and Raul Rikk, "Cyber Society and Cooperative Cyber Defence," a paper presented at the 3rd International Conference on Internationalization, Design, and Global Development, San

Diego, CA (2009), 184, the authors reiterate that cyber attacks on the banking infrastructure of a highly networked society like Estonia's can cause serious economic losses.

8. Shane Harris, "The Cyberwar Plan: It's Not Just a Defense Game; Cyber-Security Includes Attack Plans Too, and the U.S. Has Already Used Some of Them Successfully," *National Journal*, 14 November 2009, http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php.

9. Long, *Deterrence*, 17–22, 59–61, explains this phenomenon at length, as does Libicki, *Cyberdeterrence and Cyberwarfare*, 32–35.

10. James Der Derian, "Cyber-Deterrence," *Wired Magazine* 2.09, September 1994, http://www.wired.com/wired/archive/2.09/cyber.deter_pr.html.

11. Harknett, "Information Warfare and Deterrence."

12. For examples, see Richard Kugler's optimistic chapter, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington: NDU Press, 2009); and Michael Tanji's pessimistic blog, "Deterring a Cyber Attack? Dream On . . . ," *Wired.com Danger Room*, http://www.wired.com/dangerroom/2009/02/deterring-a-cyb/.

13. OP 1, OP 2, and OP 3 are supposed cases of cyber espionage by foreign states against the United States. At the direction of security review authorities of the DoD, the author can neither confirm nor deny the existence of such or similar cases. However, the deputy secretary of defense and other US government officials have openly acknowledged and discussed, in public speeches, articles, and testimony to Congress, cases highly similar to those described by the author. The author has freely drawn from media accounts of similar supposed cases and will address their details as though they did occur. This analysis should not be misinterpreted to lend credence to any unofficial account of a case of cyber espionage against the United States.

14. See, for example, Thomas Skypek, "A Pearl Harbor by Keystroke?" *Washington Times*, 7 May 2009, Op-ed section, http://www.washingtontimes.com/news/2009/may/07/a-pearl-harbor-by-keystroke/; and Skypek, "New Cyber Attacks Showcase Need for Cyber Deterrence Policy," *Hope Is Not a Foreign Policy,* http://www.hopeisnotaforeignpolicy.org/2009/07/08/new-cyber-attacks-showcase-need-for-cyber-deterrence-policy/.

15. K. A. Taipale, "Cyber-deterrence," in *Law, Policy, and Technology: Cyberterrorism, Information Warfare, Digital and Internet Immobilization* (Hershey, PA: IGI Global, forthcoming 2010), 12, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045 #368665.

16. Andrew J. Goodpaster, C. Richard Nelson, and Seymour J. Deitchman, "Deterrence: An Overview," in *Post–Cold War Conflict Deterrence*, ed. Naval Studies Board and National Research Council (Washington: National Academies Press, 1997), 13; Kugler, "Deterrence of Cyber Attacks," 330; and Long, *Deterrence*, 8.

17. Goodpaster et al., "Deterrence," 22–23; Schelling, *Arms and Influence*, 264–74; Kugler, "Deterrence of Cyber Attacks," 326, 332; Long, *Deterrence*, 8; DoD, *Deterrence Operations Joint Operating Concept Version 2.0* (Washington: Defense Technical Information Center, 2006), 42–44, http://www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc; and Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington: NDU Press, 1996), 4, http://permanent.access.gpo.gov/websites/nduedu/www.ndu.edu/inss/books/Books%20-%201996/Information%20Warfare%20 and%20Deterence%20-%20Feb%2096/.

18. Kugler, "Deterrence of Cyber Attacks," 320, 334–35; Long, *Deterrence*, 10; DoD, *Deterrence Operations*, 26; and Taipale, "Cyber-deterrence," 13.

19. Kugler, "Deterrence of Cyber Attacks," 320, 334–35; Long, *Deterrence*, 10; DoD, *Deterrence Operations*, 26; Taipale, "Cyber-deterrence," 13; and Wheatley and Hayes, *Information Warfare and Deterrence*, 4.

20. Goodpaster et al., "Deterrence," 22; Schelling, *Arms and Influence*, 36; Long, *Deterrence*, 11; and Taipale, "Cyber-deterrence," 17–18.

21. Goodpaster et al., "Deterrence," 14; Kugler, "Deterrence of Cyber Attacks," 328; Long, *Deterrence*, 10; and DoD, *Deterrence Operations*, 27–28.

22. Schelling, *Arms and Influence*, 36–43; and Long, *Deterrence*, 7–8.

23. Long, *Deterrence*, 7; and DoD, *Deterrence Operations*, 20–23.

24. Kugler, "Deterrence of Cyber Attacks," 327; and Taipale, "Cyber-deterrence," 36–39.

25. Taipale, "Cyber-deterrence," 39–40; and Peter D. Feaver, "Blowback," *Security Studies* 7, no. 4 (June 1998): 98–111.

26. Wheatley and Hayes, *Information Warfare and Deterrence*, 4.

27. Ibid.; Taipale, "Cyber-deterrence"; and Schelling, *Arms and Influence*, 227–32.

28. For a lengthier and much more detailed and technical discussion of denial of service attacks, see Carnegie Mellon Software Engineering Institute (CERT), "Denial of Service Attacks," http://www.cert.org/tech_tips/denial_of_service.html.

29. Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs* 9, no. 1 (Winter/Spring 2008): 122–23; Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," paper presented at the 8th European Conference on Information Warfare and Security, Lisbon, Portugal, 2009, 178–79; and Landler and Markoff, "Digital Fears Emerge after Data Siege in Estonia."

30. Ottis, "Analysis of the 2007 Cyber Attacks," 177–78; Lorents et al., "Cyber Society and Cooperative Cyber Defense," 183–84; and Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, no. 3 (May/June 2008): 227.

31. Lorents et al., "Cyber Society and Cooperative Cyber Defense," 183.

32. Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, 19 May 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

33. Ibid.

34. Ottis, "Analysis of the 2007 Cyber Attacks,"178; and Libicki, *Cyberdeterrence and Cyberwarfare*, 2–3.

35. Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic."

36. Ottis, "Analysis of the 2007 Cyber Attacks,"179–80.

37. Ibid., 178.

38. Executive Office of the President, *Cyberspace Policy Review* (Washington: GPO, 2009), 33–34, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May–June 2001): 109; Jason Miller, "Administration to Set New Vision for ID Management," *1500 AM Federal News Radio*, 22 September 2009, http://www.federalnewsradio.com/index.php?nid=11-&sid=1768455; Kugler, "Deterrence of Cyber Attacks," 309–10, 317, 337–38; Blank, "Can Information Warfare Be Deterred?" 149; and Roger Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review* (Spring 1998), http://www.iwar.org.uk/iwar/resources/nwc-review/io-spring-1998.htm.

39. Taipale, "Cyber-deterrence," 21–24.

40. Libicki, *Cyberdeterrence and Cyberwarfare*, 75–90.

41. Ibid., 52.

42. Adams, "Virtual Defense," 110; Barnett, "Information Operations, Deterrence, and the Use of Force"; Blank, "Can Information Warfare Be Deterred?" 145; Taipale, "Cyber-deterrence"; and Libicki, *Cyberdeterrence and Cyberwarfare*, 25–26.

43. Taipale, "Cyber-deterrence," 18.

44. Harknett, "Information Warfare and Deterrence"; Timothy Thomas, "Deterring Information Warfare," *Parameters* 26, no. 4 (Winter 1996–1997), http://www.carlisle.army.mil/usawc/Parameters/96winter/thomas.htm; Kugler, "Deterrence of Cyber Attacks," 315; Taipale, "Cyber-deterrence," 7–8, 25; and Kevin R. Beeker, "Strategic Deterrence in Cyberspace: Practical Application" (MSc thesis, Air Force Institute of Technology, June 2009), 10–11, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502250&Location=U2&doc=GetTRDoc.pdf.

45. Thomas, "Deterring Information Warfare"; Taipale, "Cyber-deterrence," 33–36; and Eneken Tikk, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm, and Liis Vihul, *Cyber Attacks against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008), 29–31, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

46. Bryce Meyer, "Defending the New Silk Road," *Armed Forces Journal* 146, no. 2 (September 2009): 12–16, 34–35.

47. The "cyber Silk Road" model of shared responsibility does not envision punishing Internet infrastructure providers for attacks they neither authorized nor participated in. Instead, the model envisions offering infrastructure providers incentives to cooperate with cyber attack investigations to criminally prosecute or otherwise carry out punitive measures against cyber attack perpetrators. However, if infrastructure providers refuse to provide investigative assistance, they put themselves at risk of obstructing justice and suffering legal consequences.

48. Tikk et al., *Cyber Attacks against Georgia*, 22.

49. For those interested, in "Web War I," Stephen Blank offers a passionate argument that Russia bears the guilt, and Martin Libicki offers a counterargument in *Cyberdeterrence and Cyberwarfare*, 2–3. Kugler, "Deterrence of Cyber Attacks," 318–20, makes an argument for convicting states with only circumstantial evidence, but that policy would increase the incentive for third parties to mount "false flag" operations.

50. Ottis, "Analysis of the 2007 Cyber Attacks," 179.

51. Economic sanctions provide one example. An even more severe course of action might involve physically destroying Russian profit-yielding infrastructures (e.g., oil and natural gas pipelines) in ways that would not threaten Russian lives. Of course, the latter reaction raises the peril of further retaliatory escalation by Russia, potentially even to full-scale war.

52. Jim Michaels, "NATO to Study Defense against Cyberattacks," *USA Today*, 15 June 2007, http://www.usatodayeducate.com/wordpress/?dl_id=9.

53. Travis Wentworth, "You've Got Malice: Russian Nationalists Waged a Cyber War against Georgia. Fighting Back Is Virtually Impossible," *Newsweek*, 23 August 2008, http://www.newsweek.com/id/154965.

54. David Fulghum, "Cyberwar is Official," *Aviation Week & Space Technology* 171, no. 10 (14 September 2009).

55. George Donovan, "Russian Operational Art in the Russo-Georgian War of 2008," (MSc thesis, US Army War College, March 2009), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500627&Location=U2&doc=GetTRDoc.pdf.

56. Wentworth, "You've Got Malice."

57. STRATFOR, "Georgia, Russia: The Cyberwarfare Angle," *STRATFOR.com*, 12 August 2008.

58. Fulghum, "Cyberwar is Official."

59. Ibid.

60. Sergey Samoylov and Yekaterina Yeliseyeva, "War: Hackers Attacked Our Media," *Moskovskiy Komsomolets* (Moscow), 12 August 2008.

61. Wentworth, "You've Got Malice."

62. STRATFOR, "Georgia, Russia."

63. Libicki, *Cyberdeterrence and Cyberwarfare*, 2, fn. 5.

64. Wentworth, "You've Got Malice."

65. Fulghum, "Cyberwar is Official."

66. Taipale, "Cyber-deterrence," 19.

67. Kugler, "Deterrence of Cyber Attacks," 338; Blank, "Can Information Warfare Be Deterred?" 139; John P. Callaghan and Rudi Kauffman, "Building Cyber-Security," paper presented at the 66th Annual Meeting of the Midwest Political Science Association, April 2008, 9–11, http://ubiwar .files.wordpress.com/2009/09/2008_callaghan_kauffman_building_cybersecurity_prospects_for _deterrence1.pdf; and Libicki, *Cyberdeterrence and Cyberwarfare*, 65–68.

68. Blank, "Can Information Warfare Be Deterred?" 143; Taipale, "Cyber-deterrence," 20–21; and Beeker, "Strategic Deterrence in Cyberspace," 12.

69. A "bot net" is a network of computers surreptitiously controlled by another central computer, or "bot net master." A computer that is part of a bot net can be exploited for access to the user's personal information or as a platform for attacking other computers or networks. "Packet sniffing" is observing the traffic of data packets across a network to find and exploit packets that contain valuable data. Network reconnaissance can involve a wide variety of activities such as scanning ports on a router, identifying network IP addresses, or collecting network usage information.

70. Taipale, "Cyber-deterrence," 24.

71. Barnett, "Information Operations, Deterrence, and the Use of Force"; Wheatley and Hayes, *Information Warfare and Deterrence*, 13; Taipale, "Cyber-deterrence," 36–38; Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 84–85; and Dorothy Denning, *Information Warfare and Security* (Boston: Addison Wesley, 1999), 384–85.

72. Libicki, *Cyberdeterrence and Cyberwarfare*, 16–18; and Libicki, *Conquest in Cyberspace*, 31–37.

73. Fulghum, "Air Defense Mystery in Georgia," *Ares: A Defense Technology Blog*, http:// www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogscr ipt&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3A27ec4a53 -dcc8-42d0-bd3a-01329aef79a7Post%3A54d4 da21-e359-4da4-b03b-44a98562a8af.

74. Fulghum, "Cyberwar is Official."

75. Robert Farley, "But What Does It Mean for NATO?" *American Prospect*, 15 August 2008, http://www.prospect.org/cs/articles?article=but_what_does _it_mean_for_nato.

76 Vernon Loeb, "NSA Adviser Says Cyber-Assaults On Pentagon Persist with Few Clues," *Washington Post*, 7 May 2001; and Adams, "Virtual Defense," 99.

77. Adams, "Virtual Defense," 100.

78. Loeb, "NSA Adviser Says Cyber-Assaults on Pentagon Persist with Few Clues."

79. Adams, "Virtual Defense," 100.

80. Loeb, "NSA Adviser Says Cyber-Assaults on Pentagon Persist with Few Clues."

81. Adams, "Virtual Defense," 99–100.

82. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *Time Magazine*, 29 August 2005, http://www.time. com/time/magazine/ article/0,9171,1098961,00.html.

83. Bradley Graham, "Hackers Attack via Chinese Websites: US Agencies' Networks are among Targets," *Washington Post*, 25 August 2005, http://www.washingtonpost.com/wp-dyn/ content/article/2005/08/24/AR2005082402318.html.

84. Thornburgh, "The Invasion of the Chinese Cyberspies."

85. Ibid.

86. Ibid.

87. Graham, "Hackers Attack via Chinese Websites."

88. Ibid.

89. Ibid.

90. "[REDACTED]," *GlobalSecurity.org*, http://www.globalsecurity.org/military/ops/[REDACTED].htm.

91. Kevin Poulsen, "Video: [REDACTED], the Best FBI-Produced Hacker Flick Ever," *Wired Online Threat Level*, 23 September 2008, http://www.wired.com/threatlevel/2008/09/video-[REDACTED]/.

92. "[REDACTED]."

93. Poulsen, "Video."

94. Kevin Poulsen, "[REDACTED] Hacker 'Analyzer' Escapes Jail, Community Service for Terrifying US Army," *SecurityFocus.com*, 15 June 2001, http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_ analyzer_escapes/.

95. Adams, "Virtual Defense," 103–4; Thomas, "Deterring Information Warfare"; and Beeker, "Strategic Deterrence in Cyberspace," 11.

96. Siobhan Gorman, "US Backs Talks on Cyber Warfare," *Wall Street Journal*, 4 June 2010, http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html?mod=WSJ_Tech_LEFTTopNews.

97. Scott W. Beidleman, "Defining and Deterring Cyber War" (MSc thesis, US Army War College, June 2009), 19–20, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500795&Location=U2&doc=GetTRDoc.pdf.

98. Libicki, *Conquest in Cyberspace*, 50–71.

99. Harknett, "Information Warfare and Deterrence"; and Thomas, "Deterring Information Warfare."

100. Executive Office of the President, *Cyberspace Policy Review*, 34; and Wheatley and Hayes, *Information Warfare and Deterrence*, 13.

101. Blank, "Can Information Warfare Be Deterred?" 136; Feaver, "Blowback," 98–111; and Taipale, "Cyber-deterrence," 39–40.

102. See, for example, Dale C. Copeland, "Economic Interdependence and War: A Theory of Trade Expectations," *International Security* 20, no. 4 (Spring 1996): 5–41; and Susan M. McMillan, "Interdependence and Conflict," *Mershon International Studies Review* 41, no. 1 (May 1997): 33–58.

103. Libicki, *Conquest in Cyberspace*, 126, 220–22.

104. Skypek, "A Pearl Harbor by Keystroke?"

105. Blank, "Can Information Warfare Be Deterred?" 142.

106. Feaver, "Blowback."

107. Denning, *Information Warfare and Security*, 41.

108. Libicki, *Cyberdeterrence and Cyberwarfare*, 23–24.

109. Minxin Pei, "Will the Chinese Communist Party Survive the Crisis?" *Foreign Affairs*, 12 March 2009, http://www.foreignaffairs.com/articles/64862/ minxin-pei/will-the-chinese-communist-party-survive-the-crisis?page=show.

110. See, for example, Kugler, "Deterrence of Cyber Attacks," 318–20.

111. Ben Bain, "Authentication Said Key to Cybersecurity," *Federal Computer Week*, 22 September 2009, http://www.fcw.com/articles/2009/09/22/web-mcconnell-cybersecurity.aspx.

112. Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN*, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

113. Robert McMillan, "Another Estonia Cyberattack," *PC World*, 16 January 2008, http://www.pcworld.com/article/141438/another_estonia_cyberattack.html.

114. Blank, "Can Information Warfare Be Deterred?" 136; Feaver, "Blowback," 98–111; and Taipale, "Cyber-deterrence," 39–40.

115. Schelling, Arms and Influence, 66–68. Schelling describes "salami tactics" as follows:

> Tell a child not to go in the water and he'll sit on the bank and submerge his bare feet; he is not yet 'in' the water. Acquiesce, and he'll stand up; no more of him is in the water than before. Think it over, and he'll start wading, not going any deeper; take a moment to decide whether this is different and he'll go a little deeper . . . pretty soon we are calling to him not to swim out of sight, wondering whatever happened to all our discipline . . . this [is] the low-level incident or probe, and tactics of erosion. One tests the seriousness of a commitment by probing it in a noncommittal way, pretending the trespass was inadvertent or unauthorized if one meets resistance, both to forestall the reaction and to avoid backing down." The enemy slices the "salami" of a deterrence declaration, "if there is no sharp qualitative division between a minor transgression and a major affront, but a continuous gradation of activity, one can begin his intrusion on a scale too small to provoke a reaction, and increase it by imperceptible degrees, never quite presenting a sudden, dramatic challenge that would invoke the committed response.

The European Union and the Comprehensive Civil-Military Approach in Euro-Atlantic Security

Matching Reality to Rhetoric

Darrell Driver, Major, USA

When the European Security and Defense Policy (ESDP)[1] was founded just over a decade ago, it was to be one of the crown jewels in the European Union's emergence as a new, soft civilian-superpower. The ESDP was erected on the premise that the future security environment will be defined less by traditional, state-centric military threats and much more by a wide range of diverse challenges that are transnational, multifaceted, and especially complex in nature,[2] and that such complex challenges will require the comprehensive integration of a range of civilian and military capabilities. This so-called comprehensive approach would mean that future success would depend not just on a state's ability to wield military power but its ability to employ and leverage state and nonstate civilian power as well, including "the political, security, development, rule of law, human rights, and humanitarian dimensions of international missions."[3] On this front, the EU was determined to become a leading force. According to former EU high representative for the common foreign and security policy, Javier Solana, "The comprehensive approach underpinning ESDP is its value added. The logic underpinning ESDP—its distinctive civil-military approach to crisis management—was ahead of its time when conceived."[4]

Nevertheless, 10 years into this effort, progress has failed to live up to expectations. The civil-military integration hoped for at the outset has been plagued by an ESDP institutional design that has served to separate and isolate the military and civilian aspects rather than integrate them.

MAJ Darrell Driver is a Council on Foreign Relations International Affairs Fellow with the Center for Transatlantic Relations at Johns Hopkins' Paul H. Nitze School of Advanced International Studies (SAIS). He is a strategic plans and policy officer who has served as both a planner and a faculty member at the George C. Marshall European Center for Security Studies and a social science faculty member at the US Military Academy, West Point. He holds a PhD in political science from Syracuse University.

Moreover, the vision of building the ESDP into a vehicle for EU civilian power has been plagued by chronic civilian capacity shortfalls, both in the planning and control structures of the ESDP itself and in the ability to deploy civilian experts in an operational capacity. Most problematic, however, is that rather than seize the opportunity to forge the ESDP as an integrative transatlantic and, indeed, global leader in civilian aspects of security, it has maintained a primarily insular focus on iterative institutional reforms and a series of small-step, functionally circumscribed security missions. This has severely limited the potential of a value-added relationship with the North Atlantic Treaty Organization (NATO) and has served as an obstacle to effective US–European cooperative capacity-building efforts. The insular focus has persisted despite an ESDP founding concept defined by a smart-power strategy involving complimentary development in diplomacy, defense, and comprehensive approaches to operational challenges like crisis prevention, stability, and reconstruction. These concepts are now broadly embraced on both sides of the Atlantic, and ESDP founders very early recognized and acted on the importance of such holistic integration of security capabilities. If, however, in its second decade the ESDP is to fulfill the EU's hope of becoming a more significant force for security and stability in the world, the EU must move beyond the insular focus on institutional design that has defined its first decade. It must grow to partner and take more of a leadership role in this vital area. With the Lisbon Treaty and recent ESDP institutional reforms providing important new powers of unity and coherence across the EU Common Foreign and Security Policy (CFSP) domains, there is no time like the present.

The Comprehensive Approach and the European Union—A Slow Start to a Big Idea

Of all Western attempts to forge a more comprehensive approach to security challenges, the EU's efforts to build integrated civilian and military capabilities under the European Security and Defense Policy held for many the greatest early promise. Unlike existing state and multilateral security structures, the EU was not burdened with preexisting security institutions, departments, and agencies requiring negotiation to bring them into closer cooperation. The ESDP was to be uniquely constructed and resourced from its inception to provide the civilian and military integration

necessary for smart-power strategy and comprehensive approaches to operations. Despite these aspirations, however, ESDP progress toward truly integrated security functions, planned by an integrated staff and carried out by integrated executers on the ground, has been slow to develop. Indeed, even as an organization billed as the embodiment of comprehensive approach operations, the ESDP has struggled through repeated reforms to achieve more coherence and cooperation across its civilian and military domains and continues to suffer from capacity shortfalls in a variety of key functional areas.

The European Security and Defense Policy was first announced in 1998 at the British-French summit in St. Malo, France, and formerly confirmed in June 1999 as a central feature of the EU's Common Foreign and Security Policy. The initial announcement at a bilateral summit between Europe's two most important military powers was no mistake. From the beginning, the ESDP would be defined by political contestation and compromise between Britain's desire to see it focus on the building and projection of civilian crisis-management capacities, thereby avoiding the duplication of NATO's traditional defense responsibilities, and France's desire for it to develop a separate and autonomous military capacity capable of carrying out independent combat operations. This schizophrenia of purpose meant that not one but two ESDPs were consummated at St. Malo. The first ESDP was to be the civilian power, whereby, according to Javier Solana, the EU would be uniquely suited to "use its longstanding experience and considerable resources on the non-military aspects of crisis management;"[5] the second ESDP, the military power, established for the first time an independent European military force. The result of these dual births and the member state political motives behind them can be seen most clearly in the burgeoning planning, command, and control structures within the ESDP headquarters and, especially, the near-constant attempts at their reform.

At the Nice European Council meeting of 2000, the EU began the process of establishing political and military bodies that would provide the ESDP its structural makeup. Chief among these structures would be the Political Security Committee (PSC), which would have the job of ensuring "synergy between the civilian and military aspects of crisis management."[6] Below the PSC, a European Union Military Committee (EUMC) and a supporting European Union Military Staff (EUMS) were established to provide military planning, command, and control. Remaining in its

own directorate and responsible for providing planning and control functions for the civilian side would be the Committee for Civilian Aspects of Crisis Management (CIVCOM). These bodies would form the organs of the comprehensive approach design, but despite the stated importance of coherence and synergy between the civilian and military aspects of the ESDP, it would soon become apparent that this design would face several basic challenges. First, there was no integration of civilian and military aspects below the political PSC level. This practically guaranteed incoherence and disunity as an institutional inheritance. Second, and equally as important as the divisions, was the comparative disparity in resources between the two elements. While the EUMC was composed of very experienced senior military officers, the CIVCOM was largely comprised of junior diplomats, and while the EUMC was supported by a military staff of approximately 140 officers, the CIVCOM had no independent staff.[7]

This disparity in capacity between the civilian and military staff structures persisted despite a number of attempted reforms. A civilian mission-support section of 20 officials was added in 2003 to improve support for the EU Police Mission in Bosnia and Herzegovina. Also in 2003, the UK, Italy, and the Netherlands, on the one hand, and France, Germany, Belgium, and Luxembourg, on the other, brokered a compromise on the long-standing issue of whether the ESDP should be equipped with a permanent operational command headquarters. Finding it duplicative of NATO capabilities, the British, among others, were opposed but compromised and allowed for the establishment of a civilian-military operations cell within the EUMS. To stress its distinctiveness as an EU structure, the cell was billed as a civilian-military integrative mechanism. The reality is it was a substitute for a full operational headquarters capacity, and its addition to the Military Staff meant that it was quickly dominated by the military with little connection to the remainder of the civilian staff in the Council Secretariat.[8]

From the beginning, then, efforts to constitute an ESDP planning, command, and control structure up to the comprehensive-approach task have been plagued by an inability to achieve effective staff integration and adequate resourcing of the civilian component. There are a number of reasons for these shortfalls, but paramount was the disagreement in purpose between the two primary European military powers. The French continued to resist any effort to merge civilian and military staffing functions for fear of this diluting traditional military effectiveness. The British

continued to champion a more integrated civilian-military capability as a needed complement to the traditional defense role of NATO. In the end, the ESDP headquarters structure has been the Janus–faced progeny of both visions, finding it difficult to fully succeed on either account.

As the ESDP has been plagued by its internal civilian-military divisions, the broader effort to forge a vehicle for more comprehensive and integrated security approaches has been characterized by intragovernmental divisions that have served as models of bureaucratic infighting and turf competition. The most important of these divisions sprang from the decision to institutionally separate responsibility for development assistance into two entirely different branches of EU government. Development that was focused on short-term intervention and crisis management was located inside the Council Secretariat with the ESDP, albeit in a different directorate. The lion's share of the EU development budget, however, would be focused on long-term assistance and be made the purview of the EU Commission (the EU's executive arm). While this institutional division was meant to ensure that development assistance would maintain a sustained focus and not be instrumentalized for short-term security purposes, the distinction was far from clear and was not accompanied by coordinating mechanisms adequate to ensure the two efforts were complementary.

This less-than-clear bifurcation of development authority has posed an ongoing challenge for ESDP operations. In a recent review of Europe's role in nation-building activities over the last several decades, James Dobbins and his co-authors speculate that this division of developmental assistance authority between the Council and the Commission is one likely reason the EU has lagged behind the United States in the provision of development aid in long-term support of stability and reconstruction missions.[9] It is a shortfall that has emerged in operations from the Balkans to the Congo, and it persists despite Europe's position as the world's leading overall contributor of official development assistance.[10]

A third important challenge to the realization of the ESDP as a comprehensive-approach instrument has been a continued inability to achieve its goals for deployable civilian capacity and accurately anticipate the expanded range of civilian expert requirements. At the 2000 Feira, Portugal, European Council meeting, four civilian capacity areas of police, rule of law, civilian administration, and civil protection were established as organizing areas for a comparable civilian capacity to the military side of the ESDP. Goals for this capacity were set for each area in what would

become Civilian Headline Goal 2008. Though there was much excitement over the subsequent rapidity by which member states would commit to meeting the goals, actually getting member states to fulfill these pledges of expert support has proven more difficult. The Civilian Headline Goal 2008 identified significant potential shortfalls in critical areas like police and rule-of-law functions.[11] These were areas that had been a central focus of capacity-building efforts but where deployable capacity regularly fell behind demand in a burgeoning EU mission set. There has proven to be a major difference between having a list of potential civilian experts capable of deploying in ESDP missions and actually deploying these individuals. Every judge or police officer deployed with the ESDP detracts from local governance capacity within member states. By 2009, reports on the status of civilian capacity building in critical areas had become even less sanguine. According to the European Council on Foreign Relations, the EU posted a 1,500-person total shortfall in 12 ongoing 2009 missions. The report singled out Spain as the most egregious overall example of pledge breaking, deploying only 2.8 percent of its total Civilian Headline Goal obligation.[12] Launched in June 2007, the European Police training mission in Afghanistan was scheduled to include 400 police officers from around the EU. Due to member-state abdications, however, the mission has habitually fallen around 130 officers short of that goal.

A related problem has been in identifying and building capacity within a wide range of expert areas not initially considered. As indicated previously, this includes the need for a cadre of civilian crisis-management planners to balance military planning capacity within the ESDP headquarters. It also, however, includes deployable experts in a wide range of security sector reform areas, including key functions like democratic oversight of the security sector and transparent financial management. Areas like these are necessary to build long-term security sector sustainability and effective democratic oversight and were only belatedly recognized as necessary expertise in efforts like security sector reform.[13]

Finally, the structural and capacity problems that have challenged efforts to build a comprehensive approach within the European Union have been mirrored in the circumscribed nature of ESDP operations to date. Since 2002, the ESDP has taken on 19 separate operations. These missions include the European Union Police Mission in Bosnia (2003), Military Operation in Bosnia–Herzegovina (2004), Border Assistance Mission to Moldova and Ukraine (2005), Integrated Rule of Law Mission for Iraq

(2005), Police Mission to Afghanistan (2007), and the Rule of Law Mission in Kosovo (2008), among others.[14] Of significance in these missions is the decidedly narrowly defined nature of each. Far from engaging in holistic, comprehensive integration of the ESDP's four civilian capacity areas with that of the military, ESDP operations generally follow the same pattern of separation and distinction that characterize its organizational structure. Much of this has, of course, been by design, as the EU has been careful to limit the scope of its missions as a means of ensuring some early successes and building ESDP momentum. Nevertheless, one area where limiting mission scope has proven difficult is in security sector reform (SSR), an area in which a 2009 EU Commission report concluded that

> despite an EU SSR policy which defines the security sector in a broad manner and which endorses a holistic approach to SSR, in practice EU SSR support to a partner country tends to concentrate only on one or two individual parts of the security sector—mainly either defence, police, justice, or border management . . . linkages between the different parts of the security sector are mostly neglected.[15]

Thus, though the ESDP was born of a vision to more effectively integrate a broad range of civilian and military expertise, efforts to effectively operationalize that vision in the field have been slow to develop.[16]

New Reforms and New Hopes—A Decade of Institution Building Comes to an Active End

Despite these difficult beginnings and ongoing capacity problems, there has, nevertheless, been increasing optimism that a recent series of reforms will serve to punctuate the ESDP's first decade of existence and bring better parity and integration to EU comprehensive-approach efforts. The first such significant reform came in 2007 with the creation of the Civilian Planning and Conduct Capability (CPCC). For the first time, the disparate and inadequate command and control structures that were to underpin civilian operations within the ESDP would be unified and bolstered in the same way the EUMC and the EUMS had done for the military component. This emerging resource and staffing parity was followed by integrative reforms in December 2008, when High Representative Solana gained approval for his plan to establish "a new, single civilian-military planning structure for ESDP operations and missions."[17] What was named the Crisis Management and Planning Directorate (CMPD) would merge the separate civilian and military directorates under a single

civilian head with a military deputy. The CMPD is to be located under the Directorate General for External and Political-Military Affairs in the Council Secretariat and, in its composition, is intended to bring together a diverse range of capabilities and administrative cultures with the mission to plan, prepare, and execute ESDP operations in a more holistic and integrated manner. Finally, the most far reaching of these decade-closing reforms has been ushered in with the final approval of the EU's long-in-coming Lisbon Treaty. Among many other things, the Lisbon Treaty amended the practice of six-month rotation of the Council presidency among member states by establishing a sitting president of the European Council. More importantly, perhaps, Lisbon consolidated foreign policy responsibility between the Council Secretariat and the EU Commission in the form of a more unified high representative for common foreign and security policy, complete with an external action service (EAS) to give the new office a foreign-service capacity that had not previously existed.[18] Though plans to combine development and diplomatic direction within the EAS and create a strong link back to the ESDP are still forthcoming, the unification of foreign and security policy under a single high representative should at least help to smooth some of the earlier disjunctures. The question going forward, however, is the degree to which these hard-fought reforms can be translated and implemented into a more tangible comprehensive approach. The test of this answer is to be found more in the nature of the EU's external relationships than in continued internal line and block reforms.

The EU and the US—The Need for an Expanded Comprehensive-Approach Partnership

Even as the EU has muddled through its decade-long coming of age for the comprehensive approach ideal, on the other side of the Atlantic, the United States has proven to be a zealous convert to the integrative security and holistic approach teachings. Signaling the potential of a new American way of war, US chairman of the Joint Chiefs of Staff, ADM Michael Mullen, has made it a central point of emphasis that "defense and diplomacy are no longer discrete choices . . . but must complement one another throughout the messy process of international relations."[19] The question remains, to what degree can such converging concepts and efforts regarding civilian power and civilian-military integration find

expression in transatlantic cooperation. It is an area with much potential for a US–EU strategic partnership, if a series of persistent stumbling blocks can be overcome.

Ten years ago, while policymakers in the European Union were talking about the importance of civilian aspects of crisis management, the United States was focused on concepts like a revolution in military affairs and rapid decisive operations, perfecting a system of war that relied on technological superiority and rapid targeting to quickly overwhelm enemy systems. The dominant question was not whether the United States could realize such a vision but, rather, whether its closest European allies would be able to keep up or, given apparent divergence in threat perception, whether many of those same allies even thought it worth the try.[20] Observers wondered aloud if either this divergence spelled the useful end of much of the transatlantic security partnership or if, at best, there might be some room for a looser cooperation through combat versus constabulary functional specialization.[21] Nevertheless, one of the most important occurrences in the Euro-American security relationship in the last 10 years is the growing US realization that the early European focus on civilian power concepts and comprehensive security ideas has, in many important respects, proven prescient. In Iraq and Afghanistan, the US security establishment has come to appreciate the absolute central role that issues like societal and human security, development, rule of law, and good governance play in achieving successful stability and reconstruction. In strategic threat assessments, too, once divergent US and EU views of future global challenges have begun to converge around similar concerns. Issues like increasing attention to the prospect of a growing global multipolarity, on the one hand, and challenges like climate change, migration, resource scarcity, and nontraditional transnational threats, on the other, were first prioritized in EU security documents but have recently received focused attention on the western side of the Atlantic as well.[22] Though technological disparities have persisted as a concern on defense matters, the US security establishment has come to appreciate the many ways in which future security will be impacted by a variety of factors outside the traditional realm of defense and the corresponding importance of building capacity in areas from development to diplomacy to deal with these challenges. Though the EU proclaimed itself an early leader in this area, the benefit of first mover alone will not be enough. New multilateral and collective

concepts will be required to capitalize on the transatlantic attention these ideas have received.

NATO: Necessary but Not Sufficient

NATO's central role has been to guarantee the transatlantic space against existential threat, undergirding the stability of a zone of trade and economic exchange that forms the foundation of the global economy.[23] If NATO does nothing but provide for territorial defense in this space alone, it has contributed immeasurably to North American and European member state interests. Nevertheless, absent reliable comprehensive approach alternatives, the last decade has seen NATO grow into an organization that has operated increasingly out of area, both in terms of its military functional and European geographical responsibilities. In stability and reconstruction operations from the Balkans to Afghanistan, NATO has responded to complex crisis management and counterinsurgency demands with force structures that were organized and maintained for traditional defense missions. The question, going forward, for NATO has been whether these kinds of missions will be institutionalized with the level and breadth of civilian capacity required to improve effectiveness in these areas. The answer almost assuredly will be no.

At the early insistence of Denmark and facing a growing, complex insurgency in Afghanistan, the alliance endorsed the concept of the comprehensive approach at the Riga Summit of 2006. It took the following 18 months ahead of the Bucharest Summit of 2008 to agree on an action plan for developing and implementing NATO's contribution to comprehensive-approach operations, the subsequent policy details of which were assigned to a newly formed comprehensive task force within NATO Headquarters. Since Bucharest, however, translating conceptual agreement on the importance of comprehensive approach has proven exceptionally difficult. In fact, the effort to expand the potential scope of NATO operations into the broader areas of security-related activity have been plagued by a number of inveterate obstacles, any one of which is likely to prevent the defense alliance from playing anything more than a military support role to more comprehensive operations. The most important of these challenges has been the simple existence of the ESDP. As previously discussed, the EU had already set about defining its niche in security affairs in terms of a unique mixture of civilian and military strategic and operational capacity required for comprehensive-approach

operations. With 21 of the 26 NATO members also member states in the EU,[24] there has been scant desire to risk functional competition between the two organizations by building a similar civil-military capacity in each. The point could not have been made more precisely in a recent EU Institute for Security Studies report on the future of the ESDP in which the authors were keen to stress NATO's role as "a military alliance and not a crisis management organisation."[25] Second, in addition to alliance apprehension over nondefense functional expansion, there is also mounting concern regarding NATO's role in out-of-Europe operations.[26] This latter point has been a central feature of ongoing negotiations over a new NATO strategic concept. The concern is that out-of-area operations have served to dilute and confuse NATO's central role as a Euro-Atlantic guarantor against existential threats.[27] Since this is its chief value for European parliaments and publics, there is sensitivity against risking further NATO popular support by employing the alliance in anything other than core mission areas. In light of the 2008 conflict between Georgia and the Russian Federation and more recent Russian military exercises in Belarus, Eastern European NATO allies have been particularly keen to see NATO affirm its territorial defense role more emphatically.

The result of these trends is the likely inability of NATO to develop significant civilian-power capacity. Instead, the alliance will continue to define its role as providing defense support to comprehensive-approach efforts. This circumscription of the alliance to a supporting role presents Europeans and Americans with two choices: leave transatlantic cooperation in the increasingly important nondefense security field to bilateral relationships, or forge a new EU–US partnership framework on comprehensive security approaches. As will be argued in the subsequent section, it is in the interest of both the EU and the United States to seek the latter arrangement.

The Comprehensive Approach—New Avenues for US–EU Partnering

The EU no longer has a monopoly on smart-power appreciation and comprehensive-approach aspirations. Indeed, six years after observers faulted US military operational efforts in Iraq as severely limited by an unhealthy separation between military and civilian domains of action,[28] the larger US interagency planners appear capable of talking about little else than the importance of civil-military and civil-civil integration in comprehensive security approaches. At the tactical and operational levels, the provincial reconstruction team (PRT) model and new Army and Marine

Corps doctrines have emphasized the centrality of concepts like good governance, economic development, and rule of law in stabilization and counterinsurgency activities. At the strategic level, the 2005 DoD Directive 3000.05 instructed the US military to treat stability and reconstruction operations on equal priority with combat operations, and National Security Presidential Directive 44 established the secretary of state, through the newly formed office of the coordinator for reconstruction and stabilization (S/CRS), as the lead entity for integrating US government efforts in the stability and reconstruction domain. Indeed, the quest for more effective interagency operations has become what one recent report described as the "weather issue," for its ubiquity in US national security discussion and debate.[29] Thus, as the EU absorbs its latest round of reforms for forging more effective civilian-military security integration, the United States finds itself in the midst of its own comprehensive-approach renaissance.

Despite this convergence of vision on both sides of the Atlantic and a 60-year history of deep security cooperation, there has been precious little effort to expand cooperation in this area. In light of the recent embrace of comprehensive-approach principles in the United States, the likely position of NATO as a support player rather than a comprehensive-approach leader, and the near completion of a decade of EU institutional redesign and refinement, there is an important opportunity for a strategic framework between the United States and the EU on comprehensive-approach cooperation.

A number of areas exist where such a relationship might quickly prove beneficial on both sides of the Atlantic. First, for Europe moving forward from the Lisbon Treaty, expectations for a more coherent leadership role for EU foreign policy have been high. Nevertheless, the selection of relatively unknown politicians for the Lisbon-created posts of a permanent president and a newly empowered high representative for foreign and security policy have done little to satisfy anticipation that Europe might finally be capable of matching its global economic might with a leading foreign and security policy voice.[30] Moving to formalize and expand transatlantic comprehensive-approach cooperation would provide an opportunity for visible European foreign and security policy leadership at a pivotal time. Second, EU–US strategic partnering in this area could serve to ease pressure on the NATO alliance regarding the proper location of these broader aspects in the transatlantic security architecture. This would avoid the unwanted EU prospect of comprehensive-approach cooperation

becoming a bilateral matter between the United States and individual EU member states. Third, the ability to forge a closer security relationship directly between the EU and NATO has consistently been blocked by alliance member Turkey in an attempt to extract concessions from the EU on both Turkish membership and a satisfactory resolution to the Cyprus dispute. A closer EU–US comprehensive-approach relationship would help circumvent this inveterate obstacle to closer NATO–EU security cooperation, allowing the United States to be a more effective interlocutor between the defense role of NATO and the comprehensive capabilities of the EU–US partnership.

Finally, though the EU has proclaimed itself a global leader in comprehensive security approaches, it has, nevertheless, resisted efforts to view development and diplomacy primarily through a security lens.[31] This cautious perspective on foreign policy writ large has been at the heart of EU self-concepts regarding its global identity as the world's first "normative power." By contrast, the United States, though working to dampen these perceptions, has been plagued by criticisms that it is overly military-centric in its security and foreign policy.[32] Much of this military-centric focus, however, has been influenced by the prevailing security environments in Iraq and Afghanistan. As the United States emerges from these two conflicts, there will be an expanding need to think about the application of comprehensive security solutions in light of a foreign and security policy not dominated by the immediacy of ongoing stability and support missions. Issues like crisis response and, especially, crisis prevention will become increasingly important. By acting to forge a strategic partnership now, the EU has an opportunity to play an influential role in this debate. In sum, Europe has default strategic connection with the United States in a broad security domain that far exceeds the need for traditional defense capabilities.[33] It is not in the EU's interest for the only security relationship between Europe and the United States to remain in the circumscribed area of traditional defense. Both the United States and the EU increasingly recognize that future threats will require more expansive and holistic solutions.

The United States, similarly, should welcome the prospect of EU partnership and, at times, leadership in this area as having great potential to improve comprehensive approach legitimacy and future civilian capacity. First, the current US administration has been keen to find visible global partners to deal with a growing list of current and future security challenges.

With the EU viewing itself as a comprehensive-approach leader, a bilateral Euro-Atlantic partnership could encourage the EU to take a more active role in operationalizing this vision. Second, for reasons of legitimacy, future crisis management and prevention missions should not be defined by unilateral US involvement. Indeed, successful crisis management and prevention missions, from humanitarian and peacekeeping to stabilization and reconstruction, require a level of international, host nation, and even donor country domestic legitimacy that is difficult, if not impossible, to achieve through unilateral effort.

Finally, though the United States has made important progress in the establishment of civilian operational capacity, including increased budgets for development and diplomacy and the ongoing establishment of a 4,200-person Civilian Response Corps.[34] The scale and scope of demand in areas like rule of law, agriculture, governance, and economic development is likely to outstrip the United States' ability alone to respond to all but the most limited of contingencies without again leaning heavily on its military. Despite the above mentioned civilian capacity problems, EU member states provide approximately €60 billion per year in official development assistance (ODA); approximately €12 billion of this is managed by the European Commission. The EU's humanitarian assistance budget is approximately €937 million, and its operational European Security and Defense Policy budget is €250 million.[35] In addition, the ESDP maintains a roster of over 10,000 deployable experts in the primary areas of civilian crisis-management expertise. Chief among these has been a variety of civilian expert areas where the United States, for reasons of national experience, has no capacity at all.[36] This includes, for instance, the EU's ability to draw on gendarmerie forces, like the Italian Carabinieri and the European Gendarmerie Force (EGF), as well as the EU member states' experience and capacity in interior ministry–based rule of law and justice functions—a structural similarity shared with most developing states but an area in which the US federal and state governments operate quite differently.[37] The United States would greatly benefit from an EU partner in these areas, but these are relationships that must be established and cultivated before the call to crisis occurs.

In this vein are a number of areas where the advantages of EU–US strategic partnering are quickly apparent. The supporting elements of doctrine and concepts, education and leadership, and training and planning will need further development as these integrative civilian capacities

mature and the comprehensive approach assumes a more coherent role in ordering security thinking and responses. Most of these areas received attention in the 2007 joint EU–US work plan on crisis management; however, with the exception of a data sharing agreement, little effort has been made to act on the plan.[38] Nevertheless, the above mentioned trends offer an important new window of opportunity for EU–US cooperation across a range of issues.

The most important area in which collaborative effort has the potential to sustain long-term commensurability and cooperation is in the development of an intellectual foundation for comprehensive-approach strategies and operations, especially the need for a common comprehensive approach definition and concept.[39] This is something that has long been required in the transatlantic community but, as previously discussed, has been hampered within NATO by disagreement over its role in other-than-defense-related activities. The US Institute of Peace (USIP) recently released its *Guiding Principles for Stabilization and Reconstruction*;[40] USIP and EU planners should seize the opportunity to create such a document for the Euro-Atlantic space.

A common document of this sort would provide the intellectual foundation required for a shared system of transatlantic education and training in the comprehensive approach domain. The EU has the potential to become a much needed global leader and US partner in civilian education for comprehensive security approaches, including courses and programs from the tactical-functional to the ministerial-strategic levels. For instance, the German government supports, through an implementing nonprofit partner, the provision of a course in development diplomacy which has been heralded as a model for the kind of educational opportunities required for future US diplomats.[41] The EU might seek to replicate programs of this nature. In fact, one recent document went so far as to recommend the establishment of a US–EU school for conflict prevention, conflict management, and postconflict stabilization that would serve to further a common understanding and approach to comprehensive operations.[42] In short, with a common conceptual foundation come numerous opportunities for Euro-Atlantic burden sharing in the critical task of building the intellectual capacity for comprehensive approaches to security challenges.

In the area of training and planning, too, the end of a decade of ESDP institutional fluctuation offers hope of useful cooperation and collaboration. Planner exchanges, for instance, have proven to be critical means

of strengthening professional development, communication, cooperation, and understanding within the framework of alliance military operations. The EU's ongoing establishment of the Crisis Management Planning Directorate provides an excellent opportunity for US interagency planners to participate in an organization going through the early struggles of integrating civilian and military crisis prevention and response planning. Such an experience would be useful for US planners, who would return to take part in the Civilian Response Corps' continued maturation. Perhaps no proposal has been more ambitious in this area than that offered in February 2008 by US ambassador to NATO, Victoria Nuland, who argued, "If we truly believe in a transatlantic comprehensive approach to security—one that combines the best of our soft and hard power—we need a place where we can plan and train for such missions as a NATO–EU family."[43] Given the obstacles to establishing such a NATO–EU fusion cell in the near future, an initial step to address the current dearth of transatlantic planning capacity in the area of comprehensive civilian-military operations could be to begin with a bilateral US–EU arrangement.[44] Operational exchanges and integration also provide the opportunity to offer mutual personnel assistance while bolstering individual professional development. In this area, there are already some modest examples of US–EU operational cooperation, including the US Customs and Border Protection's participation in the EU Commission's Customs and Fiscal Assistance Office (CAFAO) program in Bosnia and the US participation in the EU Rule of Law Mission (EULEX) in Kosovo, which included the agreement to provide up to 80 police officers and eight judges and prosecutors.[45]

Of course, the first place the United States would like to see enhanced cooperation in civilian-power operational participation is in Afghanistan. Assuming a significant civilian-power role in Afghanistan would provide a single-stroke opportunity to affirm the maturation of the EU comprehensive-approach vision. Nevertheless, there are a number of other areas where attention has not been as focused but where EU forethought and action could prove similarly important. One need only review the range of failed state indexes to identify some leading suspects. Somalia, for instance, has habitually topped even Afghanistan as the leading failed state in the world. So, too, there is increasing concern about the stability of Yemen, a nation with great potential as a terrorist-harboring, ungoverned space but also with great potential as a demonstration case for EU crisis-prevention leadership. In a world with a strong EU–US crisis management

relationship, these are the kinds of discussions of forethought that would occur before the ad hoc pleas of assistance once again emerge to dominate the discourse.

Conclusion

It has been said that US expectations of the EU are at once too high and too low.[46] On the issue of the comprehensive approach in particular, this is a fitting statement for the great partnership potential the EU represents as compared to the abiding American incredulity that this potential will be realized. Europe was correct in its early emphasis on the expansiveness and complexity of future security challenges and the need to look beyond defense to more comprehensive solutions to these problems. This vision was, indeed, as Javier Solana contended, "before its time." Yet, as a result of the events of the past decade, the EU is no longer a lone convert to the comprehensive approach faith. The question from the newly converted is rightfully: now what? With the tidal waters of institutional formation and redesign receding on a more settled EU institutional landscape, there is an important opportunity for the EU to fully embrace its stated role as a global civilian power partner and leader. The world and the United States, in particular, would be most wise to welcome this coming of age. SSQ

Notes

1. European Security and Defense Policy is referred to as Common Security and Defense Policy (CSDP) with the Lisbon Treaty. However, since *ESDP* was the term employed for much of the history discussed here, the term is retained for use in this article.

2. Nicole Gnesotto and Giovanni Grevi, *The New Global Puzzle: What World for the EU in 2025?* (Paris: European Union Institute for Security Studies, 2006).

3. Rintatoski and Autti point out that there is no universally shared definition on comprehensive approach; however, it is generally accepted that it includes these dimensions. Kristiina Rintakoski and Mikko Autti, eds., *Comprehensive Approach Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management, Crisis Management Initiative* (Helsinki: Finland Ministry of Defence, 2009), 9.

4. As described here by Javier Solana, the terms *comprehensive approach* and *civil-military cooperation* will be used interchangeably throughout the article to refer to this general integrated security effort. Javier Solana, "Remarks by the EU High Representative for the Common Foreign and Security Policy," in *ESDP@10: What Lessons for the Future?* (Brussels: EU Institute for Security Studies, 2009), 7.

5. Daniel Plesch and Jack Seymour, *A Conflict Prevention Service for the European Union* (London: British American Security Information Council, 2000), 15.

6. "Presidency Report on the European Security and Defence Policy," in *Presidency Conclusions of the Nice European Council (7–9 December 2000)*, annex VI, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/en/ec/00400-r1.%20ann.en0.htm.

7. The Swedish presidency in 2001 did add a police unit to the Council Secretariat to provide planning expertise on police missions. However, this unit was not assigned to support CIVCOM but was instead placed in a separate directorate; also, it came with only eight officers. For more on this, see Carmen Gebhard, *The Crisis Management Planning Directorate: Recalibrating ESDP Planning and Conduct*, vol. 7, no. 4 (Vienna: Institute for Advanced Studies, 2009).

8. Decision making within the EU resides in three primary and distinct institutions. The Parliament is elected by and represents the citizens of the EU; the Council of the EU represents the member states; and the European Commission is the executive arm, representing the EU itself. For more on these distinctions, see "EUROPA—European Union Institutions and Other Bodies," http://europa.eu/institutions/index_en.htm.

9. James Dobbins et al., *Europe's Role in Nation-Building: From the Balkans to the Congo* (Santa Monica, CA: RAND, 2008), xxix.

10. *Euromapping 2009* (Brussels: German Foundation for World Population and European Parliamentary Forum, 2009), 19, http://www.euroresources.org/euromapping.

11. *Final Report on the Civilian Headline Goal 2008* (Brussels: Ministerial Civilian Capabilities Improvement Conference of EU, 2007), 14807/07.

12. Daniel Korski and Richard Gowan, *Can the EU Rebuild Failing States? A Review of Europe's Civilian Capacities* (London: European Council on Foreign Relations, 2009), 14.

13. Maria Derks and Sylvie More, *The European Union and Internal Challenges for Effectively Supporting Security Sector Reform* (Clingendael, Netherlands: Conflict Research Unit, Clingendael Security and Conflict Programme, Netherlands Institute for International Relations, 2009), vi.

14. Stéphane Pfister, "La Gestion Civile Des Crises: Un Outil Politico-Stratégique Au Service De L'union Européenne" ["Civil Crises Management: A Political Strategy Tool of the European Union"] (PhD diss., University of Geneva, 2008).

15. Derks and More, *European Union and Internal Challenges*, v–vi.

16. One recent report went so far as to claim that "the truth is that most EU missions are small, lacking in ambition and often strategically irrelevant." Korski and Gowan, *Can the EU Rebuild Failing States?* 22.

17. *Presidency Conclusions of the Brussels European Council (11–12 December 2008)*, doc. 17271/1/08, http://register.consilium.europa.eu/pdf/en/08/st17/st17271-re01.en08.pdf.

18. Antonio Missiroli, *The Impact of the Lisbon Treaty on ESDP* (Brussels: Directorate General Policy Department External Policies, European Union, 2008).

19. Greg Jaffe, "Joint Chiefs Chairman Mullen Outlines a more Restrained Art of War," *Washington Post*, 5 March 2010.

20. Collectively, the European Union states have ranked second behind the United States in total military expenditures per year. However, the real difference in these expenditures is quite significant. Moreover, many European militaries were finding it difficult to reform beyond their manpower-intensive, territorial defense–focused past, making the actual disparity in technological sophistication even greater than spending alone indicates. Bastian Giegerich, "European Positions and American Responses: ESDP–NATO Compatibility," in *European Foreign Policy in an Evolving International System: The Road toward Convergence*, eds. Nicola Casarini and Costanza Musu (New York: Palgrave Macmillan, 2007).

21. John Hillen, "Superpowers don't do Windows," *Orbis* 41, issue 2 (1997).

22. *Global Trends 2025: A Transformed World* (Washington: National Intelligence Council, 2008); and Giovanni Grevi, "Scanning the Future: American and European Perspectives," EU Institute for Security Studies policy brief, 2008.

23. Trade and investment between the United States and Europe alone is worth $3.75 trillion in total commercial sales each year and leads to the employment of 14 million people on both sides of the Atlantic. Daniel Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2009: Annual Survey of Jobs, Trade, and Investment between the United States and Europe* (Washington: Center for Transatlantic Relations, 2009).

24. These dual-member countries include Belgium, Bulgaria, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and the United Kingdom.

25. Álvaro de Vasconcelos, ed., *What Ambitions for European Defence in 2020?* 2d ed. (Paris: European Union Institute for Security Studies, 2009), 19.

26. Peter Viggo Jakobsen, *NATO's Comprehensive Approach to Crisis Response Operations: A Work in Slow Progress* (Copenhagen: Danish Institute for International Studies, 2008), 15.

27. Daniel Hamilton et al., *Alliance Reborn: An Atlantic Compact for the 21st Century* (Washington: Center for Transatlantic Relations, 2009), 21.

28. See, for instance, Robert Egnell, "Explaining US and British Performance in Complex Expeditionary Operations: The Civil-Military Dimension," *Journal of Strategic Studies* 29, no. 6 (2006).

29. Christopher Lamb et al., "National Security Reform and the Security Environment," in *Global Strategic Assessment: America's Security Role in a Changing World* (Washington: National Defense University Press, 2009), 412.

30. Selected by member state vote on 19 November 2009, the compromise for first president of the European Council was Belgian prime minister Herman Van Rompuy, and the high representative for foreign and security policy chosen was little-known European trade commissioner Catherine Ashton.

31. Vasconcelos, ed., *What Ambitions for European Defence in 2020?* 14.

32. See, for instance, Ann Scott Tyson, "Gates Warns of Militarized Foreign Policy," *Washington Post*, 16 July 2008; and "Defining the Military's Role toward Foreign Policy," in *Senate Foreign Relations Committee* (Washington: Government Printing Office, 2008).

33. For more on this argument, see Vasconcelos, ed., *What Ambitions for European Defence in 2020?* 19. Also, Daniel Hamilton and Frances G. Burwell, *Shoulder to Shoulder: Forging a Strategic US–EU Partnership* (Washington: Center for Transatlantic Relations, 2009).

34. *Introduction to the Civilian Response Corps* (Washington: Office of the Coordinator for Reconstruction and Stabilization, 2009), http://www.crs.state.gov/index.cfm?fuseaction=public.display&shortcut=4QR; and B. Nora Bensahel, Olga Oliker, and Heather Peterson, *Improving Capacity for Stabilization and Reconstruction Operations* (Arlington, VA: RAND, 2009).

35. For more on these figures, see Benia Ferrero-Waldner and Louis Michel, *Annuel Rapport sur les Politiques Communautaires en Matiere de Developpement et D'Aide Exterieure et sur leur Mise en Oeuvre en 2008* (Brussels: Commission Europeenne Office de Cooperation EuropeAid, 2009); Julia Streets et al., *Improving Humanitarian Assistance: A Transatlantic Agenda for Action* (Washington: Center for Transatlantic Relations and Global Public Policy Institute, 2009), 13; and Hamilton and Burwell, *Shoulder to Shoulder*, 42.

36. Robert M. Perito, *The Interior Ministry's Role in Security Sector Reform* (Washington: US Institute of Peace, 2009), 13.

37. For a discussion of EU advantages in these areas, see Hamilton and Burwell, *Shoulder to Shoulder*, 42.

38. This work plan followed the April 2007 EU–US Washington Summit assessment on crisis management and included pledges to improve cooperation in capacity building, analysis, and response and the coordination of crisis prevention and response activities.

39. See, for instance, Julian Lindley-French, *Enhancing Stabilization and Reconstruction Operations: A Report of the Global Dialogue between the European Union and the United States* (Washington: Center for Strategic and International Studies, 2009), viii. Also see Rintakoski and Autti, eds., *Comprehensive Approach Trends*, 30.

40. *Guiding Principles for Stabilization and Reconstruction* (Washington: US Institute of Peace and US Army Peacekeeping and Stability Operations Institute, 2009).

41. The statement regarding the Inwent (Internationale Weiterbildung und Entwicklung gGmbh) course being a model educational opportunity for US diplomats was provided by Dr. Anne Marie Slaughter, US State Department director of policy and planning, "Speaking Event at the Center for American Progress," Washington, DC, 16 November 2009.

42. Hamilton and Burwell, *Shoulder to Shoulder*, 49.

43. Victoria Nuland, "US Ambassador to NATO Victoria Nuland's Speech in Paris: Ambassador Discusses Strengthening Global Security for Europe," (speech to Press Club and US Chamber of Commerce, Paris, 22 February 2008), http://www.america.gov/st/texttrans-english/2008/February/20080222183349eaifas0.5647394.html.

44. Hamilton and Burwell, *Shoulder to Shoulder*, 47.

45. "Assistant Secretary Fried Welcomes US Participation in EULEX Kosovo Mission," US Mission to the European Union, 2008, http://useu.usmission.gov.

46. Statement delivered by the former foreign minister of Hungary, Janos Martonyi, speaking at Paul H. Nitze School of Advanced International Studies, Washington, DC, 3 December 2009.

Book Review Essay

James D. Kiras

Toward a Grand Strategy against Terrorism edited by Christopher C. Harmon, Andrew N. Pratt, and Sebastian Gorka. McGraw-Hill, 2010, 448 pp., $82.81.

Textbooks are designed to serve a number of purposes and users. For the professional educator, they should offer convenience in that a course can be logically and readily built around the materials included. A good textbook should fill an identified gap in the market and serve as both anchor and departure point for a course. As an anchor, such works should introduce students to core concepts and ideas.

Textbooks can serve other unintended purposes. They can act as mirrors, reflecting the prevailing social norms or political currents. They can also chart how policies or academic understanding of a subject change over time. This is especially the case with the American and Western European understanding of terrorism since 11 September 2001. The title of one of the first textbooks to appear after the attack, *Terrorism and Counterterrorism: Understanding the New Security Environment*, reflects a society and policy community confronting what it perceived as a paradigm shift to national security.[1] This textbook was spearheaded by the staff at West Point's nascent Combating Terrorism Center and contained an eclectic mix of classic articles and book excerpts on various aspects of terrorism (by such notable experts as Bruce Hoffman, Martha Crenshaw, Mark Juergensmeyer, Magnus Ranstorp, and Walter Reich, among others) as well as cutting-edge conference papers, reports, and original research chapters. These were quickly followed by textbooks on defeating terrorism,[2] terrorist groups and law enforcement responses,[3] the relatively undefined but emerging growth industry of "homeland security,"[4] and one of the capabilities which could potentially make "new" terrorism so devastating: weapons of mass destruction.[5] A subsequent revised edition of *Terrorism and Counterterrorism* reflected how policy and academic thinking on new terrorism has evolved, including chapters on al-Qaeda, suicide terrorism, cyber terrorism, genomic terrorism, civil liberties, and the linkages between terrorism and organized crime.[6] A more recent textbook offering relegates terrorism to one of a number of phenomena that share similar characteristics but are better described under the rubric of "armed groups."[7]

Another form of textbook related to terrorism is more pragmatic in nature—the functional manual. These are not designed to educate but rather to provide the necessary information to train those who must detect or respond to terrorism. There are two main purposes for such works—inform or scare. The best provide useful information on a panoply of subjects written in the plain, unambiguous

---

Dr. James D. Kiras is an assistant professor at the School of Advanced Air and Space Studies, Air University, Maxwell AFB, Alabama.

language of the operator. Many restrict themselves to descriptions of groups, weapons, and behaviors to aid in the identification of terrorists.[8] Still others are handbooks for first responders to aid in securing areas and establishing procedures to save lives and preserve evidence useful in identifying and potentially convicting terrorists. Other functional manuals look beyond information and procedures to provide prescriptions in the form of unchanging laws or rule-of-thumb principles.[9] Such information is useful in dispelling some of the fear generated by terrorism, particularly fear associated with the unknown.

At the other end of the spectrum, some functional textbooks detail worst-case scenarios and offer questionable tips and guidance on how to survive the most destructive terrorist attacks. Consider the following advice from one such book: "If you are 10 miles within (*sic*) a nuclear attack, shelter in a basement or inner room for a day or two with a radio."[10] As terrorism analyst emeritus Brian Jenkins insightfully observed, America is "uniquely susceptible to nuclear terror" given our cultural "obsession with decline and doom" reinforced by popular culture in the form of fiction, television programs, movies, government messages of fear (including the ambiguous terrorist threat-level warning system), and the news media, which create a particularly acute sense of collective anxiety. Jenkins concludes, however, with a calm and sober assessment that nuclear terrorism is a "long-shot possibility" and, therefore, we must not allow ourselves to be ruled by our fears and give in to the doomsday fantasies perpetuated by manuals devoted to preparedness.[11]

The latest addition to this crowded field is another offering from textbook giant McGraw-Hill: *Toward a Grand Strategy against Terrorism.* This volume shares one thing in common with its predecessor, *Terrorism and Counterterrorism*—both textbooks are affiliated with counterterrorism (CT) programs at Department of Defense (DoD) institutions. *Toward a Grand Strategy against Terrorism,* however, did not have its genesis on the banks of the Hudson or Potomac rivers but rather in Europe at the George C. Marshall European Center for Security Studies in Garmisch, Germany.

Unsurprisingly, *Toward a Grand Strategy against Terrorism* is roughly organized along the same lines as the Marshall Center's terrorism curriculum. This offers a number of advantages as well as constraints. The textbook is divided into four units of study: the problem [of terrorism] and its history; law, force, and the military option; instruments of national power; and case studies on or related to terrorism. Much like other textbooks, each unit of study is subdivided into chapters on related subjects, and most will be discussed in detail below. The first unit discusses the problem and its history and features three chapters. The first chapter is on the evolution of terrorism from its past through to its future. The second looks at how and why terrorist groups either succeeded or failed in the twentieth century. The last chapter in this unit, on cooperation against terrorism, looks at international and interagency methods as the solution to the problem. The discerning reader will divine that the first two chapters fit well thematically with the unit of study, while the third seems out of place—it discusses a solution to the problem rather than the problem and history of terrorism per se. The second unit on law, force,

and the military option features four chapters, while the third unit features eight on subjects ranging from diplomacy to managing crises. The last unit on case studies contains five chapters. This imbalance in the number of chapters is an observation rather than a criticism, as some subjects within terrorism are more complex, or have a less-developed literature base, and require deeper and broader coverage. This observation, however, is a symptom of the underlying problem with most edited volumes, including *Toward a Grand Strategy against Terrorism*—the lack of a perceivable unifying theme and vision for the work and firm editorial control to knit the chapter threads and sections together. For a scholarly edited volume, this is the rule rather than the exception, as many of the articles are on esoteric topics. For a textbook designed to appeal to a broader audience, and in particular undergraduate or graduate-level courses of study outside of the Marshall Center, a lack of unity can become problematic.

The reason for this trenchant general critique is that *Toward a Grand Strategy against Terrorism* is not the only textbook which takes a wider policy- and security-oriented view of terrorism. In 2004 Georgetown University Press published a textbook edited by Audrey Kurth Cronin and James Ludes with the muscular title *Attacking Terrorism: Elements of a Grand Strategy*, which is still in print. Cronin and Ludes compiled chapters by leading scholars such as David Rapoport, Martha Crenshaw, Timothy Hoyt, Adam Roberts, and Carnes Lord and policymakers and former counterterrorism officials such as Lindsay Clutterbuck, Paul Pillar, Michael Sheehan, and Daniel Gouré on subjects ranging from sources of terrorism and the issues raised by strategy and grand strategy through discussions of the various policy instruments that could be applied against it. The quality of each essay is very strong, but two features make *Attacking Terrorism* work as a textbook: a firm yet indistinguishable editorial hand and a succinct introduction that explains the overarching logic of the chapters and the unifying theme and a conclusion that weaves the chapter themes together into a discussion of the subject of the book—grand strategy. For better or worse *Toward a Grand Strategy against Terrorism* and its component chapters will inevitably be compared in some manner with its competitor volume. The good news is, *Attacking Terrorism*, despite its advantages, has two problems of its own. First it is in need of updating to stay contemporary and relevant. Second it does not contain many of the features increasingly demanded by publishers, educators, and students such as short case studies or explanatory text boxes and graphics as well as additional online resources such as detailed case studies, questions for discussion, and visual aids.

Toward a Grand Strategy against Terrorism is significantly different from *Attacking Terrorism* in that its primary audience is not the policymaker or the general student but rather the counterterrorism practitioner. It is strongest when it speaks to its audiences on their terms. For the CT operative, this is best done in a direct and unequivocal manner. The fundamental approach is ultimately pragmatic and functional, as opposed to philosophical and academic. There is little room for the broader, and in some cases self-indulgent, questions that vex the study of terrorism, such as the pejorative and subjective nature of the term or discussions of the

root causes and underlying motivations (save for a grudging two-page homily), among others. One example is the implicit question contained in the statement "one man's terrorist is another man's freedom fighter." Rather than let students grapple with this question and provide them with fodder to reach an answer, as in a civilian academic institution, Nick Pratt runs directly over it when he says, "Although fashionable at conferences and cocktail parties, this expression serves at best as a weak lecture transition sentence or merely an empty witticism between neophytes. Murderers of young children are never 'freedom fighters'."[12] *Toward a Grand Strategy against Terrorism,* as a whole, is not concerned with the primary strategist's questions of "why," "who," and "when," but instead cuts at those of greatest concern to the operator: "what" and "how."

Nowhere are the needs of the operator more directly addressed than in James Q. Roberts' chapter, "Building a National Counterterrorism Capability." Roberts is principal director, Special Operations Capabilities, in the Pentagon and has served in uniform in special forces and in a number of senior government counterterrorism positions. He quickly zeroes in on the focus of his chapter, which is the "benchmark for a competent counterterrorism capability."[13] This benchmark is the ability to conduct a successful hostage rescue operation. Roberts makes the argument that competence is reached when there is an alignment between the three components of what he labels as an "Iron Triangle" of CT decision making. These components are: a "hammer," or specialized rescue forces; the "eyes," specialized intelligence and investigative components that establish the conditions for rescue success; and the "brains," the national political leadership. For each of these components, Roberts goes into their specific functional requirements. In the case of rescue forces, these include specialized selection, training, and equipment; necessary skills; and rotation rates, among others.[14]

The strengths of Roberts' chapter lie in his ability to convey his knowledge and experience in a forthright manner to CT operators. In particular, his central message is that counterterrorism success is not just a function of individual or unit skill but also rests on the quality of the intelligence and investigative apparatus and the education and wisdom of the political authority. He concludes with advice on how to build a governmental CT team and when and why it should meet. In Roberts' own words, he is seeking to provide "a 'cookbook' for operators, intelligence personnel, negotiators, and policymakers."[15]

Those looking for practical advice, lessons learned, basic principles, and other "cookbook" elements will not be disappointed with *Toward a Grand Strategy against Terrorism.* While some of the recipes in this textbook are short on descriptions of the required ingredients—such as Roberts', which would have benefited from examples and illustrations—other chapters provide these in considerable detail. For example, Christopher Harmon's chapter, "Illustrations of Discrete Uses of Force," also focuses on hostage rescues, which he labels as "the most challenging and intriguing of all forcible counterterrorist actions."[16] After a brief introduction and discussion of a number of such rescues—including "Dragon Rouge" in the Congo (1964), the "Entebbe Raid" in Uganda (1976), Mogadishu in Somalia

(1977), De Punt in the Netherlands (1977), and the Lima Embassy siege and rescue (1996–1997)—Harmon treads some of the same ground as Roberts on the importance of intelligence and offers a number of principles for the use of force in counterterrorism.[17]

Other chapters provide other sensible fodder for the practitioner. The chapter on "Intelligence and Counterterrorism" provides "Tools of the Trade" and "Lessons Learned and Signposts for the Future."[18] The next chapter, "Following the Terrorist Money Trail," outlines terrorist financing methods, strategies to combat terrorist financing, and the steps and elements required to allow nations to combat terrorist financing on their own or in conjunction with the United States or the international community.[19] The chapter on cyber terrorism does not provide advice but rather advocates steps that countries must take to operate more effectively in the virtual realm. The section on cyber CT—divided into discussions of particular technical, legal, structural, rehearsal, global/strategic, and offensive issues—is written in terms that call to mind an action or decision memorandum. Seventeen paragraphs begin with action or decision verbs that range from the useful ("Maximize Use of Reporting Software to Benefit Law Enforcement") to the commonsense and insipid ("Ensure Use of Security Software" and "Adequately Fund Cyber CT Efforts").[20]

Despite its no-nonsense, matter-of-fact approach, *Toward a Grand Strategy against Terrorism* does contain a number of constructive departure points and scholarly chapters, which make it useful for more academic environments. Despite its rather gruff approach (in addition to the example quoted above, consider his use of the term *wacko-perp*) and occasional offhand conclusions, Andrew Pratt's chapter methodically walks through a thought-provoking list of seven examples that question "was this an act of terrorism or some other form of violent activity?"[21] This is perhaps more important than Pratt realizes. To this day, some Americans, including serving officers (in the author's experience), equate the attack of 11 September 2001 and the atomic bombing of Hiroshima on 6 August 1945 as acts of terrorism.

Christopher Harmon's chapter, "How Terrorist Groups End," is remarkable for its clarity, breadth, and utility. Harmon manages in 42 pages to provide a handy overview of terrorism in the twentieth century; a framework for analyzing terrorist groups' successes, failures, and longevity; and numerous points for classroom discussion. In his chapter, "Ideas Matter," Patrick Sookhdeo offers one of the most cogent explanations of the ideology and worldview of Islam that is informative, nuanced, and accessible. Most troublesome for Western, and in particular American readers, is his conclusion that "the war against the ideology that drives al-Qaeda and similar radical Islamist jihadi groups is of necessity a long and many-sided one. The search for quick fixes, for easy methods, for compromise and appeasement serves only to strengthen the extremists."[22]

Despite its functional focus, Celina Realuyo provides the exemplary textbook chapter. She introduces core concepts, makes the complicated seem accessible and even simple, provides examples and graphics to assist students in understanding

ideas, and walks the reader through a case study which, in turn, utilizes the organizational framework of the chapter. Particularly noteworthy is her attention to detail; for example, the graphic she provides on page 213, compiled from numerous sources, makes the nebulous *hawala* financial system almost immediately understandable. Also noteworthy is Tom Wilhelm's chapter on the security architecture of Pakistan's tribal belt. Like Sookhdeo's chapter, Wilhelm provides a wealth of information not only on the security forces in Pakistan's troublesome frontier region but also their context—history, legacy, organization, and cultural customs and codes. All of the aforementioned chapters, and a number of others in *Toward a Grand Strategy against Terrorism,* delve into subjects not covered in *Attacking Terrorism*.

Other chapters in *Toward a Grand Strategy against Terrorism* are ambitious in scope or nature but ultimately not as successful. A few, unfortunately, are in the section with the greatest potential value for educators—the case studies. The study on the German approach to effective multilateralism seems out of step with most of the rest of the volume. Whereas many chapters are written for and in some cases by (former) operators, this case study is written in academic language for other academics. In addition, the sober judgment of author Rolf Roloff throughout his chapter gives way to an oddly misplaced and wildly optimistic assessment of the counterterrorism progress made by the G-8 nations. Another case study deals with the intriguing question of how France has built its specific judicial and security system to counter terrorism. This system, which includes new laws, special judges, and extended detention powers, has proven remarkably successful, as this chapter suggests. One element curiously missing is a detailed discussion of the role played by paramilitary (*gendarmerie*) forces in France's security system, and in particular, the division of labor and issues related to the use of the *Gendarmerie nationale,* the *Police nationale*, and the French Armed Forces (*Armées françaises*). France in particular has relied on a hybrid of military and police forces as part of its CT successes. Two questions remain unanswered: (1) Are such forces necessary for CT success, or are they unique products of France's specific national context and the groups it has faced? And (2) are they still useful against modern terrorists, or are they anachronisms? More references and tighter linkages between some of the case studies and Harmon's chapter on how terrorist groups end might have answered these questions. A more troubling aspect of Jean-Paul Raffenne and Jean-Francois Clair's chapter is the clarity and style of the authors' prose. At times it is difficult to read: "Other than this, no specifically adapted legislation existed after 1981, while this type of terrorism was growing in effect, with the number of indiscriminate attacks and organizations implicated in acts of violence multiplying on our soil."[23] Here the editors and the publisher of this textbook must bear the responsibility. These examples point to a lack of consistency in style, format, and expression throughout the text. Another example illustrates this point: the term used to describe the current wave of terrorist violence in different chapters often appears to be a reflection of the author's personal preference. How should one label the current wave of global political violence we face? Is it "hyper-terrorism" (Gorka),

"Salafi-Jihadist" terrorism (Pratt), plain "jihadist terrorism" (Wither), "Islamist terrorism" (Sookhdeo), or "a global Salafist insurgency" (Cavoli)?

The difference in opinion over what to label global political violence is not a flaw unique to *Toward a Grand Strategy against Terrorism* but is instead symptomatic of a larger malady. This malady is significant disagreement, within policy-making circles and between allied nations, over the threat that global terrorism poses. At one end of the spectrum, represented most clearly by Sebastian Gorka in his chapter, "International Cooperation as a Tool in Counterterrorism," is the notion that hyper-terrorism is a threat so different, diverse, and potentially damaging from previous terrorism that sweeping changes are required for organizations, forces, and processes. He concludes that "the only viable option is to radically reform our nation state–level instruments to make them more applicable to the new tasks at hand."[24] Boaz Ganor, in the "Afterword," echoes Gorka's clarion call: "The threat is so great, that the international community must stop simply *managing* it, and start really *preventing* and defeating it—which requires agencies around the world, from diverse fields and disciplines, to unite their efforts, combine forces, and formulate a new strategy to combat terrorism."[25] Under the rubric of what US Special Operations Command has termed a "Global Counterterrorism Network" (GCTN), counterinsurgency campaigns, including those in Afghanistan and Pakistan's tribal belt, are related theaters of action in a broader global struggle as three of the chapters (by Christopher Cavoli, Michael Fenzal, and Tom Wilhelm) suggest. Diplomacy is not merely a tool, but as the subtitle of the chapter "Toward a Grand Strategy against Terrorism" suggests, it is "The First Weapon against Terrorism."

Within a number of countries in Europe, where the Marshall Center is based, this vision and the sweeping changes it demands are not only a source of unease but also prove a difficult sell. Many of the European case studies in *Toward a Grand Strategy against Terrorism* discuss the strides made domestically against terrorism since 11 September 2001 but are more subdued on the subject of international, multilateral, and coalition efforts. National preferences; historical, cultural, and legal legacies; and the success of law enforcement efforts lead to significant differences in opinion over the type of action to take. Evidence from Europe suggests that the leaders of some states remain wary of subscribing to the "long war" vision, which is prevalent in American CT circles, and the changes it demands. Senior political and military leaders in Germany have continued to refer to their operations in support of the International Security Assistance Force in Afghanistan as "peacekeeping," as opposed to "counterinsurgency" (much less "counterterrorism") operations. Christopher Harmon puts into words this fundamentally different European perception: "Perhaps no democratic society can afford to be endlessly in a state of war, without becoming a thing ugly to itself, or a marvel of an unwanted archetype—what Sparta was among the ancient Greeks. For the same reason, a democratic society cannot enslave its citizens to a system of pervasive intrusion and intelligence gathering, citizen against citizen."[26]

Despite its modest flaws, such as unevenness in the length and quality of and supplementary educational material within the chapters, *Toward a Grand Strategy*

against Terrorism is a welcome addition to the textbooks on terrorism. As mentioned above, this work is considerably different in scope and scale from *Attacking Terrorism*, despite some inevitable overlap, and many of its chapters provide contemporary perspectives and examples. Unlike the first wave of textbooks after 11 September 2001, which relied heavily on reprinted material, *Toward a Grand Strategy against Terrorism* consists entirely of original chapters. The pragmatic focus and functional approach of much of this textbook will appeal to those teaching courses for personnel inside and outside of government or those seeking to better understand the challenges and mechanics of counterterrorism. There is also enough interest on policy-related subjects for a wider audience, including those in European studies, given the heavy but not exclusively European flavor of the book. *Toward a Grand Strategy against Terrorism* may be a harder sell in the wider educational textbook market, particularly for undergraduate and graduate courses in civilian universities, considering its hard-nosed and unambiguous approach to terrorism. As an indicator or social and political barometer for how the professional CT community views the current terrorist threat, it is invaluable. For this reason the textbook may find a wider audience, if only as a useful contrast to other opinions (such as those offered by John Mueller and Ian Lustuck). It suggests that considerable differences of opinion remain in academic and practitioner circles and the gulf between how the threat of terrorism is perceived and what should be done about it may only be growing wider. The grand strategy demanded by some, and implied in this textbook, may be as elusive and far away as ever.

Notes

1. Russell Howard and Reid Sawyer, eds., *Terrorism and Counterterrorism: Understanding the New Security Environment, Readings and Interpretations* (New York: McGraw-Hill, 2002).

2. Howard and Sawyer, *Defeating Terrorism: Shaping the New Security Environment* (New York: McGraw-Hill, 2003).

3. James Poland, Understanding Terrorism: Groups, Strategies, and Responses (New York: Prentice-Hall, 2004, 2010). The first edition of this textbook was published in 1988.

4. See for example Russell Howard, James J. F. Forest, and Joanne Moore, *Homeland Security and Terrorism: Readings and Interpretations* (New York: McGraw-Hill, 2006) and the six editions of Jonathan White, *Terrorism and Homeland Security: An Introduction* (Belmont, CA: Wadsworth, 2006, 2009).

5. Russell Howard and James J. F. Forest, *Weapons of Mass Destruction and Terrorism* (New York: McGraw-Hill, 2007).

6. Howard and Sawyer, eds., *Terrorism and Counterterrorism: Understanding the New Security Environment, Readings and Interpretations*, rev. ed. (New York: McGraw-Hill, 2004), 75–85, 245–88, 303–9, 313–38.

7. Jeffrey Norwitz, ed., *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency* (Newport, RI: Naval War College, 2008).

8. Examples include Malcolm Nance, *Terrorist Recognition Handbook: A Practitioner's Manual for Predicting and Identifying Terrorist Activity*, 2d ed. (Boca Raton, FL: CRC Press, 2008).

9. See for example Jane Bullock, George Haddow, Damon Coppola, and Sarp Yeletaysi, *Introduction to Homeland Security: Principles of All-Hazards Response*, 3rd ed. (Burlington, MA: Elsevier, 2009).

10. Michael Licata, *Citizens Terrorism Awareness and Survival Manual* (Flushing, NY: Looseleaf Law Publications, 2009), 59.

11. Brian Michael Jenkins, *Will Terrorists Go Nuclear?* (Amherst, NY: Prometheus, 2008), 213–14.

12. Andrew N. Pratt, "Terrorism's Evolution: Yesterday, Today, and Forever," in *Toward a Grand Strategy against Terrorism*, eds. Christopher C. Harmon, Andrew N. Pratt, and Sebastian Gorka (New York: McGraw-Hill, 2010), 7.

13. James Q. Roberts, "Building a National Counterterrorism Capability: A Primer for Operators and Policymakers Alike," in *Toward a Grand Strategy against Terrorism*, 127.

14. Ibid., 128–29.

15. Ibid., 137.

16. Christopher C. Harmon, "Illustrations of Discrete Uses of Force," in *Toward a Grand Strategy against Terrorism*, 108.

17. Ibid., 115–17.

18. John Le Beau, "Intelligence and Counterterrorism: Examining the Critical Tools of Secrecy and Cooperation," in *Toward a Grand Strategy against Terrorism*, 201–6.

19. Celina Realuyo, "Following the Terrorist Money Trail," in *Toward a Grand Strategy against Terrorism*, 210–27.

20. John Kane, "Virtual Terrain, Lethal Potential: Toward Achieving Security in an Ungoverned Domain," in *Toward a Grand Strategy against Terrorism*, 266–69, 271.

21. Pratt, "Terrorism's Evolution," 4.

22. Sookhdeo, "Ideas Matter: How to Undermine the Extremist Ideology behind al-Qaeda," in *Toward a Grand Strategy against Terrorism*, 243.

23. Jean-Paul Raffenne and Jean-Francois Clair, "The French Counterterrorism System," in *Toward a Grand Strategy against Terrorism*, 353.

24. Sebastian Gorka, "International Cooperation as a Tool in Counterterrorism: Super-Purple as a Weapon to Defeat the Nonrational Terrorist," in *Toward a Grand Strategy against Terrorism*, 79.

25. Boaz Ganor, "International Cooperation and the Dynamic Terrorist Threat," in *Toward a Grand Strategy Against Terrorism*, 397.

26. Harmon, "Illustrations of Discrete Uses of Force," 118–19.