ENEMY WITHIN

Military Sexual Assault Inflicts Physical, Psychological, Financial Pain

By Coreen Farris, Terry L. Schell, and Terri Tanielian
Get the Big Picture

RAND Review covers the big issues with an eye for the important details.

For previous editions and free online subscriptions, visit www.randreview.org
“THIS SCOURGE MUST BE STAMPED OUT,” declared U.S. Secretary of Defense Chuck Hagel, referring to sexual assault in the military, during his commencement address at the U.S. Military Academy in West Point, New York, on May 25, 2013. The recipient of two Purple Hearts for his service as an army officer in Vietnam, Hagel urged the army’s newest officers to build “a culture of respect and dignity” in the armed forces. “We are all accountable and responsible for ensuring that this happens. We cannot fail the men and women that we lead.”

The day before Hagel’s address, President Barack Obama used his commencement address at the U.S. Naval Academy in Annapolis, Maryland, to warn graduates that military sexual assaults could erode America’s faith in the military itself, currently the nation’s “most trusted institution.” He urged the navy’s newest officers to rise above the example set by service-members who have committed sexual assault. To help counteract the scourge of sexual assault in the military, Coreen Farris and her colleagues propose a research agenda that takes full account of the types of damage being done.

On June 5, 2013, Germany and Italy became the first nations to commit to joining the United States as “lead nations” that will oversee different regions of Afghanistan after 2014, when the NATO role in Afghanistan will transition to a non-combat mission. The scourge of Taliban and al Qaeda extremism will likely persist in Afghanistan to some degree, but NATO will shift its role toward helping Afghan security institutions stabilize their own insurgency-wracked nation. Stephen Watts and others draw on numerous cases of comparable “minimalist international interventions” on behalf of partner governments over the past six decades to extract lessons for the kinds of limited efforts that could offer the greatest promise for Afghanistan and other war-torn countries in the years ahead.

Throughout the first half of 2013, governments, corporations, and militaries around the world grew increasingly alarmed by the proliferation of costly crimes committed in cyberspace. Neil Robinson suggests that one balm for this 21st-century scourge could be international coordination of cybersecurity efforts. In contrast, cyberwar efforts could aggravate matters, warns Martin Libicki in his refreshingly grounded and illuminating narrative about a topic that often comes across as abstract and incomprehensible. At least in this case, Libicki stamps out the scourge of impenetrability.

—John Godges

On the Cover: The woodland camouflage pattern has been used by the U.S. Army, U.S. Navy, U.S. Air Force, U.S. Marine Corps, and U.S. Coast Guard. COVER ILLUSTRATION BY EILEEN LA RUSSO
Dementia costs Americans hundreds of billions of dollars per year, and the annual cost could top half a trillion dollars by 2040 due to the “graying” of the U.S. population. The “market costs” of dementia already exceed those for cancer and heart disease, while the “informal costs” of home care for those with dementia can raise the total expense nearly 50 to 100 percent, depending on the calculation method. The National Alzheimer’s Project Act, signed into law in 2011, calls for these kinds of cost calculations, along with new treatments and improved care for people with dementia. In addition, says research leader Michael Hurd, director of the RAND Center for the Study of Aging, “This calls for an insurance-style solution, one in which the costs of long-term care could be spread across the entire population rather than being concentrated on the unlucky few.”

Millions of Americans provide unpaid, informal care for a family member with dementia, and many nonrelatives provide care as well. This informal caregiving represents a cost to society in the form of lost productivity and income. Researchers took two approaches to estimating the value of informal care: forgone wages (what caregivers would have earned if they had spent their time working in the labor market rather than caring for someone with dementia) and replacement cost (the cost of the equivalent service when provided through a home health agency).
Who has dementia?

3 in 20 Americans 71 or older

- 12% of women
- 9% of men
- 17% of Hispanics
- 10% of whites
- 18% of other race/ethnicity
- 15% of unmarried
- 7% of married
- 16% who didn’t finish high school
- 10% of high school grads
- 7% who went beyond high school

Dementia’s 2010 annual market costs relative to other diseases

- DEMENTIA: $109B
- HEART DISEASE: $102B
- CANCER: $77B

Dementia’s total annual economic cost will grow accordingly

- 2010: $215B
- 2020: $255B
- 2030: $361B
- 2040: $511B

(Using replacement cost)


Soaring caseload.

Cases of dementia may more than double by 2040

- 2010: 3.8M
- 2020: 4.5M
- 2030: 6.4M
- 2040: 9.1M

That’s an increase of about 5 million Americans with dementia

Soaring costs.

Dementia’s total annual economic cost will grow accordingly

- 2010: $215B
- 2020: $255B
- 2030: $361B
- 2040: $511B

(Using replacement cost)
On June 5, 2013, Germany and Italy became the first nations to commit to serving alongside the United States as “lead nations” that will oversee different parts of Afghanistan after 2014, when the NATO role there will shift to a noncombat mission, helping Afghan security institutions stabilize their own country. In the following series of essays, RAND authors draw on the historical record of “minimalist international interventions,” conducted on behalf of partner governments, to identify the kinds of limited efforts that could offer the greatest promise for Afghanistan and other countries in the years ahead.

For Stabilization Missions, Small Budgets Produce Limited Results

By Stephen Watts

Stephen Watts is a political scientist at the RAND Corporation whose work has focused on stability and peace operations, insurgency and counterinsurgency, coalition diplomacy, and political development in the wake of civil wars, particularly in Afghanistan, the Balkans, and Africa.
“Minimalist stabilization” missions, or small-scale interventions to stabilize a partner government engaged in violent conflict, could become the rule rather than the exception for U.S. military forces, given likely defense budget cuts. Limited missions such as these do not greatly increase a partner government’s odds of victory in a counterinsurgency campaign, but they do dramatically reduce that government’s probability of defeat—by degrading rebel capabilities and making it unlikely that they can topple the government.

Typically, such missions do not alter the underlying structure of a conflict, foster major political reforms in a partner government, or cut insurgents off from their resource bases. Usually, the gains can be converted into strategic success only if the underlying political or international structure of the conflict can be altered. Military power plays a role, but it is more about creating the framework within which a political process can operate.

In some cases, such modest results will be adequate. In other cases, they will not. In still others, the under-resourcing of interventions may have catastrophic results. The odds of success might be improved by three means: choosing carefully the circumstances in which minimalist interventions are launched, combining military operations with non-military instruments, and committing to stabilizing the eventual peace.

How small is small enough to be considered “minimalist”? As a rule of thumb, “minimalist” operations deploy less than one-tenth of the doctrinally accepted force-to-population ratio of 20 security personnel per 1,000 inhabitants—that is, fewer than 2 security personnel for every 1,000 residents. In practice, these operations tend to emphasize two features. First, they normally accept and work within existing local power structures rather than pursuing any broader transformative agendas. Second, they typically emphasize rapid development of the host nation’s own security forces so that responsibility for the partner’s security can be handed over as quickly as possible.

FISCAL DEBATE

The enormous costs of the U.S. interventions in Iraq and Afghanistan have sparked a backlash against military interventions generally, especially as the magnitude of the U.S. fiscal crisis has become apparent. While many critics of “nation-building” argue that the United States should abandon military interventions altogether, others continue to accept that such interventions may be necessary to secure U.S. interests. Where the United States went wrong, the latter contend, is in the scale of its ambitions and the concomitant ways and means adopted to achieve them. They argue that, rather than seeking to transform the domestic politics of foreign countries—a utopian or at least prohibitively costly goal—the United States should commit only the minimum resources necessary to stabilize the target states. Such small-scale interventions supposedly offer the opportunity to secure core U.S. interests at vastly less cost than larger nation-building missions.


AP IMAGES/JAVIER GALEANO; REBECCA BLACKWELL; BRENNAN LINSLEY
Despite the enormous stakes involved in this debate, including present-day choices about U.S. force reductions, there is little empirical evidence to corroborate many of the claims on either side. In fact, the record of 22 small-scale military interventions over the past four decades reveals their seemingly paradoxical results: While not contributing greatly to a partner government’s success, they do help such a government avoid defeat. This apparent contradiction is explained by the increasing number of indeterminate outcomes—cases in which conflicts become mired in stalemate or terminate with negotiated settlements that concede considerable political and security rights to the insurgents (see the pie charts).

Minimalist stabilization typically contributes to significant operational successes (such as degrading insurgent capabilities) but not to decisive gains. In the case of U.S. operations in Colombia over the past decade, for instance, insurgents have experienced a number of significant setbacks, but the government appears to be nearing a “floor” beneath which it is difficult to continue reducing the number of insurgents. Likewise, in El Salvador in the late Cold War period, U.S. assistance ensured that the government would not fall to Communist forces, but it was incapable of bringing the conflict to an end. Instead, the war became bogged down in a bloody, prolonged draw. In the case of French intervention on behalf of the government of the Central African Republic in the 1990s, a number of coup attempts were thwarted—but they resumed almost as soon as international forces departed, leading to the overthrow of the government within two years. These cases suggest that only with a more fundamental change in the politics or international context of a conflict does decisive success become likely.

These findings do not yield simple policy prescriptions. They do, however, caution against viewing minimalist stabilization as a panacea. Modest resource commitments generally yield modest results.

**WORTH THE TROUBLE, SOMETIMES**

What is the value of minimalist intervention if it can improve the odds of avoiding defeat but can seldom secure victory? The answer depends on the objectives and on the context of the intervention. As for the objectives, there are four rules of thumb.

First, avoiding defeat may secure at least minimal U.S. objectives if the loyalty of the partner government is of greatest concern. In El Salvador, for instance, the greatest concern was avoiding the fall of another Central American country to Communism. It is debatable whether such an outcome was worth the costs of the conflict or whether such assistance could have been sustained indefinitely had the Soviet Union not collapsed, but the United States did achieve its core objective.

Second, minimalist intervention may secure U.S. interests if the United States is not opposed to a compromise that would offer the insurgents real political power and security guarantees. Insurgents typically will have to be convinced, before they will be willing to negotiate, that they cannot achieve military victory, and minimalist interventions can help to convince them of the necessity of compromise.

Third, minimalist stabilization may be a useful instrument of foreign policy if a prolonged period of low-level violence is an acceptable outcome. The critical

---

**Minimalist Stabilization Missions Have Produced a Dramatic Increase in Indeterminate Outcomes**

![Pie charts showing outcomes for partner governments with and without minimalistic intervention.](source: The Uses and Limits of Small-Scale Military Interventions, 2012. Note: The data represent 54 cases of no intervention (left pie) and 22 cases of minimal intervention (right pie) since 1970.)

**Outcomes for Partner Governments**

- **No Intervention**
  - Victory: 35%
  - Defeat: 43%
  - Indeterminate: 22%

- **Minimalist Intervention**
  - Victory: 27%
  - Defeat: 46%
  - Indeterminate: 27%

---

**SOURCE:** The Uses and Limits of Small-Scale Military Interventions, 2012.

**NOTE:** The data represent 54 cases of no intervention (left pie) and 22 cases of minimalist intervention (right pie) since 1970.

---

**It may well be that the unintended effects of an intervention are worse than the crisis that motivated it.**
question is whether an insurgency, once degraded and contained, will stay degraded and contained. If not, minimalist intervention may become an indefinite commitment.

Fourth, minimalist stabilization may be appropriate if there is little concern about the “externalities” of prolonged conflict. Civil wars are associated with refugee flows, the spread of disease, depressed licit economic activity in neighboring states, the flourishing of transnational criminal networks, the incubation of transnational terrorist movements, the spread of instability and conflict into neighboring countries, and a variety of other ills. It may well be that the unintended effects of an intervention are worse than the crisis that motivated it.

As for the context of the intervention, there are at least three contexts in which minimalist stabilization appears to be particularly effective. One is when both the partner government and the insurgents are weak: In such cases, small forces from outside may be enough to tip the balance decisively. Another appropriate context is when there is a realistic opportunity to interdict insurgents’ resource streams; in most cases, however, such interdiction is difficult or impossible, as the examples of Colombia and Afghanistan attest. A third useful context is when a realistic path to a negotiated settlement is visible but requires outside intervention, such as a peacekeeping force, to secure.

BEYOND MILITARY MEANS

The odds of success might also be improved by combining minimalist operations with nonmilitary instruments. First and foremost are financial instruments. Many insurgencies have ended rapidly—and the post-conflict periods have remained highly stable—when insurgents have lost outside state financial sponsorship. Such a path to conflict termination usually requires a diplomatic process in which the external powers with an interest in the conflict are able to secure their core interests in a negotiated settlement.

The other potentially crucial role for nonmilitary instruments is to bind partner governments to critical reforms. Foreign assistance may provide a government with enough resources to alleviate internal pressures for reform but too few resources to enable fundamental changes. The result would be stagnation—a phenomenon commonly observed and criticized within the development community. A number of instruments have been devised to try to tie assistance more closely to reform efforts, such as embedding foreign personnel within the partner state’s government, setting up trust funds or other financial instruments that require certain standards to be met before money is disbursed, and so on. Perhaps most critical, however, is the credibility of the intervening state’s threat to “walk away” if key conditions are not met.

Finally, the odds of a successful outcome might be improved by long-term security commitments to the partner state. The fact that most minimalist interventions lead to stalemate or negotiated settlements—outcomes that are historically precarious and frequently lead to renewed fighting—suggests that the need for stabilization missions does not end immediately after the conflict but rather endures well into the post-conflict period. Such peace operations, however, are being almost completely ignored in the current debates.

PARTNERS WANTED

Because lengthy stabilization missions can place tremendous stress on U.S. forces, the United States should seek to enlist other partners in such missions whenever possible. One promising model is the “hybrid” approach used in Sierra Leone and the Democratic Republic of the Congo. In these missions, a large number of mostly lower-quality forces in United Nations peace operations were combined with a small number of forces from Great Britain or France. The higher-quality NATO troops served as a “maneuver force” capable of interceding in high-risk flashpoints or helping to organize local forces to do the same, while the remainder of the international troops provided the “holding forces” to stabilize other parts of the country. Such a model would reduce the expense of long-term, large-scale stabilizing missions and lessen the stress on U.S. forces.

Any time the United States helps to build the military capacity of other countries, it is critical that it put in place safeguards to ensure, as much as possible, that its assistance is not abused. U.S. support may embolden partner governments to take inadvisable risks, as arguably was the case in the Georgian confrontation with Russia in 2008. Partner governments may also use their military capabilities for repression and even genocide, as was the case with the Hutu government of Rwanda, which had received French military assistance for many years. In interventions in which large numbers of U.S. ground forces are present, such risks can be reduced. But in minimalist interventions, these risks are elevated. The United States should establish unmistakable “red lines” in such cases and make clear that there are extremely serious repercussions for violations of those limits.

Minimalist stabilization operations yield a reasonable chance of modest success for a modest cost. But there are definite limits to what minimalist stabilization can accomplish. Those waging the contemporary defense debates in the United States should be cognizant of these limitations and avoid the tendency—evident in history—to escape the mistakes of large interventions only by expecting too much of small ones.

RELATED READING

The Uses and Limits of Small-Scale Military Interventions, Stephen Watts, Caroline Baxter, Molly Dunigan, Christopher Rizzi, MG-1226-RC, 2012, 158 pp., www.rand.org/t/MG1226
Minimalist International Interventions

For Building Partner Capacity, Choose Partners Wisely

By Christopher Paul

Christopher Paul is a social scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School.

Stabilization missions entail a full range of activities to stabilize a partner country: establishing security, restoring essential services, supporting governance, and supporting economic and infrastructure development. One activity that often overlaps the security component of stabilization missions is “building partner capacity” (BPC), which refers to developing the security organs of partner states. These security organs could include defense ministries, armed services, maritime forces, peacekeeping forces, national police agencies, or local defense forces.

Changing economic realities and the ongoing reductions in U.S. defense spending will reduce the funding available for such security cooperation efforts. Therefore, the United States will need to increase the effectiveness and efficiency of such efforts. What can history tell us about which approaches to BPC are likely to be more or less effective under different circumstances?

Twenty years of data on 29 cases of U.S. involvement in BPC show that it works well when (a) the capacity being built meets the interests of both the partner country and the United States and (b) the activities are a good match for the partner’s baseline capability and its capacity to absorb new materiel and training. BPC is also more likely to be effective when partner nations invest their own funds to support or sustain their capacity, have highly functioning governments, have strong economies, and share broader security interests with the United States.

In other words, if BPC is consistently funded and delivered, supported and sustained, well matched to partner capabilities and interests, and shared with a partner that supports the effort and is healthy economically and in terms of governance, prospects for success are very good. BPC can still be effective when only some of these conditions are met. For instance, BPC done well, done consistently, and matched to partner absorptive capacities and interests can be effective even when the partner is not particularly strong in any dimension at the outset.

All things being equal, preference should be given to those partner nations that exhibit economic and governmental strengths. Strategic imperatives can compel a partnership with a country that lacks some of the desired attributes. Regardless of the partner or context, BPC goals and activities should correspond with what the partner wants or needs and what it is capable of absorbing. Whether working with ideal or suboptimal partners, the prospects for effective BPC increase dramatically when the goals of both parties align and when the activities fit the partner’s potential for growth, which can be determined by assessing such factors as the equipment, organization, readiness, training, technological sophistication, education, language abilities, and doctrine of a nation’s security forces.

Strategic imperatives can compel a partnership with a country that lacks some of the desired attributes.

RELATED READING
For Afghan and Other Local Defense Forces, History Holds Warnings

By Austin Long

Austin Long is a political scientist at the RAND Corporation.

From Afghanistan to Mali, current efforts to build local defense forces in the context of counterinsurgency have made the lessons learned from prior efforts especially salient. An examination of eight efforts from 1945 to the present shows that the greatest value of local defense forces lies in intelligence, not combat, and that the misuse of such defensive forces—that is, as offensive ones—can greatly reduce their effectiveness. For Afghanistan specifically, the historical record also suggests that rapid expansion of the Afghan Local Police today could weaken the relative harmony among U.S. Special Operations Forces, local forces, and the Afghan government.
Traditionally, counterinsurgents have relied on local defense forces for many reasons. These units act as force multipliers for regular armies that must cover large swaths of territory. The units have unmatched knowledge of the local terrain and populations. Local defense forces may be more motivated to fight than many regulars, because they directly see the results of security improvements on their families and communities. Employing local defense forces also depletes the potential recruiting pool of insurgents while providing the central government some sense of perceived, if not actual, popular support.

The use of local defense forces is not, however, devoid of risks. Militias often represent parochial interests that may, if unchecked, promote lawlessness, increase insecurity, and undermine the state. Lacking the discipline and training usually expected from regular troops, such militias may attempt to settle scores against other local groups, leading to an escalation of violence and political fragmentation. They may engage in corruption and predatory behavior against their own populations. And the proximity with insurgents that makes these militias a precious source of intelligence may also lead them to defect to the enemy, sometimes with the arms provided by their protectors.

Utilizing local defense forces in counterinsurgency can thus be a high-reward but high-risk strategy, making it particularly critical to identify the factors that seem to increase or mitigate the risks—especially given the currently widespread use of the strategy. With the expansion of the Afghan Local Police as a major part of the pending U.S. withdrawal from Afghanistan, the lessons learned from earlier efforts are needed more than ever.

FROM WORLD WAR II TO TODAY

The eight case studies are Indochina, Algeria, South Vietnam, Oman, El Salvador, southern Lebanon, Afghanistan, and Iraq. The cases involve a wide range of intervening countries, including the United States, the United Kingdom, France, Israel, and the Soviet Union. Although the cases differ widely in terms of their time frames, geographic locations, and intervening countries, they offer a number of strikingly similar lessons, suggesting that the past experiences can usefully inform current and future efforts.

The first lesson is that politics is paramount in local defense operations. Any intervening country must assiduously manage a tri-lateral relationship among itself, the host-nation government, and the local actors it wants to incorporate into local defense forces. There is frequently friction in this relationship that, if not carefully managed, can make the local defense effort ineffective. Of particular concern today in Afghanistan is the role of U.S. oversight in mitigating this friction. Rapid expansion of local forces can greatly increase the friction while oversight becomes strained. Finding the proper balance between speed of expansion and proper oversight is one of the central challenges of these programs.

Second, the real value of local defense forces lies in intelligence. The synergy between U.S. combat capability and local defender intelligence is devastating to insurgents, who face a choice between being defeated piecemeal by the local forces who can identify them or massing to confront the defenders, which makes the insurgents vulnerable to U.S. firepower. Misusing local defenders as offensive combat forces can debilitate them.

Third, local history can limit—or propel—the effectiveness of local defense. Where government-affiliated paramilitaries have existed before, locals may be highly skeptical of them if their behavior was negative. Conversely, insurgent behavior that antagonizes the local population can positively affect efforts to build local defense forces.

Fourth, these efforts often require more than U.S. military support. Both the Central Intelligence Agency and the U.S. Agency for International Development have provided effective, sometimes critical, support to local defense. These agencies have unique authorities and skills for managing the often- fractious politics and economics of local defense. Integrating these agencies into future programs will likely be crucial to success.

Fifth, relationships should be maintained between local defense forces and the conventional military forces that actually secure and hold terrain. Local defense forces need flexibility and autonomy. But the support of conventional forces is crucial to ensuring that the intelligence gathered by local defense forces is properly exploited and that local defenders are protected from a massed enemy.

Sixth, it is important to avoid insurgent strongholds when building local defense forces. Local forces should be built in areas where the insurgency has been weakened, by either military action or insurgent defections.

Seventh, demobilization or transition of local defense forces into a formal government security force must be handled with great care. Executing such a transition correctly takes a lot of time, whereas it can be done wrong overnight. History shows that even successful cases of transition faced numerous challenges and took considerably longer than anticipated.

APPLYING THE LESSONS TO AFGHANISTAN

Afghanistan has a long and troubled history of militias. As a result, special operations forces have made strenuous (if not always successful) efforts to dissociate the Afghan Local Police from these militias. The local police are subject to all the same restrictions as the Afghan National Police, including the restrictions regarding the use of force, and are subject to extensive control and oversight.

Efforts have also been made to manage the relationship among the Afghan Local Police, the Afghan government, and the United States.

With the expansion of the Afghan Local Police, the lessons learned from earlier efforts are needed more than ever.
Inevitably, expanding the ranks of the Afghan Local Police would necessitate combining more conventional forces with less oversight. The latter could mean using a hub-and-spoke model, in which a special operations unit in a district center oversees multiple Afghan Local Police units. Managing this shift in oversight is likely to be the single greatest challenge the program faces over the medium term.

Maintaining the limited operational and geographic scope of the local forces will also be important. As U.S. withdrawal from Afghanistan takes place, there may be pressures to increase the use of the local forces outside their home districts or in more offensively oriented ways. The case studies indicate that this is unlikely to be successful.

The future of the Afghan Local Police will hinge on continuing to manage relationships effectively. The trilateral relationship among coalition forces, the Afghan government, and the local communities must be sustained, which is hardly a given and will require extensive effort. Likewise, managing local politics across a wide variety of Afghan Local Police units and communities will require great effort. Without such management, all of the program’s previous successes will likely be rendered irrelevant.

By transforming what was once called the Local Defense Initiative into Village Stability Operations and then into the Afghan Local Police, the central government’s concerns have been substantially reduced (though not eliminated). Ongoing engagements between U.S. and Afghan leaders have kept the program on track even as the numbers of the Afghan Local Police have rapidly expanded. In terms of appropriate tactical employment of the local force, U.S. Special Operations Forces also seem to be following the lessons learned. Although locals are frequently used for checkpoint security, this is often combined with patrolling and intelligence collection.

The relative success of the program has created substantial pressure to expand it quickly. But rapid expansion is seldom associated with long-term success and could undermine the current level of harmony among all participants involved in the effort. The central recommendation for those now overseeing the Afghan Local Police is to resist pressure to change the methodology of the program for the sake of expediency. Such deviation is likely to lead to trouble.

This is particularly important in terms of where the local units are established. Trying to establish a unit in a new location simply because of its strategic importance is unlikely to be successful. It is only when the local populace is motivated to support local defense for reasons internal to the community that lasting success is possible.

Numerical increases of the program raise additional oversight questions. At present, oversight comes from U.S. Special Operations Forces, but there are a finite number of special operations personnel.

It is only when the local populace is motivated to support local defense for reasons internal to the community that lasting success is possible.

Related Reading

Left to right: Trucial Oman Scouts, trained by British officers, conduct a traditional camel patrol, with camels rented from local farmers, in February 1972. A Montagnard mountain tribesman receives training to fight Viet Cong guerrillas in South Vietnam in 1962; the trainees wore loincloths, old French uniforms, or discarded European clothing. A Malian soldier checks identity papers in Diabaly, Mali, on January 21, 2013, days after the French military intervened to recapture the country from radical Islamists.

AP IMAGES/JEROME DELAY (MALI)
Minimalist International Interventions

For Nation-Building Missions, Modest Costs Yield Meaningful Benefits

By James Dobbins and Laurel E. Miller

In May 2013, Ambassador James Dobbins was named by President Barack Obama as his special representative for Afghanistan and Pakistan; prior to this appointment, Dobbins served as director of the RAND International Security and Defense Policy Center. Laurel Miller is a political scientist at the RAND Corporation.

Of 20 major nation-building missions undertaken since the end of the Cold War, 16 have produced greater peace, 18 led to increases in democratization (according to Freedom House), 14 resulted in improvements in government effectiveness (according to the World Bank), 16 experienced economic growth (generally faster than their regions or income groups), and 15 saw improvements in human development (as measured by the United Nations Development Programme). Most of these efforts achieved their primary aim—establishing peace—while also generating these other benefits. And most did so at modest cost.
In six illustrative cases, many local factors that had contributed to conflict defied modification or elimination, despite the nation-building interventions. In Cambodia, nationalism and xenophobia endured; in El Salvador, landlessness remained a problem; in Bosnia, ethnic divisions hardened; in the Democratic Republic of the Congo, institutions continued to be extremely weak; in East Timor, regional and political identity differences continued to produce civil unrest; and in Sierra Leone, the inequitable distribution of resources persisted. Though improvements were achieved to varying degrees in these countries (as shown in the six upper tiers of the table), the governments largely remained ineffective developers of public services, poor societies remained poor, resources continued to be looted, the capabilities of security institutions were still weak, and in none of the cases was corruption seriously diminished.

Nevertheless, the nation-building operations in most of these countries succeeded in improving security, advancing democratization, expanding economic activity, and increasing human development, as did most of the rest of the 20 post–Cold War operations, ranging from Haiti to the Solomon Islands and from Macedonia to Mozambique. In most cases, the costs were low, in contrast to the much more expensive and demanding counterinsurgency campaigns conducted in Afghanistan and Iraq.

Among all 20 operations, 17 were intended to maintain peace after a settlement had been reached, whereas 3—in Somalia, Afghanistan, and Iraq—were intended to impose peace. Of the peacekeeping-type missions, all but one (in the Democratic Republic of the Congo) produced lasting peace. In contrast, none of the peace-enforcement missions has yet done so. That is to say, all but one of the interventions that were initiated on the basis of a peace agreement and with the consent of the parties to the conflict subsequently succeeded in establishing peace, whereas the three that lacked such prior consent did not.

Geopolitics and the strength of internal patronage networks help explain the failures. Afghanistan and Iraq were both invaded by the United States; thus, neither was there a peace agreement among all parties in place when international forces arrived, nor did the presence of foreign forces enjoy the consent of all parties. In both cases, the United States chose to exclude rather than co-opt the dominant patronage networks. Denied their accustomed access to wealth and power, these networks chose to fight back. Perhaps even more importantly, the disgruntled elements were able to receive substantial external support in order to do so.

Despite the failure to forestall renewed conflict in Afghanistan, there has been remarkable progress there across several other dimensions (also shown in the table). In the first ten years after the intervention, Afghan society achieved less than the average improvement in democratization but ranked third among the 20 cases in improved government effectiveness, scored second in economic growth, and showed the greatest improvement of all in human development. These results cannot be explained entirely by external aid flows, because Afghanistan was not among the largest foreign aid recipients on a per capita basis.

Nor is it simply that Afghanistan started from a lower base, because Liberia, Sierra Leone, and the Democratic Republic of the Congo were all poorer to begin with and grew less rapidly. Dramatic advances in Afghanistan’s school enrollment and life expectancy, declines in infant mortality, and rapid economic growth even in some of the most-conflicted areas of the country do reflect the emphasis of the Afghan government’s counterinsurgency and development strategies in pushing resources and public services out into the hinterland.

### DIPLOMACY PLUS RESOURCES

Across the 20 missions, the nation-building interveners had a limited set of tools at their disposal. Among these, the most decisive tool for achieving the main aims of intervention seems to have been diplomacy, when backed by economic and military assets. Thus, just as geopolitics was the most important factor in either sparking or sustaining conflict in each of the six case studies, so diplomacy

---

**Nation-Building Missions Usually Scored Important Gains, Even with Modest Levels of Assistance**

<table>
<thead>
<tr>
<th>Country (in chronological order)</th>
<th>Average Annual per Capita Assistance in the First 5 Years (constant 2010 U.S. dollars)</th>
<th>At Peace in 2012</th>
<th>Net Change in Freedom Index (10-point scale)</th>
<th>Net Change in Government Effectiveness (10-point scale)</th>
<th>Net Change in Human Development Index Score (10-point scale)</th>
<th>Cumulative Growth in per Capita Gross Domestic Product (percentage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cambodia</td>
<td>38.36</td>
<td>Yes</td>
<td>+0.75</td>
<td>+0.07</td>
<td>NA</td>
<td>53.6</td>
</tr>
<tr>
<td>El Salvador</td>
<td>79.57</td>
<td>Yes</td>
<td>+0.75</td>
<td>+0.36</td>
<td>+0.7</td>
<td>20.6</td>
</tr>
<tr>
<td>Bosnia</td>
<td>384.00</td>
<td>Yes</td>
<td>+3.75</td>
<td>+1.95</td>
<td>NA</td>
<td>213.7</td>
</tr>
<tr>
<td>Democratic Republic of the Congo</td>
<td>36.46</td>
<td>No</td>
<td>+0.75</td>
<td>-0.25</td>
<td>+0.6</td>
<td>8.2</td>
</tr>
<tr>
<td>East Timor</td>
<td>361.00</td>
<td>Yes</td>
<td>+6.25</td>
<td>NA</td>
<td>+0.9</td>
<td>42.7</td>
</tr>
<tr>
<td>Sierra Leone</td>
<td>93.10</td>
<td>Yes</td>
<td>+2.25</td>
<td>+0.49</td>
<td>+0.8</td>
<td>72.7</td>
</tr>
<tr>
<td>Afghanistan</td>
<td>62.72</td>
<td>No</td>
<td>+1.5</td>
<td>+1.53</td>
<td>+1.7</td>
<td>130.9</td>
</tr>
<tr>
<td><strong>20-Country Average</strong></td>
<td><strong>156.95</strong></td>
<td><strong>Yes</strong></td>
<td><strong>+2.15</strong></td>
<td><strong>+0.61</strong></td>
<td><strong>+0.6</strong></td>
<td><strong>54.6</strong></td>
</tr>
</tbody>
</table>

**Source:** Overcoming Obstacles to Peace, 2013.
proved decisive not just in mediating peace agreements but also in improving the behavior of the external actors that had given rise to or perpetuated the conflicts.

It is important to recognize, however, that even the most skillful diplomacy and the most favorable regional environments would not have sufficed to bring enduring peace to these societies. The international community also had to be willing to bring to bear military and policing capabilities, as well as economic assistance, to establish public order, demobilize combatants, reintegrate former fighters into civilian life, and create new political and economic avenues through which formerly warring factions could compete for power and wealth via peaceful rather than violent means. Where such efforts have been inadequately resourced or unwisely executed, the result has been subpar outcomes, even in favorable geopolitical circumstances.

A few spectacular nation-building failures have created a widespread impression that these missions seldom succeed. In fact, the great majority of them over the past two decades have resulted in improved security, greater democratization, significant economic growth, and higher standards of living, and most have done so with a modest commitment of military resources and economic assistance.

Perhaps most crucially, operations that have enjoyed local consent and regional support have almost always achieved peace, even when a degree of coercion was employed to secure both. Operations that did not secure local consent and regional support did not achieve peace, although even these efforts have produced improvements in most of the other dimensions assessed, particularly in Afghanistan. These findings suggest the importance of setting realistic expectations—neither expecting nation-building to quickly lift countries out of poverty and create liberal democracies, nor being swayed by a negative stereotype of nation-building that fails to recognize its signal achievements in the great majority of cases.

**RELATED READING**
Overcoming Obstacles to Peace: Local Factors in Nation-Building, James Dobbins, Laurel E. Miller, Stephanie Pezard, Christopher S. Chivvis, Julie E. Taylor, Keith Crane, Calin Trenkov-Wermuth, Tewodaj Mengistu, RR-167-CC, 2013, 348 pp., www.rand.org/t/RR167
But these decisions could have their virtues. Access agreements are less expensive to maintain than military bases, but they still enable the United States to scale its presence up or down, depending on the circumstances. A smaller and more sporadic U.S. military presence is less likely to cause friction with local populations. Host nations are likelier to grant Washington the right to use bases occasionally than to allow it to station forces on their territories permanently, so long as they can be convinced or believe that a smaller or more intermittent military presence remains a credible deterrent to aggression.

A focus on acquiring limited access would improve the probability that the United States could begin to make inroads in critical regions where it currently has little to no presence. Periodic access to host-nation facilities would also minimize the risk of making major investments in infrastructure only to have the host nation revoke U.S. rights. Finally, the United States would raise its chances of securing forward access for any given operation by diversifying its overseas presence. For these reasons, the Pentagon should adopt a posture that is less costly, less vulnerable, and less conspicuous—yet more versatile.

TRANSITION POINTS
Over the past two centuries, the United States repeatedly adjusted its military posture in response to new threats, technological innovations, and the availability of overseas bases. Since independence, senior officials have developed and at least partially implemented seven distinct U.S. global postures: continental defense (1783–1815), continental defense and commercialism (1815–1898), oceanic posture and surge deployments (1906–1938), hemispheric defense (1938–1941), perimeter defense in depth (1943–1949), consolidated defense in depth (1950–1989), and expeditionary defense in depth (1990–present).

Until the drawdowns precipitated by the end of the Cold War, there had been a mostly consistent and linear development toward an increasing military presence overseas. However, there has also been a cyclical pattern of concentration and dispersion. On the one hand, when officials were confident in the identity and location of serious threats, they tasked forces with defending fixed locations. On the other hand, when it was unclear what types of threats might emerge or where they might be located, large portions of the military were organized, trained, and equipped as an expeditionary force that could be deployed abroad in response to emergent threats.

The permanent overseas military bases that remain today at the heart of America’s global posture are a historical anomaly. The United States gained access and deployed its forces (and often their families as well) to large foreign bases only after World War II, to contain the Soviet Union. The sprawling garrisons in Western Europe and Northeast Asia that house U.S. troops and their dependents are a legacy of the Cold War, specifically the unique situation in the early 1950s, when the global threat of the Soviet Union drove many non-Communist states together, uniting them against a shared enemy.

Moreover, because World War II had debilitated many of these nations, they required external assistance to counter the Communist bloc, and the United States was the only nation capable of providing assistance. After the Korean War, the fear of Communism impelled the weakened Asian and European nations not only to align with the United States but also to allow Washington to position U.S. troops and their families on their territories indefinitely in large bases. The conditions that gave rise to these bases, however, are unlikely to be replicated in the near future.

A NEW ERA AWAITS
The Cold War experience does underscore one pertinent historical lesson. Throughout U.S. history, the most common reason that another nation has permitted the United States to establish a military presence on its territory is a shared perception of threat. Absent a serious danger to their security, nations are unlikely to voluntarily circumscribe their sovereignty by either providing U.S. forces temporary access to military facilities on their territories or allowing the United States to permanently station its forces within their borders. In other words, a period of shared threat is the most opportune time for the United States to forge new access agreements with prospective security partners.

Today, there is a lack of consensus in the United States and abroad regarding the likely consequence of China’s economic growth and military modernization. Nevertheless, the United States has been able to exploit China’s increasingly assertive behavior to expand America’s rotational military presence in Australia and Singapore. If U.S. policymakers continue to regard an overseas military presence as essential, they would benefit from seizing on opportune moments when shared perceptions of threats are rising.

America’s global defense posture remains one of the underlying elements of U.S. grand strategy, enabling the United States to reassure allies under duress, deter adversaries, project force abroad when called on to do so, and guarantee the freedom of the commons. Yet it is not clear that America’s current overseas military presence is optimized for the future. The changes currently under way in the fiscal, political, and strategic environments could require significant revisions to the disposition and orientation of U.S. forces overseas. While the United States should retain legacy bases that remain useful for countering future security challenges, it should increasingly focus on developing access agreements instead of permanent garrisons. In light of the changes currently under way, it is also important to recall that the United States has repeatedly modified its global posture in response to new conditions.

RELATED READING
Cybersecurity Strategies
Raise Hopes of International Cooperation
By Neil Robinson

Cyberwar Fears
Pose Dangers of Unnecessary Escalation
By Martin C. Libicki

Illustration by Dori Gordon Walker and Eileen La Russe
Tangled Web

Cybersecurity Strategies Raise Hopes of International Cooperation

By Neil Robinson

Neil Robinson is an information scientist at RAND Europe.

Attacks against national and private interests in the borderless realm of cyberspace over the past few years have spurred international efforts to defend critical information infrastructures. Some of the triggering events have included the "denial-of-service" attacks against Estonia in 2007, growing concerns about the "digital espionage" capability of certain nations, and the online targeting of corporate intellectual property, classified government information, and the financial interests of companies and individuals alike.

In many European and North American countries, cybersecurity strategies have widely become viewed as increasingly important mechanisms for addressing these risks. However, the bodies in charge of leading or coordinating cybersecurity policy across the countries vary from cabinet offices to interior ministries to defense or national security directorates—an unevenness that could hinder international cooperation.

In France, China has been suspected of posing a particularly formidable threat. One concern among French officials is that electronics imported from China could be implanted with "logic bombs," trap doors, and Trojan horses, all of which could be remotely activated on command. The Netherlands, meanwhile, has singled out digital espionage by China, Iran, Russia, and other hostile states, as well as attacks perpetrated by professional criminals, as the most pressing cyber threats.

The United States has also named China as a specific culprit. In a May 2013 report, the Pentagon accused the Chinese government and military of mounting attacks on U.S. government computer systems and defense contractors in an effort to steal intellectual property and to gain strategic advantage. The report adds urgency to talks expected to begin in July between the United States and China about cyber issues.

In Germany, the government considers data security “the central common challenge for state, business, and soci-
As a nation that uses highly industrialized, complex technologies and that relies on sophisticated organizational structures more intensively than do many others, Germany is especially vulnerable to critical infrastructure attacks.

**Emerging Cyberdefense Collaborations**

Supranational cyberdefense initiatives have begun to emerge within NATO and, to a lesser extent, the European Union. One key difference between these two organizations is that NATO “owns” its own cyberdefense infrastructure (command, control, communications, computers, and information systems), whereas the responsibilities for cybersecurity (as well as national security) across the European Union generally remain the prerogative of national governments within the union.

Bulgaria, Estonia, Poland, Slovakia, Turkey, the United Kingdom, and the United States have signed agreements with NATO to cooperate in the event of a cyberattack. NATO is also strengthening the Cooperative Cyber Defence Centre of Excellence, established in 2007. Based in Tallinn, Estonia, the center constitutes a joint effort among Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Poland, Slovakia, Spain, the Netherlands, and the United States to improve cyberdefense interoperability. Turkey intends to join the effort, and NATO has shown interest in extending membership to Iceland. Ukraine is also part of a NATO working group on cyber and military reform.

Nonetheless, there are limits to NATO’s influence over the cyber systems of its 28 members. Although the majority of NATO nations agree that cybersecurity is a matter of increasing concern, not all of them share the same threat perceptions or strategic priorities. Such divergent perspectives could limit the scope of NATO action. Furthermore, NATO does not have the mandate to exercise authority over civilian or private-sector infrastructures. This issue is especially important, given the way in which cyberspace and cyberdefense cross the boundaries of the public and private sectors.

The European Union has no single approach to cybersecurity comparable to that of NATO, but the European Union does have a policy responsibility covering areas of civilian cybersecurity, cybercrime, and police and criminal justice cooperation in cyberspace. Again, however, these responsibilities across the European Union remain the prerogative of national governments.

Different national governments, as well as NATO and the European Union, have taken different approaches concerning the lead responding authorities for cybersecurity. The United States Cyber Command directs the operations and defense of specified U.S. Department of Defense networks, while the U.S. Department of Homeland Security is the primary agency responsible for defending other U.S. government networks. The United Kingdom and Canada have a central coordinating body. Estonia, France, the Netherlands, and NATO have departments or ministries specifically for cybersecurity. Finland has a highly distributed model, while in Denmark, the Danish Security and Intelligence Service takes the lead but assigns other departments responsibility over certain sectors. The European Union has an even more complex arrangement, with separate mandates covering industrial policy, cybercrime, and so on, suggesting a need for greater coordination.

These ad hoc and uncoordinated measures may not be sufficient to ensure the integrity and availability of information systems and critical infrastructure that support everyday life. In the multinational context of cyberspace, one is only as strong as one’s weakest, well, hyperlink. Further cross-government and cross-sector efforts may be required. Mapping in detail the “hubs” of institutional cyber policy decisionmaking in each country would be a valuable step toward seamless cooperation.

Future efforts should also be supported by advanced intelligence capabilities that identify and prevent prospective attacks rather than merely reacting to them. The Netherlands, the United States, and others, for example, are building “active defense” capabilities, such as an ability to break into the computer networks of adversaries, under the principle that “attack is the best form of defense.” However, the jury is still out on whether this approach would be appropriately preventive in nature or indeed could be counterproductive.

In discussions at the European Union in Brussels and in other national capitals, policymakers are seeking to ensure that the cost to adversaries of exploiting cyberspace vulnerabilities is high, that the prospects for success are low, and that business and society are prepared and resilient. Policymakers will also need to consider where to draw the line between prudent prevention and risky preemption.

**Related Reading**

In their zeal to protect themselves in cyberspace, countries need to ensure that they do not trigger even greater threats beyond cyberspace, particularly military or economic forms of retaliation. At a time when the reported level of cyber incidents continues to rise and when cyber risks are perceived as growing even faster, the odds are increasing that a country will find itself in a cyber crisis. Such a crisis could take many different forms: the escalation of tensions associated with an actual, major cyberattack; the suspicion that such an attack has already occurred and must be countered; or the simple fear that an attack might soon occur and must be preempted.

### Thick Fog of Cyberspace

The normal human intuition about how things work in the physical world does not always translate well into cyberspace. The effects, and sometimes even the fact, of cyberoperations can be obscure. The source of the attacks may not be obvious; the attacker must claim them, or the defender must attribute them. Even if the facts are clear, their interpretations may not be; even when both are clear, policymakers may not necessarily understand them.

The subjective factors of cyberwar pave paths to inadvertent conflict. Uncertainties about allowable behavior, misunderstandings of defensive preparations as offensive ones, errors in attribution, unwarranted confidence that cyberattacks are low-risk because they are hard to attribute, and misinterpreting the norms of neutrality—these are all potential sources of instability and crisis. Here are three examples of the kind of perils that lurk:

- **Computer network exploitation**—espionage, in short—can foster misperceptions and possibly conflict. Everyone spies on everyone, even allies. But one side tires of having its networks penetrated. Perhaps the frequency and volume of exploitation crosses some unclear red line; or the hackers simply make a mistake tampering with systems to see how they work and unintentionally damage something.

- One side’s defensive preparations can give the other side the notion that its adversary is preparing for war. Likewise, preparing offensive capabilities for possible eventual use could be perceived as an imminent attack. Because much of what goes on in cyberspace is invisible, what one state perceives as normal operating procedure, another could perceive as just about anything.
Because much of what goes on in cyberspace is **invisible**, what one state **perceives** as normal operating procedure, another could perceive as just about **anything**.

Difficulties of attribution can muddle an already confused situation. Knowing who actually does something in cyberspace can be quite difficult. The fact that numerous attacks can be traced to the servers of a specific country does not mean that the country launched an attack or even that it originated in that country. Even if it did originate there, this fact does not mean that the state is complicit. The attack could have been launched by a cybercriminal cartel that took over local servers, or some third party could have wanted it to look as though the state launched an attack.

A great deal depends on whether other states are perceived as basically aggressive (and must be stopped) or defensive (and can be accommodated). During the Cuban missile crisis, many of President John F. Kennedy’s advisers thought they saw another Munich 1938: A failure to respond forcefully would embolden the Soviet Union, discourage allies, and sow the seeds for a later confrontation when the United States would be in a worse position. President Kennedy, however, saw the potential for another Sarajevo 1914; he carried Barbara Tuchman’s *Guns of August* around with him, urging his advisers to read it. His perception shows great concern with stumbling inadvertently into a nuclear war because one side’s moves caused the other side to react in a hostile manner, forcing the first side to react accordingly, and so on.

In the past 20 years, there have been plenty of instances of cybercrime and cyberespionage. But there have been only three and a half cyberattacks that could conceivably rise to the level of a cyberwar: the 2007 attacks against Estonia, similar attacks on Georgia in 2008, the Stuxnet worm directed at Iranian nuclear facilities in 2009–2010, and what may have been a cyberattack on Syrian radar prior to an Israeli air strike on a supposed nuclear reactor in 2007. Of these, all but one (Stuxnet) was unaccompanied by physical violence. In part for this reason, none of these engendered a genuine cyber crisis.

In the future, however, a crisis can start over nothing at all. Because preparations for cyberattack are often generally invisible (if they are to work), there is little good evidence that can be offered to prove that one state is not starting to attack another. A state may try to assuage fears touched off by otherwise unmemorable incidents by demanding proof that the other side is not starting something. If proof is not forthcoming (and what *would* constitute proof, anyway?), matters could escalate.

In such cases, states should take the time to consider escalation carefully. There is little to be gained from an instant response. Cyberattacks cannot disarm another side’s ability to respond in kind. Each state should also anticipate the other side’s reaction to escalation, particularly what others may infer about one’s intentions. In cyberspace, as political scientist Barry Posen has written, “the defender frequently does not understand how threatening his behavior, though defensively motivated, may seem to the other side.”

Consider what happens when a state’s preparation level unexpectedly rises. Perhaps the security folks have just won their bureaucratic argument against the laissez-faire folks. System administrators could be reacting to a news item, such as discovery of the Stuxnet worm. Maybe some laboratory demonstration revealed how vulnerable the state’s key systems were—or, conversely, how easy it would be to secure them if new technologies were employed. But potential adversaries may have no insight into which motivations were present. They might assume that whatever the suddenly better-defended state does is all about them. Thus, they reason, such preparations can only be prefatory to attack. This might lead a potential adversary to attack first or take other actions that are interpreted by the presumed soon-to-be attacker in the worst way. Crisis follows.
As in the physical world, what one state regards as standard operating procedure may be interpreted as anything but by another state. But in cyberspace, two factors exacerbate the problem. First, because states constantly penetrate one another’s computer networks, they can observe many things about each other, but only in partial ways, which could lead to false conclusions and miscalculations. Second, cyberwar is too new and untested for a universal set of standard operating procedures—much less a well-grounded understanding of another state’s standard operating procedures—to have evolved.

For all these reasons, cyberwar may not be seen as it actually is, and states may react out of fear rather than reflection. An action that one side perceives as innocuous may be seen as nefarious by the other. Fortunately, mistakes in cyberspace do not have the potential for catastrophe that mistakes in the nuclear arena do. Unfortunately, that fact may prevent leaders from exercising their normal caution in crisis circumstances. Paradoxically, although the systemic features of cyber crises lend themselves to resolution (there is little pressure to respond quickly, and there are grounds for giving the other side some benefit of the doubt), the fretful perceptions of cyberoperations as they opaquey unfold may drive participants toward conflict.

Cautionary Guidelines
To manage crises and forestall their escalation in cyberspace, the following seven points may be usefully kept in mind.

The first is to understand that the answer to the question—Is this cyberattack an act of war?—is a decision, not a conclusion. Even if cyberwar can be used to disrupt life on a mass scale, it cannot be used to occupy another nation’s capital. It cannot force regime change. No one has yet died from it. A cyberattack, in and of itself, does not demand an immediate response to safeguard national security. The victim of a cyberattack could declare that it was an act of war and then go forth and fight—or the victim could look at policies that reduce the pain without so much risk, such as by fixing or forgoing software or network connections whose vulnerabilities permitted the cyberattack in the first place.

Second is to take the time to think things through. Unlike with nuclear war, a nation’s cyberwar capabilities cannot be disarmed by a first strike. There is not the same need to get the jump on the other guy—or to match his offense with your offense when it is your defense that dictates how much damage you are likely to receive.

Third is to understand what is at stake—which is to say, what you hope to gain. With cyberattack, what you are trying to prevent is not the initial attack but the next attack, the effects of which might be larger than the initial attack but might also be smaller. (The latter is particularly true if the initial attack teaches the victims that, say, making industrial controls accessible to the Internet may not have been the smartest idea.)

Fourth is not to take possession of the crisis unnecessarily. That is, do not back yourself into a corner where you always have to respond, whether doing so is wise or not. It is common, these days, to emphasize the cost and consequences of a cyberattack as a national calamity. Having created a demand among the public to do something, the government is then committed to doing something even when doing little or nothing is called for. Emphasizing the pain from a cyberattack also fuels the temptation of others to induce such pain. Conversely, fostering the impression that a great country can bear the

Perhaps more than any other form of combat, cyberwar is storytelling—appropriately for a form of conflict that means to alter information.
pain of cyberattacks, keep calm, and carry on reduces the temptation.

Fifth is to craft a narrative that can take the crisis where you want it to go. Narratives are morality plays in which events take their designated place in the logical and moral scheme of things: “We are good, you are bad”; “we are strong and competent, unless we have stumbled temporarily because of your evil.” Narratives also have to find a role for the attacker, and the development of such a role may, in some cases, encourage the attacker’s graceful and face-saving retreat from belligerence. After all, the odds that an attack in cyberspace arises from miscalculation, inadvertence, unintended consequences, or rogue actors are nontrivial. Perhaps more than any other form of combat, cyberwar is storytelling—appropriately for a form of conflict that means to alter information.

Sixth is to figure out what norms of conduct in cyberspace, if any, work best. In March 2013, the United States and China agreed to carry out high-level talks on cyber norms. Particularly useful norms are those that can be monitored before any war starts. These include norms that pledge nations to cooperate in investigating cybercrimes, that sever bonds between a state and its hackers or commercially oriented cybercriminals, and that frown deeply on espionage on networks that support critical public services (such as electrical power). Working toward useful norms may well help reduce the likelihood of a crisis, but it would be unrealistic to believe that they can eliminate the possibility.

Seventh is to recognize what a crude tool counter-escalation may be for influencing the other side. In cyberspace, what the attacker does, what he thinks he did, and what the defender thinks he did may all be different. Then there’s the similar difference between the defender’s response and the attacker’s perception of what was done in return. The attacker may think the retaliation was proportional, was understated, or went overboard in crossing red lines—red lines presumably not crossed by himself. The effect is akin to playing tennis on a rock-strewn court.

In sum, while it is worthwhile to prevent what some have characterized as a “future 9/11 in cyberspace,” similar levels of care and thought need to be given to how to manage a potential 9/12 in cyberspace. If not, countries may find, as with the historical 9/11, that the consequences of the reaction and counter-reaction are more serious than the consequences of the original action. ■

The effect is akin to playing tennis on a rock-strewn court.

Related Reading


*Managing September 12th in Cyberspace*, Martin C. Libicki, CT-384, 2013, 6 pp., testimony presented before the House Foreign Affairs Committee, Subcommittee on Europe, Eurasia, and Emerging Threats, on March 21, 2013, web only: www.rand.org/t/CT384
Military Sexual Assault Inflicts Physical, Psychological, Financial Pain

By Coreen Farris, Terry L. Schell, and Terri Tanielian

Coreen Farris and Terry Schell are behavioral scientists
and Terri Tanielian is a social research analyst at the RAND Corporation.

AWARENESS of sexual violence within the U.S. military has grown over the past decade. In the year following the 2005 implementation of a new reporting system within the U.S. Department of Defense, reports of military sexual assaults—which include rape, forcible sodomy, and other unwanted sexual contact that is aggravated or abusive—grew by 30 percent.

The new reporting system gives servicemembers the option of filing either unrestricted or restricted reports. When an unrestricted report is filed, it is provided to law enforcement for investigation, and the victim’s commander is notified. This was the only option available to victims prior to 2005. Under the new system, reports may be filed as restricted, meaning that they are kept strictly confidential; they are not released to commanding officers, and no investigation is launched. Both types of reports allow victims to record a complaint and to receive medical and other supportive services.

However, many victims still choose not to disclose their experiences because they do not want anyone to know about them, are uncomfortable making a report, do not believe that their report will be kept confidential, or fear retaliation. In short, the reported incidents are likely to substantially underestimate the true number of sexual assaults in the military.

In fiscal year 2012, a total of 3,374 U.S. servicemembers formally reported that they had been victims of a sexual assault, representing about 0.2 percent of all servicemembers. But Pentagon officials believe that the total number of formal reports represents a mere fraction of all the assaults committed. In May 2013, the Pentagon released a study estimating, based on extrapolations from a survey of active-duty men and women, that 26,000 people in the military were sexually assaulted in fiscal year 2012.

Among the reports that were filed, only the unrestricted reports provide demographic details about the perpetrators and victims. The unrestricted reports from fiscal year 2012 indicate that 78 percent of incidents involved a servicemember victim and at least 84 percent involved a servicemember perpetrator (see the pie charts). One-quarter of the perpetrators were in the victim’s chain of command.

Sexual assault victims experience physical injuries and increased risk for sexually transmitted infections, human immunodeficiency virus, pregnancy, posttraumatic stress disorder, and other psychological health problems. U.S. Department of Defense guidelines for the care of these victims appear to be well matched to civilian recommendations for care. An important next step will be to evaluate the extent to which the care that victims actually receive—including medical care, forensic services, advocacy and support services, and mental health care—matches the departmental directives for the care they ought to receive.

Everyone Pays

Sexual assaults result in costs for society as well as consequences for the individual victims. In the civilian sector, the average immediate medical cost for those who seek care is $2,084, with victims paying about 30 percent out of pocket. In addition to these immediate costs, medical care utilization grows by 56 percent annually after an assault, and this increased utilization persists for at least three years following the event. About one-third of rape victims also seek mental health services, and for those who do, the average total cost is $978, with the victim bearing 34 percent of that cost.

In addition, victims lose an average of 8.1 paid work days and 13.5 unpaid household labor days per assault. Lost productivity at work and in domestic tasks has been estimated at 1.1 million days annually. Assuming mean daily earnings of $95, the loss to the economy is $104.5 million annually.

Beyond the tangible financial costs, there are intangible ones that drive the total costs of sexual assault higher. After an inflation adjustment, the total cost of each assault has been calculated to be...
$138,204 in 2012. Multiplying this amount by the U.S. Department of Defense estimate of disclosed and undisclosed cases of military sexual assault in 2012 suggests that their total cost to U.S. society in that year alone was on the order of $3.6 billion.

Sexual assault during military service may differ from civilian assaults in a number of important ways. The nature of military service and its emphasis on loyalty and community may result in servicemembers experiencing a heightened sense of shock and betrayal when a colleague perpetrates the offense. Although male servicemembers are less likely to report an incident than are female servicemembers, the greater proportion of men in the military overall means that over half of military sexual assault victims will be male. Finally, when a servicemember is assaulted from within the chain of command, he or she may have no route by which to escape the situation and may remain vulnerable to repeated assaults and other abuses. There could be a harmful influence on career trajectories, and retention might decline.

When a servicemember is assaulted from within the chain of command, he or she may have no route by which to escape the situation.

In Reported Cases of Military Sexual Assault, Most Perpetrators and Most Victims Were U.S. Servicemembers

Above left: Veterans Kori Cioca, of Wilmington, Ohio, and Panayiota Bertzikis, of Somerville, Massachusetts, who were assaulted and raped while serving in the U.S. Coast Guard, are plaintiffs among several women and at least one man who are suing Pentagon officials, seeking change in the military’s handling of rape and sexual assault cases.

Above right: Brian Lewis, former U.S. Navy Petty Officer Third Class, testifies at a U.S. Senate hearing on military sexual assault on March 13, 2013. Lewis said he was raped in 2000 by a superior officer and was ordered not to report the crime. The greater proportion of men in the military overall means that over half of military sexual assault victims will be male.

NOTE: Percentages are based on “unrestricted” reports, the only form of reporting that provides demographic details about the perpetrator and victim. “Restricted” reports are kept strictly confidential.
Multiple barriers stand between servicemembers who have been sexually assaulted and their access to psychological health care.

Inadequate Defenses

Multiple barriers stand between servicemembers who have been sexually assaulted and their access to psychological health care, as evidenced by long wait times for those seeking care, shortages of well-qualified mental health service providers, and a limited availability of care in rural regions. Active-duty personnel are often unable to take time off during standard work hours to seek care. Worries about confidentiality may prevent some from doing so. Servicemembers report concerns that they will appear weak to leadership and that seeking help will harm their careers. Concerns about the availability of mental health records to the chain of command may be particularly problematic for victims, given that the perpetrator is within the victim’s chain of command in about a quarter of the cases.

Since 2005, the U.S. Department of Defense has worked to raise awareness of sexual assaults, to prevent future assaults, and to ensure that victims have access to an array of medical care, mental health, and legal services. The defense department should now consider several projects to help monitor the effectiveness of these efforts, to direct the provision of services, and to identify promising intervention or prevention strategies.

These projects could include a formal, anonymous survey of a representative sample of servicemembers to estimate the true extent of sexual assault across the services. The survey should be conducted by an outside entity to reduce fears that the responses may not be kept confidential. Other projects could include a needs assessment of disclosed and undisclosed victims, an evaluation of training programs for sexual assault prevention and response, and an evaluation to document the extent to which the directives requiring immediate, evidence-based care for victims are being implemented with fidelity.

Former Secretary of Defense Robert Gates has said: “The department has a no-tolerance policy toward sexual assault. This type of act not only does unconscionable harm to the victim; it destabilizes the workplace and threatens national security.” Establishing an environment that does not tolerate sexual violence is likely to be an iterative process with multiple cycles of policy recommendations, directives, implementation, scientific research, and further recommendations. Such a process has the potential to reduce the incidents of military sexual assaults and to minimize the damage they cause.

Related Reading

Physical and Psychological Health Following Military Sexual Assault: Recommendations for Care, Research, and Policy, Coreen Farris, Terry L. Schell, Terri Tanielian, OP-382-OSD, 2013, 24 pp., www.rand.org/t/OP382
If there is a commercial pot industry, businesses will have strong incentives to create and maintain the heavy users who use most of the pot. To get a sense of what this could look like, look no further than the alcohol and tobacco industries, which have found ingenious ways to hook and reel in heavy users.

Beau Kilmer, codirector of RAND’s Drug Policy Research Center, in USA Today online, April 23, 2013
The Opposition Forces

“What is required in Syria now is a program like the one the United States established in the mid-1990s to train and equip the armed forces of the Bosnian Federation. One of the goals was to eradicate Iranian and foreign radical influences from Bosnia. The leverage that the program gave the United States with the Bosnian government made it possible to achieve this objective. The Bosnian experience provides a relevant template for Syria today, but time is running short. It is critical to establish as soon as possible a task force to organize and supervise a train-and-equip program for the Syrian opposition forces.”

Angel Rabasa, currently a political scientist at the RAND Corporation and formerly a member of the Bosnia Train and Equip Task Force of the early 1990s, in U.S. News & World Report, May 22, 2013

The Chemical Weapons

“The lessons of the attack and disarmament of Iraq’s chemical weapons in the First Gulf War suggest that chemical weapons are hard to find and destroy. Lots can survive even a sustained attack. Moreover, those that remain will present a disposal operation of industrial scale and environmental concern. There is no reason to believe that the U.S. is better able to deal with chemical weapons in Syria today than it was with chemical weapons in Iraq in 1991. It will take several years—as it did in Iraq—to accomplish the destruction. During that time the material must be adequately secured by reliable forces.”

James Quinlivan, international policy analyst, on GlobalSecurity.org, May 22, 2013

The Diaspora

“Syria’s sizable émigré community has so far remained far away from the devastation, waiting in cities like Paris and London to see where the political chips will fall. But, by taking a more active role, the diaspora can help to end the conflict at home and to rebuild in its wake. Syrians abroad have an important opportunity—and responsibility—to help end the violence and contribute to the country’s political, economic, and social renewal.”

Wasif Syed, Middle East analyst, for Project Syndicate, May 22, 2013

Killer Mutant Viruses

“Authorities have to be ready for a possible worst-case scenario, if an especially deadly flu virus like H7N9 mutates to become easily spread from human to human. This could happen at any time if human and animal flu viruses get a chance to ‘mix and match’ in a person or in some types of animals, and if one resulting mutant form packs both the killer potential of the bird flu and the contagiousness of human influenza. That could be the spark for a new and deadly flu pandemic.”

Melinda Moore, natural scientist, on the Asia Healthcare Blog, May 10, 2013

Separate Beds?

“For women, marital strife can lead to a sleepless night; for men, a sleepless night can lead to marital strife. These interactions can create a vicious cycle. On nights when couples sleep together, they tend to have more fragmented or restless sleep than nights when they sleep alone. Should couples sleep together or sleep apart? Couples need to decide what works best for them and consider how to optimize their sleep as well as their time together.”

Wendy Troxel, Clinical Psychologist and Behavioral Scientist, on ABC News, May 20, 2013
Healthy Food Policy

“For two decades, subsidies to farmers have helped make corn and soy increasingly cheaper than fruit, vegetables, and whole grains. Food companies have built entire brands based on these cheaper commodities, which make up the raw material for a range of unhealthy processed foods and animal feed. If Americans don’t want to be forced to pay more for unhealthy foods, perhaps we should flip the logic on its head: Reduce the cost of healthy foods. Lowering the costs of healthy foods in supermarkets not only increases the amount of fruits, vegetables, and whole grains that people eat, but it also seems to reduce their consumption of less nutritionally desirable foods.”

Roland Sturm, economist at the RAND Corporation, and Derek Yach, executive director of the Vitality Institute, in Modern Healthcare, May 25, 2013

An Energy-Independent United States

“I would like to put a question mark at the end of the title today, because I’m going to, in some ways, debunk the importance of energy independence. We’ve seen a really healthy energy industry in the United States, especially in the past five years. Even though we’re drilling and producing more oil, it’s not going to make any difference to you in terms of the effect it has on the price at the pump, because oil is a global commodity, and the price is set by increased numbers of cars in China or increased demand in India or elsewhere, no matter how much oil we’re producing in the states. Even if by some big surge in production we would end up actually being an oil exporter again, it’s not going to really affect that price you face at the station.”

Keith Crane, director of RAND’s Environment, Energy, and Economic Development Program, on RAND’s “Events@RAND” podcast

To Libya via Sierra Leone

“By adopting a laissez-faire policy toward security in Libya after the war, the United States and its allies who helped the Libyan rebels topple [Muammar] Gadhafi share in the responsibility for the country’s current predicament. The best thing the United States and its allies can do now is to deploy a small team to train and equip a Libyan security force that is loyal to the government in Tripoli. Such a force might be roughly modeled on the successful British effort in Sierra Leone, which trained a cadre of several thousand soldiers with only a few hundred British officers in 2000 and 2001.”

Christopher S. Chivvis, political scientist, on CNN.com, May 13, 2013

Innovation Versus Bureaucracy

“Innovation is the antithesis of bureaucracy. This tension between bureaucracy and creativity is not unique to the European Commission. Innovation is about people, not process, and innovators need to operate in a free-thinking, entrepreneurial, risk-taking society to deliver.”

Jonathan Grant, research fellow, and Rebecca Helen Schindler, policy analyst, at RAND Europe, on The RAND Blog, March 13, 2013
HOW THE GREAT STATE OF ARKANSAS MAY FARE UNDER THE AFFORDABLE CARE ACT

401,000 more Arkansans with health insurance

30% more non-elderly Arkansans with Medicaid

1,100 deaths prevented annually by the increase in Medicaid enrollment

6,200 new jobs created by economic growth stemming from insurance expansion

$550M in net economic growth, accounting for subsidies, Medicaid expansion, taxes, and Medicare cuts

These calculations reflect likely conditions in 2016, given a fully implemented Affordable Care Act.


HOW THE COMMONWEALTH OF PENNSYLVANIA MAY FARE UNDER MEDICAID EXPANSION

830,000 more Pennsylvanians with health insurance

5% more non-elderly Pennsylvanians with Medicaid

net annual economic growth for the state, accounting for subsidies, Medicaid expansion, taxes, and Medicare cuts

$3.5B

35,000 JOBS retained by economic growth stemming from Medicaid expansion

$180M cumulative increase in state spending between 2014 and 2020

Unless otherwise noted, these calculations reflect likely conditions in 2016, given a fully implemented Affordable Care Act.

The Value of Perspective, in Dollars and Cents

By Michael D. Rich

Michael D. Rich is president and chief executive officer of the RAND Corporation.

At every level today, budgets are being sliced, squeezed, molded, and stretched. Whether at the kitchen table, in the boardroom, or inside the beltway, “doing more with less” is a common refrain. Yet, making sensible budget reductions is a complex and demanding task, one that can’t succeed without informed perspective—in other words, an evidence-based understanding of the true value of each and every investment, relative to overall objectives.

For the government organizations responsible for U.S. national security, this is especially important. Ill-conceived cuts and reductions can put lives at risk and usually require many years to rectify. That is why across-the-board cuts like the ones mandated under sequestration are so risky. As my RAND colleagues Stu Johnson and Irv Blickstein wrote in the previous issue of this magazine, a better approach would begin with “a prioritization of defense challenges and the risks we are willing to accept, with program and budget decisions following.”

For decades, RAND researchers have worked with the U.S. military services and other parts of the U.S. Department of Defense to strengthen the country’s national security capability while also reducing costs. The informed perspective realized from this kind of rigorous analysis makes a big difference when budgets are tallied—pointing the way to better choices about what to develop, where personnel force management can be made more efficient, and how to reengineer important combat support processes.

For instance, RAND Project AIR FORCE analysis showed that the U.S. Air Force could meet its intra-theater airlift needs more cost-effectively by procuring C-130J-30 aircraft rather than the smaller C-27J transport planes to replace the capability being lost as a result of C-130E retirements. The analysis also showed that this option was more cost-effective than conducting a service life extension program on the C-130E aircraft. The Air Force adopted RAND’s recommendation, with estimated savings of $17 billion over the life of these systems. Also, a congressionally mandated study of the cost-effectiveness of modifying the Air Force’s fleet of KC-135R/T and KC-10A tankers to add winglets—vertical additions to wing tips designed to improve fuel efficiency—found that the modification would offer some performance improvements but was not likely to reduce operating costs under most circumstances. Our recommendation against adding winglets enabled the Air Force to avoid costs of between $1 billion and $2 billion.

A RAND National Defense Research Institute analysis of how the U.S. Navy manages its public shipyards in the face of peaks and troughs in demand revealed that the Navy could save hundreds of millions of dollars per year by changing the mix of permanent resident workers and various kinds of temporary workers.

And when the cost of flying supplies to Iraq skyrocketed, the U.S. Army asked the RAND Arroyo Center to take a look. The analysis showed that a new algorithm could enable better decisions about which equipment to preposition in theater and which to retain in the United States. The Army and the Defense Logistics Agency adopted our recommended process and algorithm. Since 2004, the savings have approached $1 billion.

Sometimes, analysis points to actions with the potential to generate new savings into the future—such as when the RAND Arroyo Center recommended that the Army establish a venture capital fund to gain greater access to emerging technologies. With $25 million in seed money, the Army founded OnPoint Technologies. OnPoint’s first success was the development of a low-cost charge indicator to get more use out of one of the Army’s most often-deployed non-rechargeable batteries. The result: a $400 million saving.

We’ve collected examples like these and many others in a feature titled “Saving the Government Money” to highlight how improved processes, better personnel decisions, smart modernization, and the selective application of new technologies can add up to billions of dollars in savings for the Pentagon—and has already. All of this was made possible by independent, careful research and analysis conducted, in some instances, over many years. As government entities face down staggering budget realities, decisionmakers needing to do more with less will be best served by applying an informed perspective. Rigorous and objective analysis is the place to start. ■

As government entities face down staggering budget realities, decisionmakers needing to do more with less will be best served by applying an informed perspective. Rigorous and objective analysis is the place to start.
Renewing Communities and Building Resilience

With decades at the forefront of research on emergency planning, risk management, public health, and flood control, RAND is a global resource on community resilience in the aftermath of natural and man-made disasters. After Hurricane Katrina, RAND research and analysis supported recovery and long-term economic development in the U.S. Gulf States. More recently, RAND experts developed a planning tool to determine the capabilities and resources a community will likely require in the event of a disaster such as an earthquake, hurricane, tornado, terrorist attack, or flu pandemic. RAND is now pursuing research to identify and promote laws and programs that reduce the economic consequences of such catastrophes by enabling individuals, communities, and businesses to remain productive and receive the compensation they need to recover.

Disasters strike without warning. Philanthropic contributions help make sure that RAND is always ready to respond.

To learn more about how giving to RAND can make a difference, visit www.rand.org/giving
“I care about future generations—making sure that individuals live, with dignity, in a safe and secure world. That means we must create innovative, multi-regional solutions for a range of social and economic challenges, from poverty and education to food distribution and public health. The Pardee RAND Graduate School encourages the best and brightest students from throughout the world to think outside the box and to confront the big issues. I know that, with students and RAND researchers working together, we can help improve the future human condition.”

Generous contributions from donors such as FREDERICK S. PARDEE enable RAND, a nonprofit institution, to fund groundbreaking research in the public interest.

Frederick S. Pardee, a former RAND researcher, recently contributed $3.6 million to support the Pardee RAND Graduate School and to create its Pardee Initiative for Global Human Progress. This initiative draws on the talent and innovation of Ph.D. candidates and RAND research staff while leveraging RAND’s work in international development. Mr. Pardee contributed $10 million to RAND’s graduate school in 2003 to support the education of future policymakers, and the school was named in his honor. The Pardee RAND Graduate School is the largest public policy analysis Ph.D. program in the United States and the only program based at an independent public policy research organization.