How the United States Can Win the Cyberwar of the Future

Cold War–era deterrence theory won't cut it anymore.

BY P.W. SINGER | DECEMBER 18, 2015

There is perhaps no national security problem more 21st century in both its definition and form than cybersecurity. And yet to solve it, the ready solution in nearly every U.S. national security conversation today is that tried and true 20th-century framework of deterrence.

The conventional wisdom echoes back to the Cold War, the last period of long-term conflict. It argues that the best way to stop the frustrating array of cyberattacks on the United States — ranging from credit card theft, to emails stolen from Hollywood studios, to the millions of security clearance records lifted from the Office of Personnel Management (OPM) — is to demonstrate the capability and willingness to hit back just as hard. This rhetoric of Cold War deterrence by retaliation is appealing not just in its simplicity, but also because it seemingly demonstrates strength and resolve. It pervades the U.S. body politic, has become a staple of presidential candidate statements, and has appeared in multiple debates. Consider Republican presidential candidate Jeb Bush's call for the use of "offensive tactics as it relates to cybersecurity [to] send a deterrent signal to China," or Sen. Lindsey Graham's (R-S.C.) promise at a recent debate: "Make me commander in chief and this crap stops."

Likewise, on Capitol Hill, the same idea of returning to visions of Cold War-style deterrence holds sway. Chairman of the House Foreign Affairs Committee, Rep. Ed Royce (R-Calif.) angrily lamented the absence of a coherent national cyber-deterrence strategy and demanded "why aren't we hitting back?" Some of his Senate counterparts, including John McCain (R-Ariz.), agree. President Barack Obama is failing in his job as commander in chief by not doing "his part to deter the belligerence of our adversaries in cyberspace," McCain said in August.

But the search for cyber-deterrence by overwhelming response is no partisan issue: Indeed, it may be one of the few bipartisan areas of foreign policy today. "We need to figure out when we're going on an offensive," Rep. Adam Schiff (D-Calif.), the top Democrat on the House Intelligence Committee, said after the discovery this summer of the massive OPM breach.

Those working for Obama in the executive branch talk about deterrence in much the same way. U.S. cyber forces need to "increase our capacity on the offensive side to get to that point of deterrence," said Adm. Mike Rogers, the head of the National Security Agency and the U.S. military's Cyber Command. The Defense Department has created a task force on cyber-deterrence, and the director of the Pentagon's Defense Advanced Research Projects Agency (DARPA), Arati Prabhakar, said recently that her organization's priority is to find ways for the United States "to be able to hurl back" in cyberspace.

There are just two problems with returning to old school models of deterrence for the new school problem of cybersecurity. First, that model has the utterly unrealistic goal of a world without cyberattacks. And second, no matter how mad the United States gets, MAD — or mutually assured destruction — in cybersecurity isn't going to happen.

In other words, whacking back to end hacking certainly sounds appealing. But it is not going to work. This is a new era, and U.S. deterrence thinking needs to reflect that.

Not your grandfather's deterrence

In the Cold War, both sides possessed roughly the same nuclear weapons, and these weapons affected them both in roughly the same way. The attack to be deterred was the one that assured mutual and equal destruction in a massive mushroom cloud. Building up a potent offense, and being able and willing to use it before it was too late, translated directly into deterrence.

Today, there is no "mutual" to balance, let alone assured destruction. The United States is arguably more vulnerable to cyberattack than any of its adversaries, largely because of its wide commercial and cultural dependence on the Internet. (This is, on balance, a good thing: North Korea, for instance, may be the world's least vulnerable nation to cyberattack, but at the cost of global isolation, dictatorship, and an economy whose most important recent advance is army-run pig farms.)

There is also an inverse relationship to conventional strengths. Underpinning Cold War deterrence strategy was that the United States perceived itself weaker than the Soviet Union in conventional warfighting, and so relied on the threat of nuclear response to avoid an unequal conventional war. Today, it is the United States that has the conventional edge on its adversaries, and thus many of its attackers see cyberattacks as their asymmetric way to work around a power imbalance.

The timing is also fundamentally different. The physics of a ballistic missile's speed and arc determined the way people thought about deterrence during the Cold War. The critical 30 minutes it would take an intercontinental missile to fly across continents was essential to planning and strategy.

In cybersecurity, however, time operates by different rules. While cyberattacks seemingly move at digital speed, they actually can take months or years to plan, organize, conduct, and — most importantly — detect. An attacker often carries out long periods of preparation and intelligence gathering, all with the goals of gaining and keeping entry. The alleged Chinese OPM hacks that stole sensitive data of over 21 million Americans may be on policymakers' minds now, but they actually started as early as March 2014. Indeed, the average time it takes a victim to detect that they have been breached is 205 days. In its study of APT1, a hacking campaign linked to the Chinese People's Liberation Army (PLA) Unit 61398, the security firm Mandiant found that the unit spent as long as five years undetected inside several of its targets' networks.

The timeline of reaction is also fundamentally different. As opposed to the need to act within the tight, 30-minute window of Cold War missiles, in cybersecurity the defender's best move may well not be to strike back as rapidly as possible, but to show no outside awareness of the ongoing attack. This complicates the attacker's damage assessments. It even allows the victim to turn the tables and steer the attacker into areas where it cannot do harm, or where the victim can feed the attacker false information.

The weapons also come with different timelines — not just in their creation, but also in their utility. The Minuteman intercontinental ballistic missile (ICBM) was conceived in 1956, and served as the center of U.S. nuclear deterrence for the next three decades of the Cold War. But its utility didn't stop there. Indeed, roughly 450 Minuteman III missiles still protect the United States today, with plans for them to serve to 2030 or even beyond. By contrast, most cyberweapons depend on "zero days" — vulnerabilities the victim isn't yet aware of. What is thus potent today, a single software patch can render inert tomorrow.

The differences do not stop here. There is not just the lack of mutuality in weaponry, impact, or time, but also in the players of the game itself. The actors who the United States is supposed to be cyber deterring are far more diverse than an enemies list that included only the Soviet Union. More than 60 countries have cyber-military capabilities, ranging from large and powerful states to weak regimes. Nonstate actors — from transnational criminals to hacktivist networks to proxy groups taking advantage of the gray space in between — also play in the same game. Moreover, it is not just the different numbers, but that each actor comes with vastly different interests and stakes in the game: Akin to terrorism or crime, some players are deterrable, and some are not.

As diverse as the players are, so too are the attacks they might carry out. Those vary from theft of intellectual property to online dumps of embarrassing Hollywood studio emails, to the (not yet realized) risk of a massive kinetic attack on critical infrastructure, using Stuxnet-style digital weaponry to collapse power grids or transportation networks. So when people like McCain argue that "the level of deterrence is not deterring," they are both right and wrong. Not every kind of attack is being thwarted, yet the worst kind of attack that major states are capable of are indeed being deterred.

While attribution is often identified as a key problem in cybersecurity discussions — unlike an ICBM, a cyberattack doesn't emit a clear plume of smoke to identify the attacker — the existence of diverse attackers and diverse attacks further muddies the water: It can be incredibly complicated to determine the intent of an attack, even if its form and sender are known. When a Russian criminal group with ties to Russian intelligence was detected attacking U.S. banks in 2014, for instance, the security community debated whether it was regular old cybercrime, or an attack linked to Russian state interests, designed as a response to the sanctioning of the regime for its invasion of Ukraine. But even then, was the attack a retaliation that got caught? Or was it akin to a nuclear test in a crisis, a signal intended to be detected, a warning of greater consequences if the United States pushed further?

The problem of comparison does not stop there. Unlike in the Cold War, some attacks that target the United States are the kind of attacks it would actually like to carry out itself, or, in fact, already does. Military and administration officials have reacted relatively mildly to the OPM email breach. Why? In part, because attacks targeting a government agency's networks are the bread and butter of the online espionage operations the United States carries out against other governments. As Director of National Intelligence James Clapper said in June after the discovery of the OPM attack, "You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute." Or as Deputy Secretary of Defense Bob Work said recently about cyber-espionage, "If you ain't cheating, you ain't trying."

Perhaps where the Cold War parallels fall short the most is the idea that building up offensive capabilities will deliver deterrence. This is a constant refrain: not just the need to build up U.S. cyber offense, but the need to make sure others know the United States has those capabilities. As James Cartwright, the four-star Marine Corps general who led much of the initial U.S. strategy in cyber issues until his retirement in 2011, said, "You can't have something that's a secret be a deterrent. Because if you don't know it's there, it doesn't scare you."

The problem is that the evidence disproves this link between building up more cyber-offensive capability as the way to scare off the other side. There is not yet any direct pathway to deterrence the way building up nuclear capability yielded it back in the day. Unlike concerns over bomber and missile "gaps" during the Cold War (which notably turned out to be wrong), the United States' hugely superior position in cyberspace has never been in question. And for anyone somehow in doubt, there were the series of Washington policymakers' leaks designed to take credit for Stuxnet, the cyberattack that successfully slowed Iran's nuclear program and showed off a whole new class of cyberweapon. Then came Edward Snowden's dump of thousands of NSA documents**.** While Snowden's disclosures obviously angered his former employers, they also show that the folks at Fort Meade have much to be proud of. They have developed unmatched, amazingly exotic capabilities, from a mindboggling scale of global monitoring devices to new classes of cyberweapons that use radio signals to jump software over the previously protective physical divides between systems. And the leaks show the capability is not mere lab work, but that the NSA has used them in operations against targets ranging from Iranian nuclear research facilities to Chinese command networks.

Yet despite this offensive capability and the demonstration of its potency, attacks on the United States have only grown, in both number and intensity. In the year after the Snowden leaks proved the United States' offensive prowess, there was 55 percent more confirmed data breaches than the year before — and that doesn't even include the operations targeting major government sites like OPM or the Pentagon's Joint Staff network.

The problem is not with deterrence theory, or with cyberweapons' offensive utility, but that too many people are trying to peel off the bumper-sticker version of complicated Cold War debates on deterrence and apply them to a more complicated present and future. So what to do instead? Here are the three better ways for the United States to draw the right lessons from the Cold War and create better and more obtainable cyber-deterrence goals.

Set the norms

There is a huge value in delineating clear lines of behavior. During the height of the Cold War, the superpowers may have been a button press away from thermonuclear annihilation, but they still found a way to agree on certain norms. Sometimes these were formal arms treaties; other times they were tacit codes of conduct that guided everything from limiting spy-on-spy killings to avoiding interference with nuclear commands, all with the goal of avoiding miscalculations that could unintentionally escalate into outright war.

Yet much of the recent critique of the Obama administration in cyber-deterrence discussions has been of the agreement hammered out this fall between the United States and China to forgo government-enabled attacks on intellectual property. There is much to criticize in this agreement that is not much of an agreement. Beijing is agreeing to not do something it has always denied doing anyway, despite massive evidence it does; and recent reports allege the attacks have continued since the agreement. Even the supposed arrests of a small number of hackers in China for the OPM breach, reported with far more prominence in the United States than in China, is less a clear sign of success than a revelation of how the agreement offers up a new tool to sidestep the issue. Now, when Chinese hackers linked to government-enabled projects are caught, symbolic arrests can be offered up and the matter claimed solved.

It is for this reason that the overwhelming majority of cybersecurity experts don't expect the agreement to stop the attacks. Theft of intellectual property is integral to the Chinese mercantilist economic model. In turn, the United States is wedded to the open flow of information, but Beijing sometimes interprets platforms that share freedom of speech as attacks that threaten its internal stability. And both sides, whose militaries are engaged in an arms race in the Pacific, will of course continue to engage in espionage.

This dynamic makes reaching a formal prohibition on cyberattacks between the 21st-century powers unlikely. It does not mean, however, that there is no value in engagement and norm building. Rather than a treaty or agreement that unrealistically tries to create a Cold War-style regime of deterrence or arms control, the two sides need to flesh out a mutual understanding of the new rules of the game. Each side must understand that its opponent will continue to conduct cyber-activities ranging from espionage to theft. The most important goal is not to stop every cyberattack, but to keep them from escalating into something far more dangerous.

This leads to a fundamental change in the typical deterrence discussion. In the Cold War, everything was targeted, but outright attacks crossed the line. Today, the situation is inverted. While unwanted, some cyberattacks will have to be allowed, while certain targets must be made anathema.

No country wants its state secrets stolen, for example, but it is part of the expected dance of great powers in competition. By contrast, introducing the digital equivalent of a dormant Tasmanian devil into a nuclear power facility's operating system should be off limits to both sides — because both sides will interpret it as an incredibly escalatory step of preparing for war.

Deter through diversity

Nothing above argues against building up offensive capabilities for cyberspace. Cyberweapons have proven their value in espionage, sabotage, and conflict. And the digital domain will be as crucial to warfare in the 21st century as operations on land, air, and sea. Indeed, the cyber front of any war between the United States and China would feature not just military units like Cyber Command or the PLA's Unit 61398, but also nonstate actors that might range from Chinese university cyber militias to Anonymous hackers joining in the fight with their own goals and modes, much as what has happened in the online Islamic State battles.

This is a good illustration of another misperception: Cyberweapons are increasingly useful tools of espionage and war, but they are not comparable to "weapons of mass destruction," where the fear of a single big thermonuclear tit for tat maintained the nuclear balance. Offensive cyber capabilities, by contrast, are a key part of the toolkit to be used in both hot and cold conflicts. They are not the only tools of deterrence, nor will a fear of them make attacks cease.

That a cyberweapon is not like a WMD doesn't mean the United States has no options for exacting costs on would-be attackers to change their calculations. Indeed, it may even have more. Just as the timeline is stretched out and the players are proliferated as compared to the Cold War, true deterrence-building responses can come after the fact and in other realms. For instance, responding to IP theft by stealing back is not the only option: The defender can also go after other assets valued by the attacker or even those valued by third party actors, such as by sanctioning companies benefiting from stolen fruit. This dynamism complicates things to a degree that even the most brilliant Cold War strategist would find frustrating.

The United States will have to game out not merely the first two moves of the response — the simple "shoot and shoot back" dynamic that was the whole of a nuclear exchange — but also multiple stages after that by multiple actors. For instance, anyone advocating for trade sanctions should walk their argument through the process of not just how the sanctions for past attacks would stop future attacks, but also what the United States would do in response to a loss of overall market access were China, say, to respond in kind against some U.S. firms.

Creativity and flexibility will beat simplicity in this dynamic. Indeed, the United States may even steal ideas from one attacker's playbook as a useful tool against another. From Sony to Snowden, leaked emails and documents have been among the most vexing incidents for cybersecurity, but the irony is that the United States' system of government and open society is least vulnerable to them. For all the Sturm and Drang over revelations of questionable metadata collection and Angelina Jolie gossip, U.S. political and social stability has never been at risk from these practices. But, as Catherine Lotrionte at Georgetown University has noted, threatening to reveal the private financial data of a regime's leader, his family, or his allied oligarchs, may be far more potent.

The goal of these measures is not to prevent all attacks, like MAD did with nuclear weapons, but to change the calculus on whether an individual cyberattack is useful.

Shake it off

The third, most apt lesson from a deeper dive into the Cold War deterrence debates is the value not just in raising the costs, but also in limiting the adversary's potential gains. This is known as "deterrence by denial" — making attacks less probable by reducing their likely value. In cybersecurity, this is the magic idea of resilience.

In both strategy and football, sometimes the best defense is a good defense. A half-century ago, strategic planners did not just talk about striking back, but also having "survivable" counter or second strike missiles that would nuke the other side, even if it tried a sneak attack. This is why the United States put missiles on expensive submarines and in hardened silos.

Resilience today is about creating the capacity to power through an attack and shake it off, thereby limiting the gains to the attacker and recovering rapidly from any losses.

Building resilience is not as politically appealing or sexy sounding as striking back with new cyberweapons, because it means accepting that this is a digital world where the risk of cyberattacks is not going away. But it is not only more realistic, but also how the United States would get far more deterrence bang for its buck. Most importantly, it would defend against any kind of attacker and any kind of attack.

Unfortunately, despite the attention, rhetoric, and money the United States government spends on cybersecurity, it is still far from resilient against cyberattack. For every gain, there is still a major gap to be closed. In the military, the construction budget alone for Fort Meade, the combined headquarters of the NSA and Cyber Command, will reach almost $2 billion by the end of 2016, and the force will add another 4,000 personnel, yet the Pentagon's own tester found "significant vulnerabilities" in nearly every major weapons program.

In the broader federal government, the cybersecurity budget for fiscal year 2016 is 35 percent higher than it was just two years ago, yet half of security professionals in these agencies think cybersecurity has not improved in that period. The reasons range from continued failure to follow basic measures — as of June 2015, only about 70 percent of federal employees, for example, have implemented a requirement for personal identification verification cards that dates back to 2004 — to failing to take seriously the long-term nature of the conflict. The exemplar of these failures was the OPM, which dealt with some of the most sensitive government information, and yet outsourced IT work to contractors in China — despite warnings going back to 2009.

In October, the White House issued a post-OPM "Cybersecurity Strategy and Implementation Plan" that describes a key series of steps that every federal agency needs to take over the next 12 months. It included the basic measures that should have been in place long ago: from identifying high-value assets that need to be protected, to accelerating the deployment of detection systems. For all of Congress' talk about the issue — the word 'cyber' appears in the Congressional record 715 times in October alone, 5 times the number for all of 2014 — the role it can play to ensure the implementation of these steps could be the most important thing it does on cybersecurity. Indeed, that will likely matter more than passage of the much ballyhooed cybersecurity information sharing bill, which 87 percent of cybersecurity experts think won't affect the number of major security breaches.

This same uneven implementation plays out across industry. While corporate boards are now talking more about the problem, cybersecurity spending as a portion of IT budgets is still roughly a quarter of the rate within government IT budgets, while the consultancy PricewaterhouseCoopers' report on the state of U.S. cybersecurity described 2015 as the year "progress stalled." The report found that only 25 percent of key industry players, for example, participated in Information Sharing and Analysis Centers, which share needed cyber threat data — the same percentage as in 2014. The outcome is that some sectors like banking take cybersecurity seriously, while others, like health care and infrastructure, remain behind the curve. Indeed, a recent study by the security-ranking firm BitSight Technologies found that some retail and banking companies were better equipped for cybersecurity than even the top defense contractors.

Individuals could also contribute far more to national cybersecurity. During the Cold War, "duck and cover" was about all that a population could do when it came to nuclear deterrence. Today, the vast majority of Americans use the Internet, and they can actually make a difference in its defense. The role for policy is not about mandating basic personal hygiene practices like two-factor authentication on email, or for individuals to use different passwords for their bank account and fantasy football teams. Instead, it is about the role that government can play in cybersecurity in linking citizenry, policy, and markets, just like it does in almost every other realm.

Sometimes government can be a trusted provider of useful information to both business and the wider public. And sometimes it can go further to help shape individual and market incentives. For instance, the Centers for Disease Control and Prevention (CDC) funds research on under-studied diseases, and serves as an exchange for information provided by groups ranging from universities to drug companies. A cyber CDC could meet some of the same needs in cybersecurity.

U.S. buildings are filled with "EXIT" signs and fire extinguishers, while cars have seatbelts and crash bags. These demonstrate the efficacy of creating both voluntary standards and actual regulations to increase security — bolstered by insurance laws and markets to incentivize good behavior and best practices in everything from building construction to driving habits. So, too, the United States should support not merely research on the basic standards of Internet security, but also how to backstop them with the nascent cybersecurity insurance market. If the government can spur that market to further develop, it can potentially have a massively positive effect on national security.

The problem is not only about policy, however, but also about people. Across government and industry, there is a growing lack of cybersecurity professionals; the consultancy Frost & Sullivan estimates that the global gap between security openings and skilled people to fill them will reach 1.5 million by 2020. As of July, for example, 40 percent of the cybersecurity positions at the FBI remained unfilled, leaving many field offices without expertise. (Diversity is also a problem: Roughly 10 percent of cybersecurity professionals are women, lower than the already dismal rates in the broader IT world.)

Creating a "Cybersecurity Human Resources Strategy" by April 2016 is another of the new, and much needed, milestones in the executive branch's post-OPM plan. But it will fail if it only puts new people in old organizational boxes, using the same pipelines. Attracting more talented civilian expertise into the government can aid in an overall national strategy, by supporting deterrence by denial across broader networks. Consider, for instance, that after the embarrassment of the healthcare.gov rollout, Washington created a Digital Service to bring young Silicon Valley innovators into government to do things like fix the federal health care website design. But even after the OPM debacle, there is still not a parallel service to shore up cybersecurity.

Similarly, several National Guard units have been retasked to focus on cybersecurity, and they have performed admirably, even besting some active duty Cyber Command units in wargames. But the new units serve only as a means to organize talent already serving in the military. There is a far deeper and wider pool of talent outside the military — either because they are unwilling to meet the various obligations that come with military service (an IT tech in the National Guard, for example, is obligated to serve in any mission they are ordered to, whether it be a cyber 911, Haiti Earthquake response, or Iraq war) or they are unable to meet the various physical or legal requirements.

During the Cold War nations like Switzerland and China had "active defense" models (another terms that has been wrongly appropriated in cyber debates), based on deterring attack not by massive retaliation but by mobilizing their citizenry for broader national defense . The United States was in a unique position in the Cold War, so it had little to learn from other nations then. But today there is much to learn from others, past and present, as they wrestle with similar problems. The Estonian Defence League's Cyber Unit, for example, is a particularly good model. Akin to the U.S. Civil Air Patrol, where citizens can not only build up their own aviation skills, but also volunteer to aid government in aviation-related emergencies, Estonian citizens volunteer their expertise for cybersecurity. They aid in everything from "red teaming" — finding vulnerabilities in systems and activities before the bad guys can exploit them — to serving as rapid response teams to cyberattacks. Notably, the members are not just technical experts: The needed expertise that lies outside of government is about far more than just computer coding. To defend the national banking system from cyberattack, a mix of hackers and bankers is better than just bankers or hackers.

These efforts have helped turn Estonia from one of the first victims of a state-level cyberattack, when Russian hackers partially shut down the country in 2007, to perhaps the best-equipped nation in the world to weather one now. Estonia may not have the same capabilities as the NSA and Cyber Command, but it does have deterrence by denial and an involved populace — giving it arguably better cybersecurity than the United States.

The lesson from Cold War deterrence that best holds true today is that the most dangerous period was when both the new technology and the new competition were not well understood — which made bluster and escalation seemingly easy remedies to complex problems. Fortunately, cooler heads prevailed and both sides built up a system that delivered actual deterrence.

The United States can build a new set of approaches designed to better its cybersecurity position, while reshaping adversary attitudes and options. Or, it can keep talking tough and simple about cyber-deterrence, and continue to be a victim.

Photo credit: Thomas Trutschel/Photothek via Getty Images

MORE FROM FOREIGN POLICY

NFANTRY BDE COMMANDER

Who Is Really Putting Nepal Back Together?

Half a year after Nepal's devastating earthquake, its the smaller community organizations that are helping the country rebuild, while the giants of disaster relief lag behind.

BY KRISTIN LORD, TINA SCIABICA | DECEMBER 18, 2015

More than seven months after a devastating earthquake in Nepal killed almost 9,000 people and left millions in need of food, shelter, and basic medical care, most of the $4 billion committed by international donors has not reached its intended recipients. Children cannot go to school, buildings remain unsafe and harsh winter weather is fast approaching. One need only drive through the Nepali countryside to see that many people in rural areas are still living under makeshift shelters using tarpaulin and sticks. Only the fortunate have tin roofs to help keep out the rain and, soon, the cold winter weather. The situation has only worsened in the past three months due to a nation-wide fuel crisis and political unrest along Nepal's border with India.

Meanwhile, even the most respected international humanitarian organizations are under scrutiny for the percentage of charitable donations intended for earthquake relief that instead go to pay for overhead. Nepalis see fleets of new SUVs showcasing the logos of international NGOs on the streets of Kathmandu — visible proof of the aid operations that have set up shop in Nepal since the earthquake — but know that most areas of the country are still seeing little to no assistance. To be sure, there are legitimate reasons for global humanitarian organizations to maintain their critical global infrastructure and these important organizations must find ways to pay those costs. However, in the wake of an urgent humanitarian disaster like the Nepal earthquake, frustration with expensive models of aid delivery continues to mount, particularly when the needs of so many earthquake victims still go unmet.

litional models of disaster relief — approaches And perhaps surprisingly, they can come from l disasters.

significant role in disaster relief if they have an ch to build. In Nepal community-led tions are already in place. These models also offer a blueprint of how to build the resilience of communities around the world to respond rapidly and cost-effectively in the event of major natural disasters while addressing the ongoing needs of local communities related to literacy and education, workforce training, women's empowerment, and civic participation.

Consider the following examples:

READ Global (led by the co-author of this article, Tina Sciabica) saw its network of community-own and managed Community Library and Resource Centers ("READ Centers") jump into action within days — and in some cases hours — of the earthquakes. Operating in Nepal for more than 20 years, READ Centers are community-owned and managed, and offer educational resources and programs to improve literacy. Community members volunteer their time to serve on locally elected committees that manage the centers, and these committees determine how each center can best serve the people that live there. Because of their deep roots, they were a trusted resource after the quakes: The centers were places where villagers could recharge their mobile phones using the center's solar power, receive relief supplies distributed by the centers, and for some, a safe place to sleep because their homes had been destroyed. Six of READ's 59 Centers in Nepal suffered serious damage from the earthquakes with the majority of homes being destroyed in these communities, yet amazingly the centers mobilized more than 1,000 volunteers as providers of disaster relief in the days and weeks after the quakes.

so quickly, they were able to help other
none towers down for many days in some areas, it
many communities, let alone assess damage or
n) mountaineers attempting to summit Everest,
with supplies. But using READ facilities, local
ed help. They organized groups of volunteers to
hat were hard-hit by the quakes – driving several hours to deliver supplies and often providing the first relief to reach these communities. What READ Centers offered rural Nepali communities was the means to organize themselves to raise money and volunteer labor to build much-needed infrastructure where the community could gather safely.

The story is much bigger than what happened with the centers, however. Other community-based organizations witnessed similar results.

The dZi Foundation, another Nepali NGO that utilizes a community-driven approach, did much the same. The foundation is one of the only organizations working in some of the hard-to-reach rural areas near Everest (where some communities are a three-day walk from the nearest road), and were the only organization bringing relief to these communities in the weeks following the earthquakes. Because of the long-standing relationship in these communities, the dZi Foundation was able to hold 69 discussions with communities to assess damage and let the community decide what first needed to be addressed. The community groups decided that the most important priority was to get their children to get back to school, so dZi worked with volunteers from the communities to build several temporary learning centers. Although infrastructure and countless homes were destroyed, the communities themselves decided to prioritize the rebuilding of schools and have committed to volunteer their labor to that effort. Because education is their own priority, they have shown a great willingness to donate both money and time to ensure that need is met.

al communities in Ghorka and Dhading districts, Committees (VDCs) through its 30 partner hough Practical Action is not a disaster relief n for this effort, its relationships with local olunteer their time to help with relief efforts. The both money and time.

All of this happened against the backdrop of larger disaster relief organizations struggling to gain a foothold. For example in some areas, community members complained about large relief organizations failing to ask what communities needed before delivering large quantities of nonperishable food (dried noodles, etc.) that the community had no use for because they had large stocks of stored grain that would last for months.

Other organizations failed to engage local communities in their efforts, producing low-quality infrastructure that communities don't value. For example, UNICEF gave many grants to INGOs to establish temporary learning centers, but foreign organizations with no prior connection in communities couldn't mobilize volunteers to help with construction nor could they raise matching funds. These organizations resorted to using tarps or tents to create their structures — a solution that only works for a few months, and will falter once winter arrives.

The lesson in all of these smaller successes is that an existing social infrastructure and a trusted community hub can empower local citizens to organize and act nimbly. This is not something that happens overnight, particularly in countries where people have many unmet needs and governments have a long history of being unable — or in some cases uninterested — in meeting them.

se of civic engagement that is necessary to o creates enduring community support and a nent can do more than large amounts of money: t of 10 years when it decides to works with a that the community is set up to continue EAD Centers have existed in Nepal since 1991 and nt is unusual in traditional development agencies — it is difficult to implement given those agencies' typical focus on the execution of discrete projects for a finite time-period, fixed at the outset — but its impact can be deeper.

The advantage of these community-driven efforts, however, is that they are relatively inexpensive and can even become financially self-sustaining. Each READ Center, for instance, creates sustaining enterprises that pay the ongoing costs of operating the centers (librarian salaries and Internet access, cost of publications, etc.). READ builds the capacity of the community to form their own partnerships with local NGOs and government agencies to ensure ongoing programs on women's empowerment, livelihoods training, and literacy classes. Centers are sustained by renting tractors or storefronts, selling honey, providing ambulance services for a fee, or other products or services in demand by the local market. When compared with the costs of providing external disaster relief, let alone the effectiveness, the up-front costs to this approach are minimal. And, as an added and equally important incentive, such centers provide important support to people in rural and marginalized communities at times when there are not disasters as well.

At a time when governments and aid agencies worldwide are scrambling to figure out how to pay for both the surging costs of humanitarian and natural disasters, which totaled an estimated $24.5 billion in 2014 (up nearly a fifth from the previous year) according to the 2015 Global Humanitarian Assistance Report, as well as the costs of achieving the recently adopted Sustainable Development Goals intended to alleviate poverty around the world, it is useful to examine models that advance both agendas at once. It is even more useful to highlight sustainable, low-cost, community-led models that come from within nations in need — and help them understand that they have more power to transform their own communities than they or the rest of the world had realized.

PRAKASH MATHEMA/AFP/Getty Images

SE MILITARY

NFANTRY BDE COMMANDER