Defense & Technology Paper

109

Can You Hear Me Now? The Case for Considering Information and Communications Technology as a Critical Component of Future Postconflict Operations

Karen E. Black, Larry Wentz, and Sebastian Megens–Sedor

CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY

Can You Hear Me Now?
The Case for Considering Information and Communications Technology as a Critical Component of Future Postconflict Operations

By Karen E. Black, Larry Wentz, and Sebastian Megens-Sedor

Center for Technology and National Security Policy

Institute for National Strategic Studies

National Defense University

Contents

About the Authors

Karen E. Black is the Principal of Alaurus, an international ICT consultancy. She worked in the Afghan ICT sector from 2010 to 2015.

Larry Wentz is a Visiting Research Fellow at the National Defense University (NDU) Center for Technology and National Security Policy (CTNSP). He formerly served as a Senior Advisor to the DoD CIO and DISA.

Sebastian Megens-Sedor is pursuing a Bachelor of Arts in International Relations at the American University School of International Service. He interned at the NDU CTNSP from October 2016 to September 2017.

Executive Summary

Information and communications technology (ICT) is vital to modern post-conflict security, stability, reconstruction, and development operations for both the intervening civil-military elements and the affected nation.

The U.S. Government should designate ICT as critical infrastructure and an essential service on par with roads, power, and water and grant it the same priority regarding resource allocation and funding. Research continues to demonstrate the efficacy of ICT as a powerful enabler of security, governance, social development, and economic growth in post-conflict and developing countries.

The U.S. Government and the International Community should formally address ICT in OCONUS policy and doctrine and designate lead agencies responsible for coordinating OCONUS civil-military ICT efforts.

The U.S. Government should consider ICT in all phases of future engagements—preparation, planning, execution, drawdown, and transition—so as to more fully and effectively leverage ICT to achieve mission goals. There is a definitive need for the U.S. Government to include a civil and commercial ICT advisory function as a core capability in future interventions. Such an entity would support decision-making by leadership, coordinate ICT efforts with the US Interagency and the International Community, and advise the affected nation on the recovery and rehabilitation of its ICT sector.

[In] *Afghanistan, the thing that will most affect that culture over the long term is leaving behind that network and those cell phones . . .* [and] *the introduction of that technology is probably far more lasting than anything else we're going to do in Afghanistan and far more influential.*
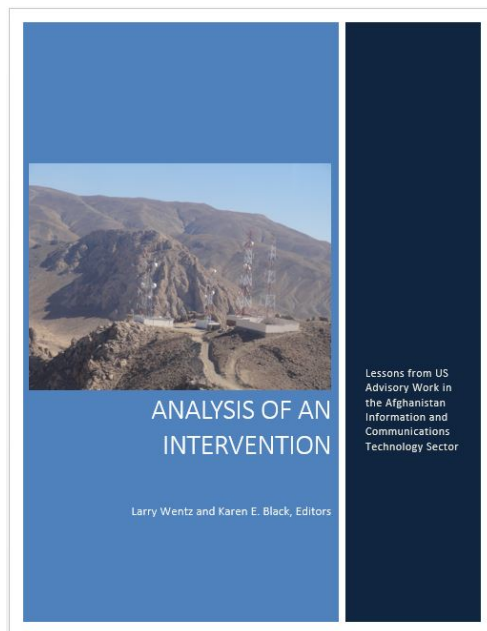
—General James E. Cartwright, USMC (Ret.)

Introduction

Information and communications technology (ICT) is vital to modern military campaigns and post-conflict security, stability, reconstruction, and development operations, arguably on par with the long-established critical infrastructures and essential services of roads, power, and water. ICT is foundational to intervening civil-military elements' complex communications, collaboration, and information-sharing needs. Moreover, it is a powerful enabler of the affected nation's security, governance, social development, and economic growth. However, neither the U.S. Government nor the international community has an officially adopted policy on the role and importance of ICT outside the Continental United States (OCONUS).

During and after engagements, there are typically a plethora of ICT participants and stakeholders: military and civil elements of the intervening force, international and non-governmental organizations (NGOs), donor governments and other benefactors, the affected nation's government, the private sector, and the local population. There are also spoilers, such as insurgents and criminals, who also use ICT—even the Taliban uses social media like Twitter, for instance. Each has its own agendas, authorities, interests, expectations, capabilities, and limitations. Yet there is no official lead agency, within the U.S. Government or internationally, responsible for coordinating OCONUS post-conflict ICT strategies, projects, available funding, or activities among and across these stakeholders and participants. The Department of Defense Chief Information Officer (DOD CIO) has worked extensively across the interagency community and with the White House to identify an entity to assume such an overarching role, but there has been no interest to date. Consequently, approaches regarding ICT and its use in post-conflict operations are ad hoc and reactive, disparate and disorganized, and do not leverage ICT effectively to support the warfighter or benefit the affected nation.

ANALYSIS OF AN INTERVENTION

Lessons from US Advisory Work in the Afghanistan Information and Communications Technology Sector

Larry Wentz and Karen E. Black, Editors

From interventions in the Balkans, Iraq, and Afghanistan, several ICT-related areas emerged as requiring immediate attention post-conflict: spectrum management; ICT-enabled information-sharing and information dominance; effective ICT sector governance, including the development and implementation of ICT policies, laws, and regulations; human ICT capacity development; the early deployment of ICT solutions to enable communications and support governance, humanitarian assistance, and emergency services; and the rehabilitation or installation of commercial ICT infrastructure and the proliferation of ICT services. The first two areas are of paramount importance to the intervening force to enable security and stability, while the third and fourth are foundational to the affected nation's reconstruction and development. ICT infrastructure and services are crucial in supporting the intervening civil-military elements' communications and information-sharing needs as well as those of the affected nation's government and citizens. However, the U.S. Government and the international community lack deliberate, holistic approaches and purposeful plans to help the

affected nation recover, restore, rehabilitate, and modernize the ICT sector. In absence of these elements, malevolent actors often step in. These themes and others are covered in great detail in *Analysis of an Intervention: Lessons from U.S. Advisory Work in Afghanistan's Information and Communications Technology Sector*.[1] This paper comprises a synopsis of some of this volume's major findings.

The failure of the U.S. Government to recognize the role and importance of ICT in post-conflict operations stems, to a great extent, from two factors. First, and most importantly, the U.S. Government does not formally consider ICT as critical infrastructure or an essential service like roads, power, and water as a matter of OCONUS policy. Therefore, it does not afford ICT the same priority in terms of resource allocation or funding. Second, the U.S. Government and the international community have a propensity to treat civil and commercial ICT as an afterthought rather than an integral component of campaigns. All too often, planners, interveners, and responders presume civil and commercial ICT infrastructure will be in place when they arrive, ICT services will be available and provided by the (generally incipient) private sector, and the affected nation's government will be capable of ICT sector governance and oversight. However, this is rarely the case. What the planners, interveners, and responders neglect to consider—or at least sufficiently accommodate—is that our interventions are increasingly in underdeveloped or developing countries that have little or no modern ICT infrastructure (particularly in rural areas), antiquated and outmoded ICT equipment, and a scarcity of high-tech skills even before an engagement, let alone afterward. As a result of these factors, adequate consideration of ICT sector recovery and the broad ranges of civil-military ICT use in overall mission planning are omitted.

Immediate ICT Needs of the Intervening Force

In post-conflict environments, two ICT-related problems of primacy for the intervening force are a desire or need to control and manage the affected nation's electromagnetic radio spectrum and the ability to leverage ICT to collect and potentially share information.

Proper spectrum stewardship is unquestionably crucial for military command and control and government communications, collaboration, and information-sharing because radio frequency spectrum underlies most modern communications systems, especially wireless. Intervening forces often attempt to assume control of the affected nation's spectrum resources and management, whether by agreement or force. Whoever controls the access to the spectrum will also control much of the means of conveying information.[2] When the affected nation is still sovereign, its spectrum resources and their management remain under its purview, which the interveners must keep in mind. The Military Technical Agreement between the Interim Afghan Administration and NATO's International Security Assistance Force (ISAF) gave ISAF the right to unrestricted use of all Afghanistan's electromagnetic spectrum free of charge. ISAF transitioned spectrum management responsibility back to the Afghans prior to it ceasing combat operations in December 2014.

For various reasons, the affected nation may not be capable of appropriately administering its assigned spectrum and may need assistance from the interveners. Spectrum utilization is managed through international treaties and national policies. The International

Telecommunication Union (ITU) allocates radio frequencies for various communications services according to its radio regulations articles. Individual countries generate frequency allocation tables and assign specific frequency bands for military, civil, and commercial communications. Countries, generally via the ICT sector regulator, also sell or license radio spectrum to operators of private radio transmission services, such as cellular telephone networks and broadcast television and radio stations.

With today's typical multilateral, multinational (alliance or coalition) campaigns in post-conflict environments, there is an array of different countries with their own military forces, bases, and embassies whose personnel often have limited or no experience operating in such an environment. Additionally, there is often an influx of international and non-governmental organizations, aid agencies, and commercial companies whose staff is similarly inexperienced in working together in civil-military operations. As such, they tend to compete in supporting recovery and reconstruction. Each has different communications systems, some of which may align with regional standards and spectrum assignments. There will likely be a need to implement a process to deconflict frequency allocation among multinational militaries and to limit interference with the commercial spectrum caused by jammers. Without a cohesive plan to manage and coordinate the assignment and use of radio spectrum in the affected nation, military, civil, and commercial communications systems are unable to operate in an interference-free environment. Such a situation can quickly become intractable, as it did in Afghanistan. Therefore, it is critical that the intervening force, the U.S. Government, and the international community consider assigning human spectrum resources to assist and provide or arrange spectrum training for the affected nation—not solely in and for the security forces. Effective civil and commercial spectrum management is paramount for and fundamental to the development of the affected nation's ICT sector and can spur significant growth in all sectors of its economy.[3] Further, access to and use of radio frequency spectrum is vital to meet political, cultural, social, and economic objectives.[4]

The other urgent need of the intervening force is ICT-enabled information-sharing. The Center for Technology and National Security Policy (CTNSP) at the U.S. National Defense University (NDU), which has long researched how to share unclassified information in post-conflict environments, asserts if U.S. or coalition forces cannot communicate, collaborate, or exchange information with the population they seek to influence, they *cannot* achieve the social, political, and economic goals for which the forces were committed.[5] The CTNSP stresses that incentivized information-sharing is vital to complex operations and creating environments conducive to information-sharing benefits U.S. Government objectives while also helping coalition partners, international organizations, NGOs, and the local community.[6]

Along those lines, two Department of Defense Directives/Instructions, DODD 3000.05 in 2005 (later reissued as DODI 3000.05 in 2009) and DODI 8220.02 (2009) require the U.S. military to collaborate with other relevant entities in planning, preparing for, and conducting stability operations and provide ICT capabilities to support sharing information within the DOD and with non-DOD partners in stability and reconstruction operations, respectively. Unfortunately, the reality of doing so often proves problematic. Militaries conventionally operate in the classified information domain over their own networks for security reasons, while other post-conflict participants by and large operate in the unclassified domain using commercially available non-

secure connectivity, services, and applications to demonstrate impartiality, neutrality, and transparency in their dealings with the affected nation's government and the local population. The two methods of operation are incompatible and the lack of information-sharing can lead to discord between and among entities with incompatible interests, incongruent agendas, and conflicting goals. It can also engender duplication of effort and waste of resources, as well as result in missed opportunities and overlooked synergies.

In Afghanistan, several ICT platforms emerged as ad hoc solutions for civil-military unclassified information-sharing, generally controlled-access portals hosted on the open Internet. All had varying degrees of usefulness and success of purpose. However, other issues abounded, such as improper or overclassification of data; storing of unclassified data on classified systems; and restricted or blocked access to the public Internet at U.S. and coalition facilities. Further, there were sensitivities surrounding the use of ".mil" and ".gov" email addresses to exchange information with non-U.S. military and government organizations so as not to appear to be part of either, making them targets instead of non-combatants. In addition to these challenges, complications arose from national policy, organizational, personnel, language, and cultural differences in the way information is viewed, protected, handled, understood, and shared, not the least of which is an inculcated culture of restricting and retaining information as power. As the CTNSP aptly declared, "Experience has proven the primary obstacles to [information] sharing are . . . social. The human beings on the ground are the ones who must implement policy and strategy, collaborate and share information, and respond to rapidly changing circumstances and conditions."[7]

The appropriate and effective collection, storing, and sharing of unclassified information is paramount in complex post-conflict operations and will only become more important in our increasingly interconnected world. The role of ICT as an enabler of information-sharing and information-dominance should be further recognized and codified strategically and tactically in future interventions, and workable, usable technical solutions should be devised to help mesh civil-military communications. Crucial improvements in ICT architectures and solutions should be accompanied by changes in attitudes and behaviors. To be successful, organizations must be willing and able to share information, facilitate collaboration and coordination, and execute a comprehensive, multifaceted, multilateral approach that fully leverages ICT.

Operative approaches for post-conflict information management should also address information dissemination to the local population as a means of influencing their perceptions and managing their expectations. Broadcast media, particularly radio but also television in early phases, followed by mobile messaging, the Internet, and social media are all powerful tools for such communications, and all rely on ICT infrastructure and services. However, the enemy can also leverage these mechanisms to spread counter and contrary communications, just as the Taliban established—and continues to use—its own radio stations throughout Afghanistan.

Early ICT Needs of the Affected Nation

In postconflict environments, the affected nation has its own set of ICT-related issues. Its initial ICT recovery and reconstruction efforts should focus on the following: early restoration or establishment of ICT sector governance; the deployment of temporary ICT infrastructure to help

bridge communications gaps, with a particular emphasis on the provision of ICT services for governance, humanitarian efforts, and emergency communications; the early recovery of ICT infrastructure to support intervening civil-military connectivity and service needs; and the development and implementation of a concerted and sustained ICT capacity development program.

Restoring ICT governance means first helping the affected nation establish a ministry or cabinet-level department of communications if none exists. Once such an entity is in place, advisors should help it to revive and update or establish new simple yet comprehensive ICT policies, laws, regulations, and enforcement mechanisms; articulate goals and expected results; and devise a simple roadmap that leaves room for innovation. Getting it right from the outset is seminal to encourage both local and foreign private investment in the ICT sector. Commercial companies, like the mobile network operators in Afghanistan, have proven they are willing to commit substantial sums even in conflict zones to build ICT infrastructure, garner service and spectrum licenses, and market and sell ICT services. However, the affected nation must provide investors several key assurances: predictability, transparency, a reasonable risk-reward ratio, and a level playing field. It is also important the affected nation consider privatizing any state-owned ICT institutions or, at the very least, ensure they are not afforded any statutory protection, special licenses, or favorable treatment if they remain.[8]

Another pressing piece to restoring ICT sector governance is the establishment of an independent ICT regulator. Regulatory responsibilities and objectives include but are not limited to:

- implementing national ICT policy
- tendering for, issuing, and collecting fees for licenses, as well as establishing associated performance metrics for them and monitoring compliance with them
- fostering market liberalization and promoting fair and unbiased competition
- preventing or curtailing abuses of market power
- administering ICT resources, such as radio spectrum and infrastructure rights of way in a non-discriminatory and transparent manner
- establishing and maintaining a national numbering plan and other ICT registries
- ensuring the adequate supply and delivery of quality ICT services at reasonable prices and regulating tariffs for such
- facilitating universal access to ICT services and administering funds for such
- reporting to and liaising with international ICT organizations, particularly the ITU, which is responsible for global spectrum and satellite resource allocations and deconfliction
- protecting ICT consumers and responding to their complaints
- collecting ICT statistics and publishing them nationally and internationally (to show progress in the sector, among other reasons).

The ministry or department of communications and the ICT regulator play pivotal roles in recovering and overseeing the affected nation's ICT sector so it can serve as a foundation for and an enabler of security, governance, and socio-economic development and growth. Post-conflict countries often emerge, or at least have the potential to, as Greenfield states, "unencumbered by the paralysis of layers of special interests and byzantine barriers to change," which can be particularly advantageous in terms of ICT.[9] They are free to adopt the latest and greatest

technologies without being hindered by legacy infrastructure and backward compatibility. However, the affected nation will likely need help to identify and implement ICT solutions and harness the transformative power of ICT.

For all of the above reasons, it is imperative the U.S. Government and the international community collaborate and coordinate civil-military planning, programming resources, and allocating funds to restore or establish, supplement, and fortify the affected nation's ICT sector governance institutions. These efforts should include civil or commercial ICT professionals to advise the Ministry of Communications (MoC) and the ICT regulator on the establishment of a legal-regulatory framework conducive to creating an enabling environment. Once established, this environment should fast-track private sector investment, ownership, and operation of ICT infrastructure and the proliferation of ICT services to meet both the interveners' and affected nation's communications needs.

Another area of immediate focus by the affected nation should be the deployment of ICT infrastructure to help bridge communications gaps, coordinate governance and humanitarian efforts, and provide emergency communications services. Solutions can be temporary and simple, such as passing out handheld satellite phones, or more sophisticated, such as implementing small-scale, closed-user group cellular networks. Reasonably low-cost, highly transportable solar-powered 3G and 4G mobile voice and data network solutions now exist. These systems can be installed quickly; used securely; and packed up, moved, and reused elsewhere, an ideal solution for troops on the move and police in remote outposts. There are other fairly economical ways to obtain satellite-based Internet services, such as installing very small aperture terminals (VSATs) or subscribing to commercial VSAT services such as YahClick. Whatever their form, initial ICT communications capabilities must be made available to the intervening force and the affected nation's military, police, government, and citizens. Establishing and promoting a free, easy, and convenient way for the affected nation's citizens to contact police, fire, ambulance, and other government services can offer tangible results and dramatically increase the population's confidence in its often-nascent government's ability to provide for them, thereby promoting security and stability.

Examples of deploying ICT infrastructure to bridge communications gaps and provide emergency calling capabilities in early post-conflict Afghanistan included the installation of an emergency cellular base transceiver station in Kabul, a network of sophisticated high-frequency handheld radios, and a series of satellite-based voice and data networks. In early 2002, there was

a near-total dearth of telephone service other than the former Taliban Tel network (see sidebar). To meet its own communications needs, the United Nations World Food Program established a private mobile network for its workers in Kabul, donated and installed by Ericsson, and allowed personnel from other humanitarian organizations as well as select Afghan government officials to use the network to coordinate aid efforts.

The U.S. Agency for International Development (USAID) provided high-frequency radios, which were inexpensive and easy to deploy. They were equipped with telephone and email services and basic computing capabilities, as well as with rudimentary printers and scanners.[10] Ultimately, the radio system was installed in 30 provinces and reportedly had significant positive impact; officials in Faryab Province were able to transmit information about periodic factional fighting and receive advice from the Karzai administration as to how to resolve the issue. Takhar Province used the radios to request emergency assistance after severe flooding.[11] Additionally, the Combined Forces Command provided radios to the Afghan National Army early on.

Three ambitious satellite-based communications systems—the Government, District, and Village Communications Networks (GCN, DCN, and VCN, respectively)—were designed to provide the early extension of essential communications services at increasingly lower subnational levels. The World Bank provided $14 million in funding for the GCN through its Emergency Communications Development Project in 2003.[12] The goal of the GCN was to equip Afghanistan's provincial governors with telephone, Internet, and video conferencing capabilities and connect them to the central government in Kabul. An American company installed the hub site in Kabul, which was connected to an international gateway in Europe, as well as satellite earth stations on MoC/Afghan Telecom Corporation (AfTel) buildings in each province. However, the GCN project was insufficiently funded so crucial connectivity from the landing sites was missing. As such, the GCN was supplemented by the Provincial Governors Communications Network (PGCN) to complete last-mile links from the satellite earth stations to the provincial governors' offices and sometimes to their homes in areas too dangerous to travel. The PGCN, which was the first WiMAX installation in Afghanistan, was also used by other government offices in provincial capitals.[13] The DOD provided funding for project management, continuity, and other support to deploy the first 20 PGCN sites and then handed primary responsibility over to AfTel for the remaining installations.

The DCN was financed by a USAID grant of $14.2 million and used to extend telephone and fax services and Internet access to the district level for use by local government officials, emergency services, and the local population. The DCN terminals generally included nine ports: four each for telephone and Internet connections and one for a fax machine. Provision of ICT services to the local population was through Internet cafés and public call offices on a fee-for-service basis, with that revenue supplementing the MoC's budget and helping to pay for generator fuel, maintenance, and ongoing operations. The anticipated financial benefits did not materialize because fuel costs were very high in many districts, the purchasing capacity of citizens was quite limited, and the Afghan budget process was not up to the task of allocating DCN operating funds to the ministry. Hence, DCN facilities were often closed during times of significant demand from the public. While the full scope of the DCN project was not realized, DCN terminals were implemented in 270 of the more than 350 legislative districts. As Afghanistan's mobile network operators expanded their coverage, there was less of a need for the DCN nodes. The MoC

upgraded and repurposed many of the DCN nodes and satellite bandwidth for the VCN and added solar power to the equipment so it could be used in areas without any or reliable electricity.

The rollouts of the GCN and DCN were accomplished in no small part due to tremendous civil-military coordination. The U.S. Provincial Reconstruction Teams often deployed Commanders Emergency Response Program (CERP) resources to finance stand-alone DCN buildings, including in 26 districts of Kandahar and Zabul provinces. Representatives from USAID negotiated with district officials for dedicated space in district government buildings that were under construction. U.S. military officers (from the South Carolina National Guard) based in Kabul identified CERP funds and installed WiMAX technology in select provincial capitals to link some government offices and other appropriate users to the GCN landing point. Others used CERP funds to install solar panels on 10 DCN sites to demonstrate ways of overcoming the high cost of diesel fuel.[14]

An American company won the contract to install and operate the GCN and DCN, whereas AfTel, the state-owned service provider that had employees in all 34 provinces, was responsible for installing the VCN. The purpose of the VCN was to establish access to ICT services in rural areas. Unfortunately, the VCN equipment had satellite bandwidth access limitations, so most VCN terminals were used only for phone calls even though the terminals had been equipped for data. AfTel also sold VCN kits to local entrepreneurs who established public calling offices where they resold phone service to their communities. The DCN and VCN were early examples of *dual-use* technologies—they were designed to give both local civic leaders and citizens access to telephone and Internet services. They are also, in theory, great models of public-private partnerships and, because they included profit incentives, good examples of planned sustainable development.

While early attempts at post-conflict communications in Afghanistan had their challenges and limitations, they served the vital functions of connecting the various levels of the fledgling administration to each other, connecting Afghan citizens to their government, and providing tools with which to counter propaganda by insurgents. Both the radio network and the VCN are still in use in Afghanistan today.

Examples of early ICT infrastructure and services in Afghanistan are the installation of a rudimentary optical fiber metro area network in Kabul, which connected various ministries and government agencies shortly after the fall of the Taliban government; various NGOs offering voice and data services, both free and for a fee via VSAT once they set up operations; and Afghan Wireless Communications Company (AWCC) and USAID establishing Internet cafés in Kabul in mid-2002. The MoC implemented half a dozen or so telekiosks (funded by France) in Kabul in 2003, and mobile network operators AWCC and Roshan launched several public call offices around the same time. Afghanistan's satellite earth station was rehabilitated and upgraded under a World Bank project that began in late 2003 to restore and increase transmission capacity between Kabul and the rest of the world. India funded a project tendered by the MoC to install a digital switch and last-mile code division multiple access (CDMA) wireless local loop services in 11 provincial capitals for a total of 35,000 telephone lines between 2003 and 2005.[15] Although this list is representative rather than exhaustive, it illustrates the wide array of early ICT efforts.

In post-conflict operations, the civil-military interveners could employ two strategies to more fully use ICT to meet both their and the affected nation's communications needs. The first would be to consider civil and commercial infrastructure like fiber optic cables, satellites, and cellular and microwave networks as dual-use technologies. The interveners could make upfront investments for the installation of ICT infrastructure in areas that require services rather than rely on the affected nation to do so. The interveners could justify the expenditures to meet their communications needs, and their initial cash infusion could jump-start ICT infrastructure deployment. That infrastructure could then be used to provide ICT services to the affected nation's government and citizens. The second strategy would be to have interveners serve as *anchor tenants* whereby they agree to buy or lease capacity on civil and commercial ICT infrastructure, thus providing seed funding to install, expand, or become operational.

The U.S. Government was an anchor tenant of Afghanistan's national fiber optic network. By leasing capacity, it achieved in-country connectivity among command centers and access to regional and global fiber transport routes to support connectivity with higher echelons of the command structure. The Afghan government received much-needed revenue to continue to build out its fiber network. The relationship proved beneficial to both countries.

To its credit, the Afghan government understood the importance of ICT to the country's rehabilitation and designated ICT a priority sector for investment, which mobilized the United States and other governments, the international community, and the private sector. Early implementation of public-private partnerships with the MoC enabled the provision of ICT services to the fledgling government. The MoC's adoption of policies that favored competition and private investment (including foreign investment) and enacting of light-touch legislation and regulation were key to jump-starting the ICT sector by encouraging commercial companies to invest in and implement infrastructure and offer services to the public. With tailored technical assistance and sustained in-country support for its ICT governance institutions from the international donor community, Afghanistan was able to accelerate the adoption and implementation of an enabling environment that maximized private investment and set new standards for the path that a post-conflict country could take from smoldering rubble to the most advanced technologies and services.[16]

Many of these activities, however, were largely independent initiatives. Participants generally had good intentions and goals, but there was no coherent, cohesive approach. This disjointedness caused duplication of time, effort, and resources or omission of important components and considerations. At times, concurrent activities were diametrically opposed or in direct conflict regarding both approaches and outcomes. The international ICT community lacked overall top-down leadership, coordination, information-sharing, and a collaborative framework for supporting informed decisionmaking, both individually and collectively.

Inherent to effective long-term security, stability, reconstruction, and development operations is the need for the affected nation to be able to sustain the advances and further the gains it experiences. This is particularly critical with regard to ICT, which is a revenue-generating, job-creating sector in and of itself as well as an enabler and accelerator of progress in all other sectors. It is also why the U.S. Government and the international community must plan for and

implement comprehensive and lasting ICT capacity development programs as part of post-conflict reconstruction operations. Such a strategy should include ICT skills development for civil and military personnel, the various tiers of ICT workers, and the general population. It should also include *soft skills* such as literacy, critical thinking, problem solving, numeracy, and effective communications as well as management and leadership competencies.[17] ICT capacity-building requires consideration not only of the physical communications systems, networks, and services that utilize them—along with the hardware and software for information storage, processing, and presentation—but also the associated management and financial and regulatory practices to ensure the technologies work together seamlessly.[18]

Two early international community efforts at ICT capacity-building in Afghanistan are of note. Through a partnership among Cisco, the United Nations Development Program, the ITU, and the Afghan MoC, three Cisco Networking Academies were established in 2002 (growing to nine by 2010). Beginning in late 2003, the World Bank funded institutional capacity-building for the MoC in policy and regulation, project management, and spectrum, as well as technical training for MoC and AfTel staff to be able to administer, operate, and maintain the government communications network. Additionally, commercial training centers popped up almost immediately in Kabul and other major cities, offering fee-based ICT training to the public.

Since those early days, myriad ICT training efforts have been implemented around the country, from free community-based training centers to master's and doctorate programs via competitive study abroad programs and scholarships and everything in between. A significant amount of ICT training was and continues to be conducted outside the country in places like Dubai, Pakistan, India, and Turkey, which is expensive and can be problematic because of visa issues. ICT capacity-building efforts have been funded by the Afghan and donor governments, international organizations and NGOs, commercial companies, public-private partnerships, and volunteer organizations, among others. As of early 2015, there were 2- and 4-year ICT-related degrees offered by Afghanistan's public and private technical and vocational institutes, colleges, and universities but no graduate-level or post-graduate ICT programs.

Afghan ICT companies, including three mobile network operators, reported that ICT graduates from Afghanistan's institutions of higher learning required 3 to 6 months of additional in-house training upon hire.[19] Millions of dollars have been spent on disparate digital literacy activities for Afghans, but there is no concerted strategy for ICT capacity development. Few programs are standards-based. There are no professional development programs or roadmaps. Cybersecurity, cyber defense, and information awareness training are practically non-existent. And ICT certifications (and even degrees) are often bought or counterfeited.

To complicate matters, affected nations often suffer from *brain drain* of educated and tech-savvy youth who flee from conflict, as is the case in Afghanistan. ICT workers are in demand internationally and are often among the first to leave, knowing they will be better compensated abroad. For example, an entry-level Afghan IT/ICT technician earns roughly $3,600 to $6,000 per year at an Afghan company, which can increase up to $9,600 or so after 2 years. Those with 3 or more years of experience plus industry certifications can garner $12,000 to $18,000 annually and up to $24,000 for management positions. Many international companies pay more, such as $36,000 to $60,000 for more senior positions. Compare those figures to entry-level IT

technicians in the United States, who earn between $28,000 and $35,000 and the national average of $68,764 for all IT technicians (all levels, all areas).[20]

The global shortage of ICT workers is expected to continue. Two reports from 2012, with slightly different figures, illustrate this point. According to the first, the global ICT sector will be looking to hire at least 1.7 million people in the coming years.[21] The second report says there are expected to be 2 million more ICT jobs than there are professionals to fill them during the same decade.[22] None of this bodes well for the future of Afghanistan's ICT sector.

ICT capacity development is a complex and comprehensive undertaking. However, it is an absolute necessity for the affected nation to be able to maintain, upgrade, and advance its physical ICT infrastructure and keep pace with the evolution of technology and ICT services. It is also important for citizens of affected nations to integrate ICT into their daily lives, allowing them to re-establish or build virtual connections with and within local, national, regional, and global communities.[23] The U.S. Government and the international community need to come together to develop a framework for ICT capacity development in post-conflict operations in underdeveloped countries. There is a plethora of resources, specifically from the ITU, to assist nations in their electronic emergence. However, they are neither considered in planning nor applied in practice in any sort of systematic or sustained fashion. The U.S. Government, the international community, and the government of the affected nation must also program funding for wide-ranging, far-reaching, and inclusive ICT capacity development programs, with resources specifically set aside for females, children, the elderly, minorities, those in rural and remote areas, and other disadvantaged or typically underserved populations.

The Changing Nature of Conflicts

Modern warfare has undergone a metamorphosis, and methods of conflict now include political, economic, informational, cyberspace, humanitarian, and other non-military measures. Revolutionary technology changes have reduced the salience of state borders and physical territory and increased the lethality and disruptive capabilities of non-state actors.[24] Moreover, the amorphous nature of modern security threats—conflict and terrorism—have made it increasingly difficult to define a uniquely military role and mission.[25] The lines between war and peace have become blurred.[26] The term *post-conflict operations* is a misnomer today because elements of the various forms of conflict (including, for example, pockets of insurgency and terrorist activities) remain for some time in a landscape churning with political, economic, and security competitions that require constant attention by the intervening and affected nation's security forces.[27] In fact, the transition from conflict to peace and prosperity can take years—or even decades—as experience has shown. To operate more effectively in the space in between war and peace, the U.S. Government will need to explore and implement additional means to bridge the civil-military divide and employ and integrate improved whole-of-government approaches in future operations.

However, the U.S. Government's drawdown of its civilian workforce and cutbacks in funding for the State Department and other civilian agencies in the 1990s reduced its ability to effectively engage, assist, and communicate globally with soft power capabilities.[28] As budgets and capacities of civilian agencies stagnated or declined, they no longer had the resources to respond

effectively or rapidly deploy needed civilian expertise. As a result, the military became engaged more and more to step into the breach, expanding the military's role and sidelining civilian agency participation.[29] While the U.S. Government is attempting to expand civilian capacity and rebalance civilian and military roles, when a crisis hits, senior leadership still has a tendency to call upon the military to lead its response. Consequently, the military as an institution may become demoralized and less effective because the U.S. Government is trying to force one institution to do too many things.[30] Likewise, the State Department, aid agencies, and NGOs have expressed concerns and resentment about the militarization of aid and the shrinking of the humanitarian space.[31] The military was not, and is still not, adequately trained to take on the roles of the civilian agencies in post-conflict recovery, reconstruction, and development actions.[32] More specifically, employing commercial ICT infrastructure and services to facilitate the intervening force's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and information-sharing and to underpin and accelerate the affected nation's stability, reconstruction, and development is not a traditional military mission. Such activities are generally counterculture to the military; it is not trained to execute them, nor does it have adequate policy, doctrine, tactics, techniques, and procedures to support them.

ICT Is a Powerful Enabler and Accelerator of Post-Conflict Reconstruction and Development

The effectiveness of counterinsurgency operations (COIN) and donor dollars in accomplishing security, stability, reconstruction, and development objectives has been called into question after the extensive deployment of both in recent conflicts. To a great extent, neither achieved its desired results, and the outcomes were incommensurate with the outlays. On the other hand, evidence of the efficacy of ICT in social development and economic growth continues to accumulate. A growing body of research correlates increases in mobile phone penetration with gains in a country's total factor productivity, GDP, and overall economic growth.[33] Similarly, increases in broadband Internet penetration, upgrades from 2G to 3G mobile broadband services, and growth in mobile data use are definitively linked to increases in GDP growth.[34] ICT has also been demonstrated to be a significant driver of job creation and revenue generation.[35] ICT is "pivotal . . . both as an industry in itself and as an enabler for adjacent sectors and services."[36] While citizens of developed countries rely on digital devices for just about every aspect of everyday life, the use of ICT for new goods and services can be transformational in post-conflict and developing countries.[37] Fully 80 percent of the benefits of ICT come from its usage but only 20 percent from its production.[38]

The success of the ICT sector is—or at least was—an extraordinary accomplishment for Afghanistan. The contribution of ICT to Afghanistan's security, stability, reconstruction, and development to date has been remarkable and revolutionary. As of December 2015, cumulative investment in the Afghan ICT sector exceeded $2.3 billion.[39] Six mobile network operators served nearly 90 percent of the Afghan population and covered 90 percent of the geographic area of the country. In 2016, 40 percent of Afghans reported living in areas with Internet access, 62.2 percent in urban areas and only 32.6 percent in rural areas.[40] At the end of 2014, there were over 2 million Afghan Internet users (some estimate as many as 5 million), including more than 600,000 3G mobile broadband subscribers.[41] More Afghans now get their news through their

mobile phones more than from their mosques.[42] The percentage of Afghans who used the Internet as a source of news and information increased 8.4 points from 3.2 percent in 2013 to 11.6 percent in 2016.[43] Afghans utilized social media extensively in the 2014 presidential election, and social media has given rise to an influential and far-reaching citizen journalism movement. Social media use in Afghanistan increased 43 percent in 2016, and 3 million Afghans are active on at least one social media platform.[44] These trends, particularly if they continue, have the potential to be revolutionary for Afghanistan's future. Bringing Afghanistan out of the digital dark ages also benefits the West. A report by the Pew Research Center shows Muslims outside the United States who use the Internet are much more likely than other Muslims to have a favorable opinion of Western culture.[45] In 2013, former Vice Chairman of the U.S. Joint Chiefs of Staff General James Cartwright said, "As we leave Afghanistan, the thing that will most affect that culture over the long term is leaving behind that network and those cell phones because [the Afghans] are talking across mountains and social barriers that heretofore have never been crossed by that culture . . . [and] the introduction of that technology is probably far more lasting than anything else that we're going to do in Afghanistan and far more influential."[46]
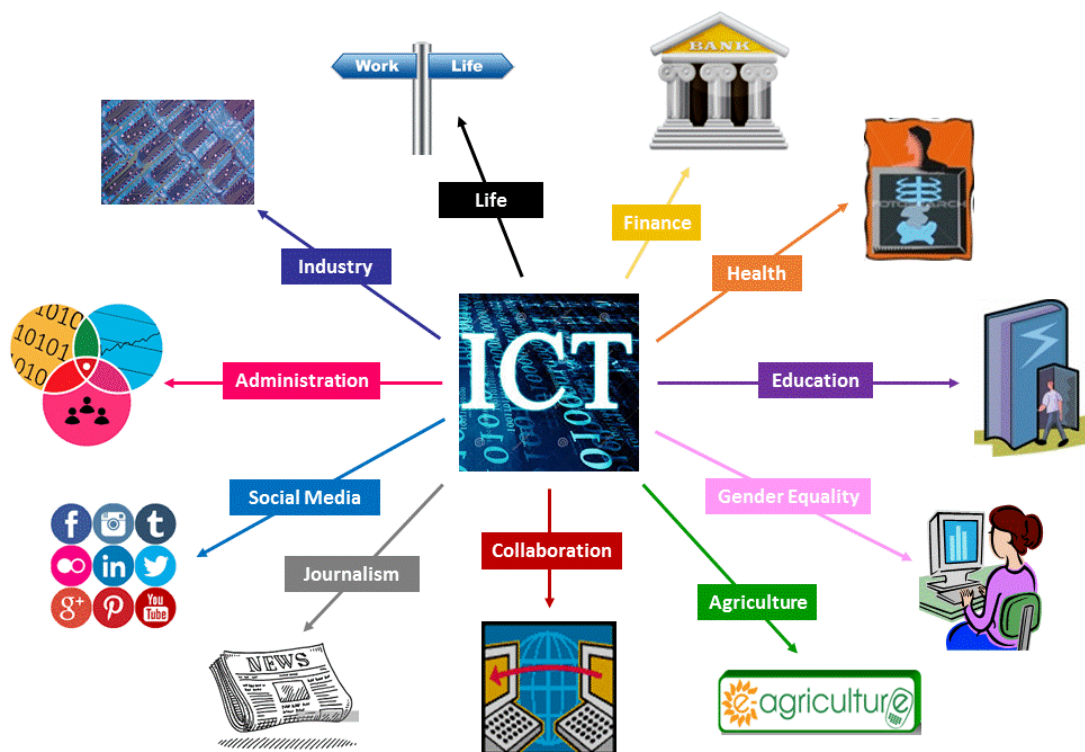

Figure 1. Examples of ICT as an enabler of socioeconomic development and growth

ICT has broadened Afghans' worlds, boosted productivity and economic output, spurred innovation and social change, and improved healthcare and education. Extending these opportunities is critical to accelerating economic and social growth while enabling the transition from a resource-based to a knowledge-based economy.[47] The next stage of Afghanistan's evolution should concentrate on integrating ICT into the everyday personal and professional lives of its people. ICT can and should be a catalyst to achieve the interdependent goals of

security, governance, social development, and economic growth, all of which underpin lasting stability, peace, and prosperity.

The Need for Professional Civil and Commercial ICT Advice

Given all the above, the need for professional ICT experts in post-conflict operations is justified, if not obvious: to meet civil-military interveners' and the affected nation's communications needs; to facilitate ICT-enabled information-sharing; to address civil and commercial ICT sector challenges in restoring the ICT sector; and to identify and pursue opportunities to employ ICT for security, governance, and socio-economic development and growth. Civil and particularly commercial ICT experts are well-suited to build relationships with executives at commercial fixed and mobile network operators, service and equipment providers, and others in the ICT ecosystem, such as educators, manufacturers, and developers. They can engage with state-owned ICT enterprises and facilitate their privatization if warranted. They will likely know of or quickly be able to find and help implement ICT solutions for specific needs and situations. Additionally, professional civil and commercial ICT experts can provide decisionmakers with regional and international ICT resources and advise them regarding international standards, industry best practices, and technology trends.

Properly planned for and utilized, ICT can help create an informed civil-military intervention; organize complex activities; and integrate security, stability, reconstruction, and development efforts with and within the affected nation, making operations more effective overall. Real-world experiences suggest ICT can significantly increase the likelihood of success in these efforts if it is engaged as part of an overall intervention strategy that coordinates the actions of outside interveners and focuses on generating effective results for the affected nation.[48] Hence, there is an urgent need for the U.S. Government to formally designate a professional civil and commercial ICT advisory capability to support decisionmaking by leadership of the intervening force, the international community, and the affected nation in post-conflict operations. Such a capability is imperative to help the affected nation restore or establish ICT sector governance and facilitate the rehabilitation or installation of ICT infrastructure and the provision and use of ICT services.

Ad Hoc Experiments in Afghanistan: Senior Telecommunications Advisors

During Operation *Enduring Freedom* in Afghanistan, two different yet functionally similar ad hoc experiments with forward-deployed U.S. Government ICT advisors yielded tangible results and lessons for future interventions. Dubbed *Senior Telecommunications (Telecom) Advisors* (STAs) at the time, their overarching responsibilities were essentially twofold: to garner and share information regarding the ICT sector with the U.S. Government and ISAF and to advise and assist Afghanistan's public ICT sector officials. The former responsibility included serving as the key leader and advisor for and liaison to the ICT sector and advising the senior civilian representative on ICT-related policy, legal, regulatory, investment, financial, and other ICT issues and activities of interest. It also involved advising the military commander on civil and commercial ICT-related issues and the potential uses of ICT to meet C4ISR needs and mission objectives, including COIN operations.

The latter comprised working with the Afghan Minister of Communications, the Chairman of the board of the Afghanistan Telecom Regulatory Authority (ATRA), the CEO of state-owned AfTel, the U.S. interagency community, the international community, and commercial ICT companies to develop and promulgate ICT policies, laws, and regulations; deploy and protect ICT infrastructure and provide ICT services; utilize ICT to accelerate progress in other sectors; and develop an ICT-literate workforce and citizenry. Important to the execution of the STA functions was how they served as harmonizers, coordinators, and connectors within and across the entire ICT ecosystem (including international organizations such as the World Bank, and U.S. interagency community initiatives of USAID, the Department of Commerce, and others). The STAs also provided informed situational awareness and served as one-stop shops for ICT-related information and advice for the U.S. Government, the coalition, the international community, and the Afghans. In a nutshell, the STAs provided ICT-related thought leadership and strategic thinking to help shape the ICT environment for the success of the strategies of the U.S. Government, NATO, and Afghanistan for post-conflict security, stability, reconstruction, and development.

The first STA was installed at the Afghanistan Reconstruction Group (ARG) at the U.S. Embassy Kabul between 2005 and 2008. The ARG, which was sponsored by the NSC, the Department of State (DoS), and the DOD, was created to assist with the Afghanistan reconstruction effort without creating an additional bureaucratic overlay to the ongoing process.[49] In addition to telecommunications, the ARG worked reconstruction activities in transportation and infrastructure, aviation, water, energy, finance, mines and industry, and agriculture, among other sectors. The Afghanistan Reachback Office (ARO) at the Pentagon supported the ARG. Telecommunications was embedded in the ARG infrastructure section and under the economic umbrella at the ARO. Telecom experts from ASD-NII (now DOD CIO) and the NDU CTNSP assisted both the ARO and STA in the ICT arena. In fact, the STA designated the ASD-NII and NDU CTNSP team as its primary reachback element and supported it in the Continental United States (CONUS) as well as on temporary duty (TDY) in Afghanistan.

The mission of the ARG STA was to provide telecom advisor (TA) functional support—which was not clearly defined in either State or Defense policy—related to all aspects of the emerging Afghan ICT sector, prioritize advisory support issues, and work ICT activities with and across U.S. Government, coalition, international community, and Afghan ICT stakeholders. A key element of the ARG STA's engagement plan was to create and recruit interested civil-military members working ICT initiatives on the ground in-country to join an ICT Integration Team— known as an *I-Team*—to coordinate efforts. The concept was simple and effective: develop concentric rings working outward from a core capability to coordinate U.S. Government efforts regarding the recovery of the ICT sector and the use of ICT by other sectors. The ARG STA also established a second I-Team for coordination among Afghan ICT stakeholders and projects. In addition to the formal arrangement with the ARO, the ARG STA created two additional ad hoc reachback teams, one for access to the broader telecommunications/ICT industry for ideas and solutions and the other for access to U.S. Government entities for ongoing ICT-related support. The ASD NII and NDU CTNSP reachback team facilitated coordination and interactions between the STA and the two ad hoc teams.

As collateral damage and an unintended consequence of the ARG's dissolution in mid-2008, the STA position and the execution of its TA-related functions ceased. The ARG STA returned the TA function and related ICT responsibilities to the U.S. Embassy Economic (ECON) section, which had a small staff and different priorities. The DOD and DoS agreed an active TA function served a valuable purpose and should be reestablished by recreating an STA position in Kabul. In the absence of follow-on actions to reincarnate the STA position, the U.S. Embassy ECON section established a Telecom Working Group to keep appropriate focus on TA functions needed to support the ICT sector and serve as a forum for ongoing interagency community ICT engagement across Kabul and with interested civil-military ICT parties in Washington. The ASD-NII and NDU CTNSP reachback element continued providing ICT support from CONUS between 2008 and 2010 for U.S. interagency ICT coordination and to address requests for ICT support from Afghanistan from the Combined Joint Task Force (CJTF)-101 CJ6 and the U.S. Embassy and USAID Mission in Kabul. The Defense Information Systems Agency (DISA) began funding the CONUS ICT reachback team when discussions commenced between State and Defense to re-establish the TA function in Kabul by creating a STA position at either the U.S. Embassy or ISAF/U.S. Forces Afghanistan (USFOR-A) or both.

A confluence of events, initiated to a great extent by former President Barak Obama's announced troop and accompanying civilian surge, along with USFOR-A's interest in Afghanistan's fiber optic and spectrum resources, prompted the CJTF-101 CJ6 to assume responsibility as the principal spokesperson for ICT with Afghan counterparts in 2008–2009. Understanding it would have to ensure reliable communications for the additional warfighters and their intra-theater mission partners, between 2008 and 2010, DISA worked with the commander, USCENTCOM, his J6, and the DISA-CENT support element to design and implement a high-capacity strategic communication network for use in Afghanistan. Before its installation, U.S. and coalition forces were dependent on commercial and military satellite communications and tactical satellite and microwave links, which had limited bandwidth capacity and induced significant delay. From the end of 2008 and continuing into early 2010, DISA, NDU, and ASD-NII discussed reincarnating the senior telecom advisor position and related TA functions and possibly introducing a supporting team similar to the Iraq Communications Coordination Element (ICCE) established by the Multinational Force (MNF)-I Deputy Chief of Staff for Communications and Information Systems (DCS CIS) in Baghdad.[50] The deliberations were driven by several factors: experiences in and lessons from Iraq; ARG personnel with on-the-ground ICT experience in Afghanistan; ICT-related demand signals from the field; DISA, ASD-NII, and NDU CTNSP personnel with U.S. interagency community and Afghanistan experience; the potential use of ICT for security, governance, and socio-economic development as part of emerging COIN activities; and the need to improve collaboration and information-sharing in theater.

Ultimately, Defense and State agreed the DOD would take the lead to reestablish the STA position and execute the related TA functions, with the DoS supporting the concept and DISA as the designated sponsor. The approved approach was for DISA to establish a senior telecom advisor position at ISAF to support Commander of International Security Assistance Force (COMISAF) and his senior staff and work with U.S. Embassy Kabul and USAID Mission as well as with coalition forces and international organizations. The position was to be filled by a civilian (SES or equivalent), senior enough to operate in direct support of COMISAF and his staff and to work with senior-level U.S. Embassy and USAID Mission leadership. The forward

footprint was to be small, just the STA and two professional commercial ICT support contractors. DISA also redirected the ASD-NII and NDU CTNSP reachback team to support the STA from CONUS and with frequent TDYs to provide on-the-ground support in Kabul and down-range missions in Afghanistan as appropriate. Due to the demands for billeting on ISAF because of the surge, contractors were to be housed outside the wire with their own transportation and private security detail, which also gave them relative freedom of movement. However, upon arrival in Kabul in mid-2010, the STA inherited eight Civilian Expeditionary Workforce (CEW) positions from the ISAF CJ6, recruiting for which had already begun.[51] The CJ6 had been assembling a team to coordinate the various ICT programs and projects in-country and holistically focus ICT initiatives and resources in support of stakeholders, with the vision for ICT to become the critical enabler of socio-economic development in Afghanistan. This capability aligned with the STA's mandate; thus, the eight CEW positions became the Telecom Advisory Team (TAT) under the STA.

The STA/TAT's purpose was to facilitate and coordinate the U.S. Government's and ISAF's strategic interests in ICT in Afghanistan; provide ICT expertise to advise and assist Afghanistan's public ICT institutions; assist and support the private ICT sector as needed; and gain and maintain informed situational awareness across the Afghan ICT ecosystem to create synergies among activities and initiatives of various stakeholders. Its mission was to facilitate the further development of the ICT sector and assist the Afghan government in employing ICT to enable governance, stability, and socio-economic development.

The DISA-sponsored STA/TAT operated at ISAF Headquarters in Kabul from July 2010 to October 2014. STA leadership rotated roughly every year, with the civilian SES being replaced by U.S. Army colonels in years 2 and 3 before reverting to a senior civilian during its final 16 months or so of operation. The types and lengths of deployments of CEW personnel varied, which led to continuous training and team-building. The frequent rotations of CEW personnel and the resultant changes in areas or levels of expertise unfortunately hindered efforts to build peer-to-peer relationships with Afghan ICT counterparts. The support contractors were embedded at the Ministry of Communications and Information Technology (MCIT) compound, where ATRA and AfTel were also located, which allowed them to maintain a consistent presence, build and nourish relationships, participate in ad hoc and drop-in meetings, and work with their counterparts day in and day out.[52]

DISA formally established and led a CONUS-based reachback team to support the STA/TAT, which included DISA, DOD CIO (formerly ASD-NII), NDU CTNSP, Gartner, and Deloitte CONUS. The team played an important role in harmonizing activities across the U.S. interagency community and telling the STA/TAT's story in and around Washington, DC, and elsewhere. Reachback worked areas of interest to the STA/TAT and the broader U.S. Government and engaged in activities with Afghans and other relevant parties and stakeholders in theater and CONUS, including with international organizations such as the World Bank.

During its first year of operation, the STA/TAT socialized its existence, intentions, plans, and goals with the civil-military participants, donor community and aid agencies, Afghan public sector officials, commercial companies, academia, and other ICT stakeholders. It also conducted and published a comprehensive current-state assessment of ICT in Afghanistan. This evaluation

laid the groundwork for the STA/TAT's development of four primary strategic pillars of engagement: terrestrial ICT backbone, cellular service coverage, ICT to support the extension of legitimate governance and stability operations, and ICT to support socio-economic, growth, and capacity development. The STA/TAT became recognized as key members of the U.S. Government, ISAF, and Afghan stabilization teams. Quite significantly, the STA/TAT was successful in having ISAF and the Afghan government recognize ICT as critical infrastructure and an essential service, and they were able to include ICT in ISAF's official operations plan (as an appendix to the Stability Operations annex). ICT remained a component of successive ISAF campaign plans thereafter.

Building on that foundation and momentum, in its second year, the STA/TAT developed and published an official strategy predicated on two primary lines of effort: sustainability of the ICT sector and ICT as an enabler of stability. Both lines of effort included overarching initiatives and desired endstates. In the third year, the STA/TAT tweaked the strategy in response to changes in mission objectives and to reflect the operating environment, needs, and capabilities of the time. By the STA/TAT's fourth year, ISAF was in full drawdown mode because of former President Obama's order to cease combat operations by the end of 2014. ISAF's focus narrowed to training, advising, and assisting Afghanistan's security entities, to the exclusion of most other activities. Consequently, the STA/TAT tapered off, limited its efforts, and reorganized its remaining work under two main categories: security force assistance and civil ICT support.
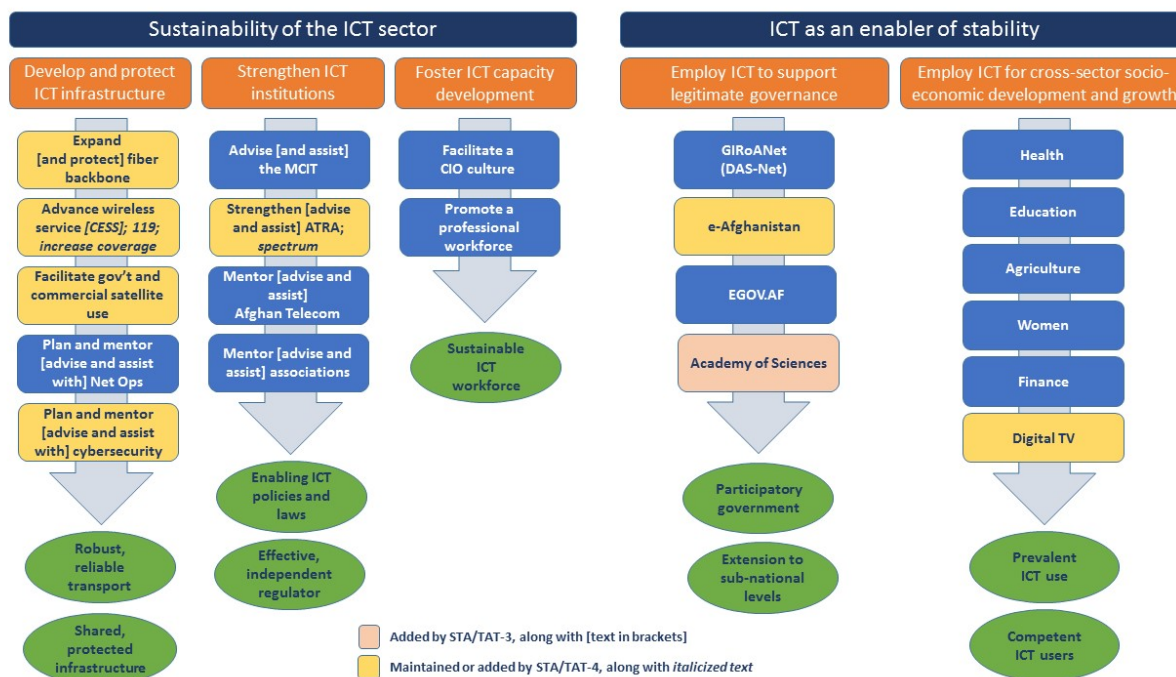

Figure 2. STA/TAT Afghanistan ICT Strategy

Similar to how the elimination of the STA position was an unintended consequence of the dissolution of the ARG, the transition of ISAF to NATO's follow-on Resolute Support Mission (RSM) resulted in the STA/TAT entity and its reachback team ceasing operations in October 2014. While the STA/TAT was a U.S. entity operating at ISAF, it got caught up in ISAF's

transition planning and drawdown. The State and Defense Departments made a verbal agreement (before the reincarnation of the STA at ISAF) for State to assume the TA function from the DOD in the future. With the dissolution of the STA/TAT entity, the U.S. Embassy Kabul ECON section, whose portfolio includes telecommunications, was given responsibility for the TA function but no resources to execute it other than as another duty as assigned. ICT was not one of the Embassy's or ECON's top interest areas and it had to compete with higher-priority initiatives. The STA/TAT transitioned responsibility for a few of its tasks and projects-in-progress to the RSM or the Afghans. The TAT's civilian ICT contractors moved to the RSM CJ6/Train, Advise, and Assist (TAA) element for the duration of their contract until March 2015 and continued working a limited scope of ICT issues. USFOR-A subsequently contracted with civilian ICT experts to continue their support to RSM CJ6/TAA through January 2016. Although another attempt was made to continue ICT civil support activities in addition to the CJ6 TAA military support, much of the STA/TAT's original work program was aborted or abandoned when the office was closed in 2014.

Both experiments to provide civil and commercial ICT advice in Afghanistan—the ARG STA and the STA/TAT—were largely considered successful. They made substantial and significant accomplishments in the areas of ICT sector governance; infrastructure deployment, protection, and use (particularly Afghanistan's national fiber network); spectrum management and transition; the advancement of ICT services (notably 3G mobile broadband, wireless broadband, and satellite); ICT associations; and human ICT capacity development. Furthermore, they fostered, enacted, and supported numerous efforts to employ ICT for governance, such as second-generation government networks and the national electronic identity card and to utilize ICT in finance, for healthcare, in education, and to promote gender equality. Their efforts were impactful and made a difference in several key ICT areas of concern to the U.S. Government, the coalition, the international community, and the Afghans. Both the ARG STA and the STA/TAT served as one-stop shops for situational awareness of the Afghan ICT sector, the use of ICT by other sectors, and commercial ICT advice. They were harmonizers, connecters, and facilitators across the various participants of the complex civil-military ICT ecosystem. Both organizations demonstrated the value of having in-country U.S. Government civil and commercial professional ICT expertise and employing a more holistic approach to ICT sector recovery in post-conflict operations. Both of the STA ARG and the STA/TAT experiments included CONUS-based reachback elements, thus operated as distributed virtual teams. This arrangement provided great benefits but also posed many challenges. Nevertheless, the reachback teams were integral to the success of both the STA ARG and the STA/TAT and, among other valuable functions, provided continuity of operations and institutional memory for both. Reachback support should be included in deploying forward an STA position to execute TA functions in future operations.

An important attribute of the ARG is that it was created by and reported to senior U.S. Government civilian leaders such as the Director of the NSC, the Secretary of Defense, and his key senior advisor at the Pentagon ARO. The STA/TAT benefited from different top cover; it had senior civilian and military leaders from the Deputy Assistant Secretary of State for International Communications and Information Policy in the Economic and Business Affairs Bureau, the USAID administrator for the Office of Afghanistan and Pakistan Affairs, the DOD CIO, and the Director of DISA. Civilian-led operations are best aligned with civilian leadership and military-led operations with military leadership.

A key aspect of the STA/TAT arrangement is that it was a U.S. DOD entity and, as such, it operated under military (both U.S. Government and ISAF) rules—which were not as limiting as those of the State Department—for operations in hostile areas. State tends to be more risk averse and limits freedom of movement, whereas militaries provide force protection as standard operating procedure. However, being identified with military elements had its drawbacks, such as when the STA/TAT showed up at the MoC—or elsewhere—with military members of the team in uniform and with weapons. The decision to deploy two U.S. Army colonels as TAT directors in the second and third years—in contrast to SES civilians in the first and fourth years—resulted in a change in organization reporting in the ISAF chain of command (from commander ISAF level to Deputy Chief of Staff for Stability Operations) and decreased the STA's visibility to and engagement with senior U.S. Government and ISAF officials.

Another differentiator between the ARG STA and the STA/TAT was the STA/TAT's use of professional commercial ICT experts. The civilian contractors lived and worked in Kabul and had relative freedom of movement and the flexibility to more fully engage with their Afghan counterparts than other U.S. Government civil-military personnel. This was especially true when threat levels increased because the contractors had their own armed security protection and were able to continue to operate relatively unencumbered. In the first year of the STA/TAT operation, U.S. Government civilian and military personnel also embedded at various ICT entities and had quite a measure of mobility, but as the security situation deteriorated beginning in the fall of 2011, both ceased and off-compound visits were tightly controlled. In early 2012, ISAF increased its force protection posture and required armed guards to accompany all personnel traveling off base. In the STA/TAT's case, this meant armed escorts, generally other TAT members, sat in on their meetings with Afghan civilians, which was not well-received. Resultantly, and also due to the additional demands on TAT personnel, visits became shorter and less frequent. To complicate the situation further, Former President Hamid Karzai outlawed private security companies in March 2013. Between that and the elevated threat environment, the company that supplied the civilian ICT contractors to the STA/TAT made a corporate decision to remove its personnel from the country. DISA contracted a replacement, but the process left the STA without professional commercial ICT support in-country for 6 months. The original contractors joined the reachback team and fulfilled the duration of their obligation stateside.

The above is neither the sum total of the ARG STA's or STA/TAT's work or accomplishments nor lessons observed from those experiments. What is clear, however, is the use of an ICT advisory capacity can yield tangible benefits to the warfighter and the affected nation. To successfully operate in post-conflict environments like Afghanistan, we need to have a substantial, well-thought out, and well-resourced civilian effort comprising professional civil and commercial ICT experts. Planners need to begin with the end in mind and specifically address when and how to manage the transition of the lead for ICT responsibilities from civil to military personnel and back. Planners and ICT advisors together must proactively devise arrangements for the disposition of ICT activities, manage the turnover of ongoing efforts to the affected nation to assume and sustain, and organize follow-on advice and assistance. The need for further ICT support does not go away because we do.

The use of ICT in post-conflict operations has demonstrable, evidence-based benefits. ICT has been proven to be an effective tool—perhaps the most effective—to help achieve security, stability, reconstruction, and development goals. Even the U.S. Government admits it is now well-established that Internet connectivity is one of the most important drivers of economic growth and opportunity, which, in turn, leads to stability, peace, and prosperity.[53] Accordingly, it has embarked on an effort to increase Internet penetration and use in the United States and abroad.

Bridging the Digital Divide: The Global Connect Initiative

The information age allows people to use mobile phones, the Internet, social media and professional networking accounts, computers, tablets, and other devices and applications to digitally collect, store, analyze, and share just about anything, anytime, anywhere. However, the Internet remains unavailable, inaccessible, and unaffordable to a majority of the world's population.[54] According to the World Bank, the digital dividends—the benefits from using these technologies—are unevenly distributed between developed and developing countries, urban and rural areas, and males and females.[55] This *digital divide* is evident in Afghanistan, as indicated in the table, which compares the number of Internet users in Afghanistan to Internet users in neighboring and similarly poor countries. As the table illustrates, Afghanistan has significantly lower Internet penetration than all its neighbors and ranks above only Guinea in Internet penetration among comparably impoverished nations.

The digital divide in Afghanistan also manifests itself it terms of gender. Afghan males are twice as likely as females to have mobile phones and three times as likely to have personal access to the Internet.[56] Four times as many Afghan males use computers.[57] Of Afghanistan's 3 million monthly active Facebook users, 86 percent are male and only 14 percent are female.[58] The World Bank asserts that access to digital technologies for everyone requires closing the remaining digital divide, especially in Internet access.[59]

Closing the digital divide is a priority for the U.S. Government.[60] The Global Connect Initiative, a multi-stakeholder effort launched in September 2015 and led by State Department, aims to bring 1.5 billion new Internet users online by 2020 by stimulating the expansion of ICT infrastructure, both in the United States and in other countries.[61] Robert A. Kinn, former FCI senior information analyst supporting the DOD CIO Information Enterprise, Architecture, and Engineering Office and DOD CIO representative to the GCI working group, noted GCI has survived multiple reviews by the Trump administration as of mid-2017.

The *five categories of action* under the Global Connect Initiative are: expanding international cooperation on connectivity, strengthening the financing of connectivity, implementing development assistance, building capacity on technical and regulatory best practices, and developing stakeholder partnerships.[62] According to the World Bank, greater digital adoption will not be enough. To get the most out of the digital revolution, countries also need to work on the *analog complements* by strengthening regulations that ensure competition among businesses, adapting workers' skills to the demands of the new economy, and ensuring that institutions are accountable.[63]

What Needs to Be Done

The U.S. Government has taken an important first step in acknowledging the socio-economic and development benefits of ICT. Nevertheless, it has a long way to go in recognizing the importance of ICT in post-conflict operations and doing something about it. The ICT sector is one among many competitors for the attention of policymakers and practitioners in the complex reconstruction context. It merits more attention than it has been paid.[64]

Table. Afghan Internet users compared to neighboring and similarly poor countries, 2016 (Internet Live Stats)

Afghanistan versus Neighboring Countries					
	Pakistan	**Uzbekistan**	**Afghanistan**	**Tajikistan**	**Turkmenistan**
Country rank based on number of Internet users	20	37	99	114	134
Population	192,826,502	30,300,446	33,369,945	8,669,464	5,438,670
Number of Internet users	34,342,400	15,453,227	2,279,167	1,622,924	789,151
Percentage of population using the Internet	17.8%	51.0%	6.8%	18.7%	14.5%
Number of non-users (Internetless)	158,484,102	14,847,219	31,090,778	7,046,540	4,649,519
Increase in number of Internet users, one year	3,024,054	893,596	101,366	67,230	47,737
Percentage change in Internet users, one year	9.7%	6.1%	4.7%	4.3%	6.4%
Percentage change in population, one year	2.07%	1.36%	2.59%	2.21%	1.21%

Afghanistan versus Similarly Poor Countries*					
	Liberia	**Guinea**	**Afghanistan**	**Togo**	**Uganda**
Rank on IMF poorest countries list	10	11	12	13	14
Country rank based on number of Internet users	145	158	99	138	50
Population	4,615,222	12,947,122	33,369,945	7,496,833	40,322,768
Number of Internet users	395,063	236,932	2,279,167	545,020	7,645,197
Percentage of population using the Internet	8.6%	1.8%	6.8%	7.3%	19.0%
Number of non-users (Internetless)	4,220,159	12,710,190	31,090,778	6,951,813	32,677,571
Increase in number of Internet users, one year	53,123	10,688	101,366	49,352	395,857
Percentage change in Internet users, one year	15.5%	4.7%	4.7%	10.0%	5.5%
Percentage change in population, one year	2.48%	2.68%	2.59%	2.63%	3.31%

Per the International Monetary Fund, based on GDP per capita, current prices, 2016 (US dollars)

Successful approaches to leveraging the role and use of ICT in post-conflict reconstruction need to be rooted in a thorough understanding of the affected nation's national political, legal, economic, social, cultural, and communications contexts.[65] Civil-military interveners, international and non-governmental organizations, as well as donors, aid agencies, and the myriad other post-conflict participants need to have an informed understanding of an affected nation's ICT landscape and components. It is important to understand the overarching communications culture, including government practices, supply chains, and business processes, both formal and informal. They need to know who makes things happen in the ICT sector and who the spoilers are. In post-conflict environments, there are often nefarious state actors and countries whose strategic interests may not align with ours. This is certainly the case in Afghanistan, where Pakistan, Iran, and China have all garnered substantial pieces of the ICT pie. There needs to be the equivalent of an intelligence preparation of the battlespace for the ICT sector. Along those lines, the U.S. Government should consider sponsoring a team of civil and commercial ICT experts to research ICT governance, infrastructure, services, and players in countries of interest on an ongoing basis. This team would also establish and maintain

relationships with principal ICT counterparts of those countries and within the international community, thereby having *go to* points of contact before an engagement.

There is an urgent need for the U.S. Government and the international community to establish OCONUS policy and doctrine regarding the role, importance, and use of ICT in post-conflict operations. The U.S. Government must also institutionalize its approach for having and providing professional advice and assistance on civil and commercial ICT matters. Specifically, the U.S. Government must:

- formally recognize ICT as fundamental to future OCONUS security, stability, reconstruction, and development missions and include ICT in formal planning for such
- designate ICT as critical infrastructure and an essential service and give ICT priority, with regard to planning, resource allocation, and funding, on par with roads, power, and water
- establish a lead agency for OCONUS ICT matters; define and agree on ICT roles, relationships, and reporting requirements; determine who has the ICT lead and when in post-conflict operations; and decide when and how to transition responsibilities back and forth (civil-military-civil)
- institutionalize an OCONUS ICT advisory capability, similar to approaches used in Iraq and Afghanistan and incorporate lessons from all
- agree upon and implement cooperative OCONUS ICT-related arrangements with the international community and coordinate in advance with their responding ICT stakeholders.

The ICT advisory capability would be the U.S. Government's voice for all ICT-related matters and include a senior spokesperson to deal with civil-military leadership of the intervening forces and governments, the international community, and the affected nation. The ICT experts should be facilitators, connectors, and harmonizers, as well as the trusted source of informed situational awareness, strategic thinking, and thought leadership pertaining to ICT matters and efforts. Civil-military interveners need to know how to work together to leverage ICT to meet their and the affected nation's strategic and tactical communications needs and employ ICT as an enabler of security, governance, and cross-sector socio-economic development and growth *before* an intervention, rather than learning during the intervention. To that end, the U.S. Government should implement agreed-upon ICT-enabled information-sharing arrangements that facilitate collaboration, coordination, and information-sharing within the U.S. interagency community and with and among international civil-military partners and affected nation counterparts in post-conflict operations. Further, it is important the U.S. Government and the international community develop strategic communications plans to conduct influence operations, effectively manage expectations—both their own and those of the affected nation—and report progress.

Another consideration for the U.S. Government and the international community in future post-conflict planning is knowing when to intercede with an ICT advisory capability. Ideally, it should be during the so-called *golden hour*,[66] during which the interveners can most easily accomplish recovery and reconstruction in the affected nation. The golden hour is after significant hostilities have ceased but before the public mindset shifts from viewing the interveners as occupiers rather than liberators. Civil-military interveners need to be cognizant of

the local population's needs, desires, expectations, capabilities, and limitations and view them through the eyes of those they are trying to help, rather than try to shape the affected nation's priorities and options according to their own experiences and beliefs.

To achieve their security, stability, reconstruction, and development goals, now and in the future, the U.S. Government and the international community must acknowledge, accept, and take action to elevate the role and importance of ICT in post-conflict operations. They must fully incorporate ICT into all phases of interventions: planning, execution, drawdown, and transition. They must define in advance the conditions for success for ICT to support the warfighter effectively and benefit the affected nation substantially. The U.S. Government and the international community should develop holistic approaches and establish frameworks for ICT-enabled interventions. This methodology should include assessing the civil and commercial ICT environments of countries of interest, developing guidelines for recovering and rehabilitating the ICT sector, and creating implementation roadmaps complete with existing resources for known challenges and benchmarks to assess progress. No two countries are alike, so a rigid, one-size-fits-all approach will not work. With the volume of case studies accumulated to date,[67] a flexible blueprint of options with anticipated outcomes would be sufficient to guide ICT sector recovery work. All efforts should be driven by policy goals of the U.S. Government and the affected nation and conditions on the ground. However, first-order priorities should include consideration of spectrum management; ICT-enabled information-sharing; effective ICT sector governance; the early deployment of ICT solutions to enable communications to support governance, humanitarian assistance, and emergency services; early rehabilitation or installation of commercial ICT infrastructure and services to support the interveners C4ISR needs and the communication needs of the affected nation; and human ICT capacity development to maintain and evolve the ICT sector.

Conclusion

ICT has proven to be a basic enabler of informal social and economic discourse, leading to a strengthening of civil society and the promotion of security, internal stability, job creation, social services, and economic solidity in affected nations. It has become a demonstrated enabler of national transformations as we saw in Afghanistan.[68] The ICT sector was one of the country's biggest and most visible success stories. For many years, the ICT sector was the largest contributor to the Afghan government's coffers through revenue generated from private investment, taxes, and license and spectrum permit fees. ICT was ultimately surpassed by transportation and civil aviation, but it still ranks high among Afghanistan's most viable legitimate industries.

Since former President Obama's announcement that combat operations would cease by the end of 2014, precipitating the drawdown and transition—or lack thereof—of DOD-sponsored ICT train, advise, and assist activities to other U.S. elements or the Afghans, we predicted problems for the ICT sector. Challenges include, but certainly are not limited to, the shifting of NATO, U.S. Government, and international community support away from ICT and toward other sectors; a deteriorating security situation, including threats and attacks against ICT personnel and facilities; a lack of reliable power for ICT equipment; spectrum interference and poor spectrum management; and the flight of human technical, management, and other capital.

The installation of Afghanistan's National Unity Government in September 2014 precipitated changes in ICT sector leadership, decisionmaking, and business processes, all of which impacted the governance and continued modernization of the ICT sector, the use of ICT in other sectors, and the provision of ICT services. The top positions at the MCIT, ATRA, and Afghan Telecom have all turned over, some more than once. Many other high-ranking personnel at all three departed; some were fired, while others resigned. ATRA now reports directly to the Office of the President, which, on its face, is a positive change, because sector regulators should be independent. However, President Mohammad Ashraf Ghani Ahmadzai has added several ICT advisors and demonstrated increased interest in how the ICT sector is run. These reforms have created confusion as to who is responsible and accountable for ICT sector governance. Further, ministry management authority and internal decisionmaking have been eroded. As a result, the ICT sector lacks clear guidance, direction, management, and oversight. This turmoil has prompted donors such as USAID and the World Bank to temporarily withdraw financing for Afghan ICT projects.

Changes in business processes, like a new requirement for government entities to use the National Procurement Authority (NPA) for purchases exceeding $100,000 have introduced bureaucratic-driven delays in acquisitions. This condition has affected state-owned AfTel's ability to obtain needed materiel to maintain and upgrade its ICT infrastructure. Further, AfTel's ability to support and expand ICT services such as wireless data has been degraded, diminishing its already lacking effectiveness to compete with private sector operators. Other government organizations have suffered an exodus of ICT-savvy skills and are also affected by the requirement to use the NPA for their high-dollar ICT purchases.

Private ICT companies, namely the mobile network operators (MNOs) and ISPs, are suffering from upheaval in the ICT sector as well, all while their actual and addressable customer bases continue to shrink and their revenues decline. Additionally, insurgents have knocked out a third of Afghanistan's cellular towers, and they restrict the operational territory and hours of use. As a result, MNOs have shut down hundreds of cellular towers around the country because of the high cost of security to protect them, coupled with reduced revenues in those areas.

Political power struggles and divisions and a deteriorating security situation are eroding consumer and investor confidence alike, further slowing economic growth. The Afghan Chamber of Commerce and Industries reported kidnappings of businessmen in the private sector increased 5 percent in the first 6 months of 2017, which has resulted in a 40 percent drop in investment in the country.[69] Weaker (than past) performance of the ICT sector, once a cash cow, is a negative influencing factor, compounding economic woes. For the 2007 fiscal year, the ICT sector accounted for 20 percent of all receipts by the Afghan treasury, largely from taxes and spectrum and license fees.[70] That contribution dropped to 10 percent as transportation and civil aviation increased, but they are still significant figures.[71] To combat declining ICT sector revenues, the Ghani administration imposed a 10 percent top-up tax (per SIM card recharge), which has eroded mobile phone usage even further. A sector that was once praised for its successes and touted as a model can no longer claim that title. Gains of the past 15 or so years have begun to slip away. Such a shift could have significant unintended consequences, especially since the ICT sector is ill-prepared to sustain operations on its own without the support and attention of the international

community.[72] The swift and significant decline of the ICT sector illustrates the requirement for ICT advisory support to continue beyond the withdrawal of warfighters. The Afghans' need for ICT assistance did not disappear because we decamped.

Afghanistan began its *Decade of Transformation* with the confluence of three major transitions—security, governance, and the economy—occurring at the same time.[73] One might think managing this triad simultaneously would be Afghanistan's greatest challenge. However, another trio—the Taliban, al Qaeda, and the so called Islamic State—is far more troubling to both Afghanistan and the United States. Instability and uncertainty, coupled with war weariness and donor fatigue, are preventing the U.S. Government and the international community from further engagement and investment in the Afghan ICT sector at a time when it is as important as ever to fully and effectively leverage ICT to meet the coalitions' and Afghans' communications needs. If conditions continue to worsen, it could tip the risk-reward ratio so that some of Afghanistan's commercial ICT companies give up and pack it in. That could snowball into a slow downward death spiral for the private sector and even the ICT sector as a whole and leaves room for the Chinese, Russians, and Iranians to step in to fill the gap (which is currently occurring). Afghan leaders are embracing them as defense against the United States.[74]

The success of post-conflict operations in general, and Operation *Enduring Freedom* in particular, are heavily dependent on a mature or maturing civil and commercial ICT sector. The sector must be able to provide civil-military interveners, other post-conflict participants, and the affected nation with ICT infrastructure, connectivity, services, applications and therefore, access to and the ability to collect and share information and attain information dominance. Achieving these ends will require continued support from the U.S. Government and the international community. As President Donald Trump implements a new strategy to prevail in Afghanistan, he and the international community should consider ICT another weapon in their war chest and an ICT advisory element as a core mission capability.

In Afghanistan, technology has created a cultural shift that could turn out to be more powerful than any militia.[75] If we had arrived in early post-conflict Afghanistan with a formal OCONUS ICT policy and associated doctrine and a concerted plan to utilize ICT to enable security, governance, social development, and economic growth—those elements that propel stability, peace, and prosperity—we may not still be there today. It is up to the U.S. Government and the international community to take action to leverage ICT for success in Afghanistan and future post-conflict operations. It is not a matter of nation-building but of urgent national security.

Notes

[1] Larry Wentz and Karen E. Black, eds., *Analysis of an Intervention: Lessons from U.S. Advisory Work in Afghanistan's Information and Communications Technology Sector* (Washington, DC: Center for Technology and National Security Policy, 2017), available at <http://inss.ndu.edu/Media/News/Article/1258699/analysis-of-an-intervention-lessons-from-us-advisory-work-in-afghanistans-infor/>.

[2] International Telecommunication Union, "SMS4DC: Spectrum Management System for Developing Countries, Version 3: Spectrum Management Fundamentals; Part 1: International." (Powerpoint presentation), available at <https://www.itu.int/en/ITU-R/seminars/rrs/RRS-13-Africa/Documents/Tutorial/SM_Fundamentals_Part1.pdf>.

[3] Portions of the paragraph are paraphrased from Dr. Chi Nche and Karen E. Black, "Radio Spectrum in Post-Conflict Environments and Stability Operations—Afghanistan: A Case Study" in Wentz and Black, *Analysis of an Intervention*, 383–428.

[4] Ibid.

[5] Chickasaw Nation Industries Technical Services (CNITS), LLC, *Research and Analysis Project for UNCLASSIFIED Information Sharing in Afghanistan: A Model for US Military and Coalition Commanders, the US Intelligence Community, and US Homeland Security,* (Albuquerque, NM: CNITS, January 28, 2011, 28.

[6] Ibid, i.

[7] Ibid, 31.

[8] Paraphrased from Oliver Dziggel, "ICT Policy and Regulatory Framework," in Wentz and Black*, Analysis of an Intervention*, 297–324.

[9] Ibid., 320.

[10] "USAID/OTI and Codan: Helping to rebuild lives in Afghanistan," codanradio.com, available at <www.codanradio.com/wp-content/uploads/2012/06/afghanistan_casestudy.pdf>.

[11] Ibid.

[12] World Bank, *Afghanistan - Emergency Communications Development Project* (Washington, DC: World Bank, 2003), available at <http://documents.worldbank.org/curated/en/391521468740673621/Afghanistan-Emergency-Communications-Development-Project>.

[13] Worldwide Interoperability for Microwave Access, a family of wireless communications standards that enables the delivery of last-mile wireless broadband Internet service.

[14] Based on contributions from Lane Smith, formerly of USAID, who worked on the GCN and DCN projects.

[15] Code division multiple access is a method used by some radio communications technologies that makes it possible for several transmitters to send information over a single communications channel simultaneously, thereby allowing multiple users to share finite frequency bandwidth without interference.

[16] Paraphrased from Dziggel, in Wentz and Black*, Analysis of an Intervention*, 298.

[17] Paraphrased from Dr. Maria Beebe and Karen E. Black, "The TAT's Efforts to Foster ICT Capacity Development," in Wentz and Black*, Analysis of an Intervention,* 639–683.

[18] Ibid, 659.

[19] Development Alternatives, Inc. (DAI), *Afghanistan Technical and Vocational Education Training (TVET) Providers Inventory* (Washington, DC: USAID, November 2011), 20, available at <http://pdf.usaid.gov/pdf_docs/pnaea952.pdf>.

[20] Afghan salary data supplied by a U.S. Government IT/ICT expert contractor who received data from Afghan companies in September 2017. U.S. salary data from "IT Technician Salaries in the United States," Indeed.com, available at <www.indeed.com/salaries/IT-Technician-Salaries>.

[21] Nidhi Tandon, *A Bright Future in ICTs: Opportunities for a New Generation of Women*, International Telecommunication Union, February 2012, vii, available at www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Documents/ReportsModules/ITUBrightFutureforWomeninICT-English.pdf>.

[22] Dr. Hamadoun I. Touré, "Welcoming Remarks," International Girls in ICT Day 2012, New York, April 26, 2012, available at <www.itu.int/en/osg/speeches/Pages/2012-04-26.aspx?>.

[23] Beebe and Black, "The TAT's Efforts to Foster ICT Capacity Development," in Wentz and Black, *Analysis of an Intervention*, 639.

[24] Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales from the Pentagon* (New York: Simon and Schuster, 2016).

[25] Kathy Gilsinan, "We Have No Idea What War Is," *The Atlantic* (August 10, 2016), available at <www.theatlantic.com/international/archive/2016/08/rosa-brooks-war-military/494846/>.

[26] Dr. Frank G. Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," *2016 Index of U.S. Military Strength* (Washington, DC: The Heritage Foundation, 2016), available at <http://index.heritage.org/military/2016/essays/contemporary-spectrum-of-conflict/>.

[27] Ibid.

[28] Brooks.

[29] Ibid.

[30] Gilsinan.

[31] Brooks.

[32] Ibid.

[33] See the following: Deloitte, *What is the impact of mobile telephony on economic growth*, November 2012, available at <www.gsma.com/publicpolicy/wp-content/uploads/2012/11/gsma-deloitte-impact-mobile-telephony-economic-growth.pdf>; Deloitte, *Economic Impact of Mobile Communications in Serbia, Ukraine, Malaysia, Thailand, Bangladesh and Pakistan*, January 2008, available at <www.telenor.rs/media/TelenorSrbija/fondacija/economic_impact_of_mobile_communications.pdf>; and Vodafone, *Africa: The Impact of Mobile Phones,* The Vodafone Policy Paper Series, no. 3, March 2005, available at <www.itu.int/osg/spu/dtis/documents/Papers/vodafonepapers.pdf>.

[34] See the following: World Economic Forum, "ICT for Economic Growth: A Dynamic Ecosystem Driving the Global Recovery," (2009), available at <www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf>; World Bank, *Information and Communications for Development: Extending Reach and Increasing Impact,* 2009, available at <https://openknowledge.worldbank.org/handle/10986/2636>; and Deloitte, *What is the impact of mobile telephony on economic growth*.

[35] ITU4U, "Digital Divide Progress Report: 15 Year Review," *itublog*, August 26, 2015, available at <https://itu4u.wordpress.com/2015/08/26/digital-divide-progress-report-15-year-review/>.

[36] GSM Association, *The Mobile Economy in 2016*, Summary Extract, available at <www.gsmaintelligence.com/research/?file=e888862e19a8097c48291a8f66b4ddc5&download/>.

[37] Ibid.

[38] Rob Atkinson, "ICT and Innovation: Powering National Economic Growth." (presentation at Boeing's Leading and Nurturing a High Tech Enterprise event, St. Louis, MO, December 6, 2010).

[39] Statistics from December 2015 are the most recent reliable numbers the authors have from the Afghanistan Telecom Regulatory Authority (ATRA), the official ICT statistics collector and publisher. ATRA no longer has current figures on its website and those on the Ministry of Communications and Information Technology's website are from September 2015.

[40] Zachary Warren et al., eds., *Afghanistan in 2016: A Survey of the Afghan People*. (San Francisco, CA: The Asia Foundation, 2017), 131–133, available at <http://asiafoundation.org/wp-content/uploads/2016/12/2016_Survey-of-the-Afghan-People_full-survey.Apr2017.pdf>.

[41] Adapted from a chart on the Islamic Republic of Afghanistan Ministry of Communications and Information Technology's website, available at <http://mcit.gov.af/Content/images/Eng%20-%20Internet%20Users.png>.

[42] Zachary Warren and Nancy Hopkins, eds., *Afghanistan in 2015: A Survey of the Afghan People* (San Francisco, CA: The Asia Foundation, 2015), 11, available at <www.asiafoundation.org/resources/pdfs/Afghanistanin2015.pdf>.

[43] Ibid.

[44] Ziaulhaq Ateed, "Social media use in Afghanistan jumped 43 percent in 2016," 1TVnews.af, September 2, 2107, available at <http://1tvnews.af/en/news/afghanistan/27738-social-media-use-in-afghanistan-jumped-43-percent-in-2016>.

[45] Neha Sahgal, "Among Muslims, Internet Use Goes Hand-in-Hand with More Open View Toward Western Culture," Pew Research Center (blog), May 31, 2013, available at <www.pewforum.org/2013/05/31/among-muslims-internet-use-goes-hand-in-hand-with-more-open-views-toward-western-culture/>.

[46] John Reed, "Let freedom ring: Gen. Cartwright says 4G *[sic]* is America's lasting legacy in Afghanistan (Updated)," *Foreign Policy* (January 24, 2013), available at <http://foreignpolicy.com/2013/01/24/let-freedom-ring-gen-cartwright-says-4g-is-americas-lasting-legacy-in-afghanistan-updated/>.

[47] Deloitte, "Value of Connectivity: Economic and social benefits of expanding internet access," February 2014, 4, available at <https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology-media-telecommunications/ValorConectividade.pdf>.

[48] Franklin D. Kramer, Larry Wentz, and Stuart Starr, "I-Power: The Information Revolution and Stability Operations," *Defense Horizons,* no. 55 (February 2007), available at <http://handle.dtic.mil/100.2/ADA466767>.

[49] Ibid.

[50] The DOD CIO Information-Sharing Directorate's engagement with the Afghan ICT sector was driven by perceived needs to improve information-sharing as per its DODD/DODI 3000.05 (and other draft DODD/DODI documents), along with its interest in leveraging experiences in Afghanistan from 2004 onward to elevate ICT in and for U.S. Government OCONUS activities.

[51] The Civilian Expeditionary Workforce program recruits volunteer DOD employees to assist in overseas operations for assignments generally between 6 and 12 months, after which they return to their home organizations.

[52] The Ministry of Communications was renamed the Ministry of Communications and Information Technology in 2007.

[53] U.S. Interagency Steering Group, *The Global Connect Initiative: Accelerating Entrepreneurship and Economic Opportunity by Expanding Internet Access Globally*, December 2016, 6, available at <https://share.america.gov/wp-content/uploads/2017/01/Final-version-of-the-GCI-Report-2016-01-115PM.pdf>.

[54] World Bank, *World Development Report 2016: Digital Dividends* (Washington, DC: World Bank), available at doi: 10.1596/978-1-4648-0671-1., 8.

[55] Ibid, 200.

[56] Warren et al, *Afghanistan in 2016: A Survey of the Afghan People*, 131–133.

[57] Nancy Hopkins, ed., *Afghanistan in 2013: A Survey of the Afghan People*. (San Francisco, CA: The Asia Foundation, 2014), 12, available at <https://asiafoundation.org/resources/pdfs/2013AfghanSurvey.pdf>.

[58] Ateed.

[59] Deepak Mishra, et al., *World Bank Development Report 2016: Digital Dividends* (Washington, DC: The World Bank, 2016), 2, available at <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>.

[60] Global Connect Initiative, *U.S. Government Support for Companies Investing in the Information and Communications Technology (ICT) Sector*, available at <https://share.america.gov/wp-content/uploads/2016/04/4.-GCI-Interagency-Factsheet-FINAL.pdf>.

[61] Ibid.

[62] U.S. Interagency Steering Group, 6.

[63] *World Bank Development Report 2016,* 2.

[64] "Afghanistan," *2016 Index of Economic Freedom* (Washington, DC: The Heritage Foundation, 2016), available at <www.heritage.org/index/country/afghanistan>.

[65] Tim Kelly and David Souter, *The Role of Information and Communication Technologies in Postconflict Reconstruction* (Washington, DC, The World Bank, 2014), 40, available at <https://issuu.com/world.bank.publications/docs/9781464800740?e=0/6688927>.

[66] As observed, defined, and related by former Secretary of the Army Martin R. (Marty) Hoffman.

[67] Information and communication technology for development.

[68] Tarek Saadawi and Louis Jordan Jr., eds., *Cyber Infrastructure Protection* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, May 2011), 92–93, available at <https://ia600703.us.archive.org/30/items/CyberInfrastructureProtection_112/10-Cyber.pdf>.

[69] Zabihullah Jahanmal, "Investment Drops By 40% Due to Kidnappings: ACCI," TOLOnews.com, September 13, 2017, available at <www.tolonews.com/afghanistan/investment-drops-40-due-kidnappings-acci>.

[70] Islamic Republic of Afghanistan Ministry of Communications and Information Technology, *Afghanistan National Development Strategy: Information and Communication Strategy 1387–1391 (2007/08–2012/13)*, February 2008, available at

<http://mcit.gov.af/Content/files/ICT%20Sector%20Strategy%20-
%20English%20final%20Singed(2).pdf>.

[71] Islamic Republic of Afghanistan Ministry of Communications and Information Technology,
*The Ministry of Communication and ITs' [sic] activities and achievements report 1381–1393
(2002–2014)*.

[72] Larry Wentz, Frank Kramer, and Stuart Starr, *Information and Communication Technologies
for Reconstruction and Development: Afghanistan Challenges and Opportunities* (Washington,
DC: National Defense University Center for Technology and National Security Policy, January
2008), 48, available at <http://ctnsp.DODlive.mil/files/2013/07/DTP-045.pdf>.

[73] 2015–2024, as agreed at the Tokyo Conference on Afghanistan held July 8, 2012, and codified
in the Tokyo Declaration, "Partnership for Self-Reliance in Afghanistan: From Transition to
Transformation."

[74] As observed by a former advisor to the ISAF STA, who spent 10 years in Afghanistan across
multiple projects and sectors. His most recent ICT assignment was in early 2017.

[75] Farah Stockman, "Three reasons for hope in Afghanistan," *Boston Globe*, April 9, 2013,
available at <www.bostonglobe.com/opinion/2013/04/08/gambling-
pomegranates/dekCKppa3xT9QeEKGqEqlJ/story.html>.