

## Moore's Law: A Department of Defense Perspective

by Gerald M. Borsuk and Timothy Coffey

### Overview

The past 50 years have seen enormous advances in electronics and the systems that depend upon or exploit them. The Department of Defense (DOD) has been an important driver in, and a profound beneficiary of, these advances, which have come so regularly that many observers expect them to continue indefinitely. However, as Jean de la Fontaine said, "In all matters one must consider the end." A substantial literature debates the ultimate limits to progress in solid-state electronics as they apply to the current paradigm for silicon integrated circuit (IC) technology. The outcome of this debate will have a profound societal impact because of the key role that silicon ICs play in computing, information, and sensor technologies.

The consequences for DOD are profound. For example, DOD planning assumptions regarding total situational awareness have been keyed to Moore's Law, which predicts the doubling of transistor density about every 18 months. While this prediction proved to be accurate for more than thirty years, we are entering a period when industry will have increasing difficulty in sustaining this pace. Under the current device and manufacturing paradigm, progress in areas such as total situational awareness will slow or stagnate. If DOD planning assumptions are to be met, the DOD science and technology program would be well advised to search aggressively for alternate paradigms beyond those on which Moore's Law is based to ensure new technology capabilities. The purpose of this paper is to examine the current prognosis for silicon IC technology from a DOD perspective.

### The Current Situation

The integrated circuit electronics revolution can be said to have begun on February 23, 1940, when Russell Ohl of Bell Laboratories observed anomalous behavior of the electronic properties of a cracked silicon crystal. His investigation led to the discovery of what is now known as the *pn junction*. Ohl's interest was in developing a better crystal oscillator. He has commented that Bell Laboratories managers were not especially interested in his work and preferred that he focus

on issues related to vacuum electronics, where the real opportunities were perceived to lie. Fortunately, Walter Brattain was one of the first to review Ohl's discovery. Consequently, Bell Laboratories undertook a program to produce a solid-state switch to replace vacuum tube amplifiers and unreliable mechanical relays necessary for telephony. This program led to the discovery of the transistor in December 1947 by Brattain, John Bardeen, and William Shockley. In 1958, Jack Kilby invented and demonstrated an elemental integrated circuit composed of resistors and an active transistor device. Robert Noyce independently invented another form of the integrated circuit based upon silicon planar technology. At that point, the stage was set for the scientific and technical revolution in solid-state electronics that produced the tremendous capabilities in electronics, computers, communications, and information technology that we are experiencing today.

In 1965, Gordon Moore predicted that the number of active transistor devices on a silicon integrated circuit would double about every 12 months.<sup>1</sup> He based this prediction upon a log-linear plot of device complexity over time using just three empirical data points from his employer, Fairchild Semiconductor Corporation. In 1975, Moore revisited this topic at the Institute of Electrical and Electronics Engineers International Electron Devices Meeting. At that time, (presumably with knowledge of the technical attributes of silicon metal-oxide semiconductor [MOS] device scaling<sup>2</sup> and his own observations of improvements in silicon planar manufacturing technologies, including economy of scale and batch processing of silicon wafer), Moore revised his prediction, stating that transistor density would double about every 18 months. This prediction became known as Moore's Law. It must be remembered that this "law" is actually an empirical prediction, not a law of nature.

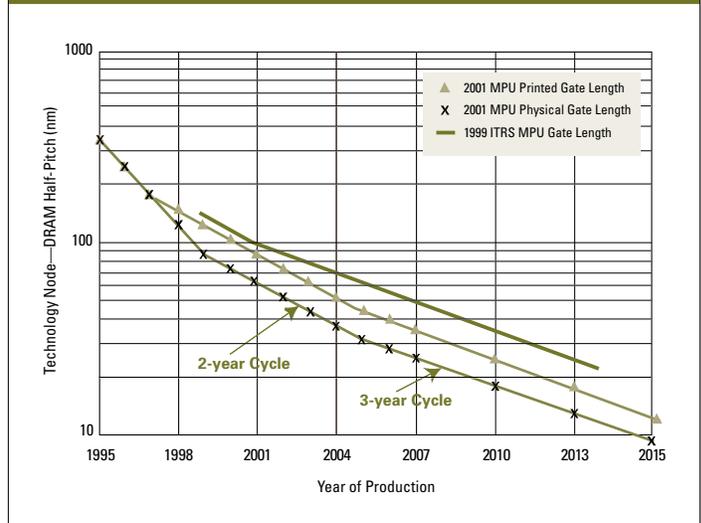
The semiconductor industry established Moore's Law as a goal in the development of ICs. The information technology industry uses it as a predictive tool to allow efficient planning of investments. Thus, Moore's Law became a self-fulfilling prophecy for the past 30 years.

Figure 1 plots integrated circuit gate feature size as a function of time in recent years and projects it into the future. The number of transistors that can be placed upon a given unit area increases as the inverse square of the feature size due to the technical attributes of device scaling. The ability of the semiconductor industry to reduce feature size continuously underlies the validity of Moore's Law and the enormous advances that have occurred in semiconductor electronics over the past 40 years. These advances in silicon integrated circuit electronics form the foundation of the great advances in computer capability and information and sensor technologies. To the extent that feature size reduction (and the resolution of all associated issues, such as other scaling attributes, on-chip interconnects, and manufacturing technologies) continues, Moore's Law will accurately predict these trends. If feature size reduction slows or fails for any reason, Moore's Law fails as a predictor, unless a viable paradigm other than feature size reduction is found. The question becomes that of determining the prognosis for continued feature size reduction and, if there are problems in this regard, assessing the prognosis for alternative paradigms. The stakes are high because we have progressed only about halfway on a log plot through the available feature size space of an integrated circuit, leaving available another three orders of magnitude in physical size reduction (assuming that the size of an atom sets the ultimate limit). Clearly, some signs of future difficulties are apparent. Three definitive regions can be discerned in the curves of figure 1. Through 1999, Moore's Law, on an 18-month cycle, prevailed. The slope starting in 1999 and predicted by the International Technology Roadmap for Semiconductors (ITRS) roadmap to continue to 2005 is one of a 2-year cycle time. From 2005 to 2016, a 3-year cycle time is projected.

DOD has depended on rapid advances in electronics of all types (for example, digital, radio frequency, mixed signal, and electro-optic) to maintain technological superiority. The department is expecting advances in electronics to continue this technological superiority indefinitely. However, potential problems are beginning to appear, specifically with digital ultra large silicon integrated (ULSI) circuits. To understand this, one must examine the paradigm on which Moore's Law is based. The law is rooted in the attributes of device scaling most simply expressed as the reduction in transistor active gate feature size and the so-called batch semiconductor manufacturing technologies necessary to make these ULSI circuits economically. A high yield of circuits with ever-increasing function complexity and performance has been the desired goal.

*Device scaling.* Silicon has played a predominant role in the progress of integrated circuits. This element is found in abundance in the Earth's crust, is relatively easy to purify and form into large boules, has excellent physical and electronic properties, and has the extraordinary attribute that a stable and electronically well-behaved oxide is easily formed on its surface. This oxide of silicon,  $\text{SiO}_2$ , is better known to most simply as glass or sand. A particular transistor

**Figure 1. IC Feature Gate Size**



device, the metal-oxide semiconductor field-effect transistor (MOSFET), and a particular circuit topology, namely the complementary metal oxide semiconductor (CMOS), have evolved to become the standard structures used in the scaling of the ULSI integrated circuit. No fundamentally new inventions were needed to undertake this scaling, which allowed industry to focus on the physics and fabrication science and technology of device scaling and not to be diverted by the need to invent a fundamentally new device.

Device scaling involves the scaling of the applied electric field, active channel lengths, junction dimensions and their electronic properties, insulator thickness, capacitance, and power dissipation—to name but a few of the geometric and material properties involved. The considerable innovation that has been required to accomplish device scaling should not be minimized. However, by maintaining focus on essentially one device type (although there were other device structures along the way, such as the bipolar transistor), one circuit topology (again, with several alternative topologies along the way, such as the n-channel MOS [NMOS], emitter-coupled logic [ECL], and integrated injection logic [I<sup>2</sup>L]) and a limited number of materials, industry was able to focus its creativity and resources. This in no small measure contributed to the rapid rate of progress over the past 40 years. The ability to fabricate well-behaved transistor switches was due to the fact that the properties of these devices did not demonstrate significant quantum mechanical properties. This situation is now changing. Scaling based simply upon Moore's Law is projected to approach atomic dimensions by the year 2050. However, it is generally accepted that the current device physics paradigm will not permit CMOS switching transistors with well-behaved characteristics with feature sizes on the order of several atoms. In fact, the silicon IC electronics community recognizes that the present paradigm will encounter problems long before 2050.<sup>3</sup>

A brief review of several scaling arguments suggests some of the concerns. The detailed scaling of MOS devices is well understood but is technically complex and beyond the scope of this paper. However, many of the essential aspects can be understood

**Timothy P. Coffey is a senior research scientist at the University of Maryland. He currently holds the Edison Chair for Technology at CTNSP. Gerald M. Borsuk is Superintendent of the Electronics, Science and Technology Division, at the U.S. Naval Research Laboratory.**

from simple geometric arguments involving such elementary concepts as electrical resistance and capacitance. The resistance of a wire, for example, increases with its length and decreases with its cross-sectional area. The capacitance of a structure increases with its cross section and decreases with the separation between the plates of the capacitor. The devices (integrated circuits) we are interested in are predominantly resistive/capacitive systems connected by an array of switches (transistors). Such interconnected switching systems have time constants characterized by the product of the effective resistance and the effective capacitance (generally referred to as the RC time constant). These simple concepts are sufficient to gain a rudimentary understanding of what has transpired in the evolution of microelectronics over the years and some of the key issues facing this field at this time. Two of the principal features of solid-state electronics are the length scales involved and the voltages used. Let us suppose that we scale a selective length by a factor  $\alpha$  such that a length  $L$  becomes  $L/\alpha$ . Similarly, scale voltage by a factor  $\beta$  such that a voltage  $V$  becomes  $V/\beta$ . Applying these simple geometric arguments to the key properties of wire-connected CMOS switching circuits creates table 1.

Before using table 1 for predictive purposes, it is reasonable to ask if it accounts for past developments. For example, in 1970, the feature size was about  $2 \times 10^4$  nanometers (nm). In 2000, it was about  $2 \times 10^2$  nm, resulting in an  $\alpha = 10^2$ . Table 1 would therefore predict that the transistor density should have increased by  $10^4$  over this time. In 1970, Intel microprocessors had about  $10^3$  transistors per die; hence, the prediction of table 1 for the year 2000 would be about  $10^7$  transistors (10 million) per die. The actual number was about twice this value. This is in reasonable agreement, considering that chip areas more than doubled over this time. In 1970, ICs performed at clock rates (the rate at which a chip's logic elements are toggled) of about  $2 \times 10^3$  cycles per second; hence, the prediction for 2000 would be about  $2 \times 10^9$  cycles per second ( $\sim 2$  gigahertz [GHz]), which is approximately correct. Table 1 provides merely a back-of-the-envelope guide to scaling and should not be used for more than that. In particular, table 1 does not permit *ab initio* calculation of the parameters. The initial parameters must be provided from experimental observation.

Keeping in mind the above caveat, table 1 can be used to illustrate some of the challenges facing the semiconductor industry today. The transistor clock rate in the central processing unit core of a microprocessor is about three GHz. These microprocessors perform about eight floating point calculations per clock cycle. Let us conduct a simple gedanken experiment that ignores the potential sophistication of computational architecture improvements. Assume, for the purpose of discussion, that one could reduce the feature size to the ultimate limit of one atom (that is,  $\sim 0.27$  nm for a silicon atom). Of course, the scaling shown in table 1 will break down well before this limit is reached. Therefore, the predictions do not represent reality. Nevertheless, they illustrate some of the problems that will be encountered as feature sizes approach the limit. Since feature sizes are about 130 nm in high-volume IC production, this size reduction would correspond to  $\alpha = 481$ . For this condition, table 1 predicts that microprocessor performance density would increase by a factor of  $\sim 100$  million. The clock rate (assuming it scales as the transistor cut-off frequency) predicted by table 1 would be more than a terahertz.

**Table 1: Geometric Scaling**  
(scale selected lengths by factor  $\alpha$ ; scale voltages by factor  $\beta$ )

Parameter	Scaling
Resistance at device level $R_D$	$R_{D0}\alpha$
Resistance of long wires $R_W$	$R_{W0}\alpha^2$
Capacitance at device level $C_D$	$C_{D0}\alpha^{-1} \kappa^*$
Capacitance of long wire $C_W$	$C_{W0}$
Charging time at local interconnect level $\tau_D$	$R_{D0}C_{D0} \kappa$
Charging time at long wire $\tau_W$	$R_{W0}C_{W0} \kappa\alpha^2$
Charging time through transistor $\tau_T$	$\tau_{T0}\alpha^{-1}$
Transistor frequency $f_T$	$\alpha/\tau_{T0}$
Energy per unit area $E_A$	$E_{A0} \beta^{-2} \alpha$
Energy per unit volume $E_V$	$E_{V0} \alpha \beta^{-2}$
Power per unit area $P_A$	$P_{A0} \beta^{-2} \alpha^2$
Transistor density (# transistors per unit area) $D_T$	$D_{T0} \alpha^2$
Performance density (transitions/sec) $f_T D_T$	$f_{T0} D_{T0} \alpha^3$

\*  $\kappa$  is scaled dielectric constant.

As a result, since instructions and data cannot move faster than the speed of light, one transistor at best could only interact with other logic elements that are within  $\sim 2 \times 10^{-2}$  centimeters (cm) of its location. For today's microprocessors operating at about 3 GHz, this maximum interaction length is on the order of 10 cm. This implies that, for today's chips, instructions and high-speed data can be moved across the entire chip each cycle. (In reality, other limitations, such as transistor current drive and interconnect line charging time, place more practical limits on transmission lengths of the highest speed signals for today's ULSI ICs.) Obviously, this architectural approach will break down long before reaching feature sizes of the order of one atom. Dealing with this issue will involve a substantial change in the prevailing paradigm (for example, moving to computing architectures that are highly local in character). While it may be possible to accommodate this need, the accommodation will be done by introducing greater complexity, thereby potentially jeopardizing the present scaling paradigm.

Another important parameter is power dissipation. The current GHz clock rate microprocessor IC dissipates about 40 watts/cm<sup>2</sup>. Today's chips are operating at lower voltages, and microprocessor architectures in particular employ self-actuated power limiting features that turn off those circuits within the IC that are not involved in the function being performed. This strategy has dramatically reduced power dissipation and is being driven by low power portable devices, such as cellular phones and personal digital assistants (PDAs). To understand the issue on a more fundamental level table 1 shows that using constant voltage scaling ( $\beta = 1$ ), the power dissipation of today's

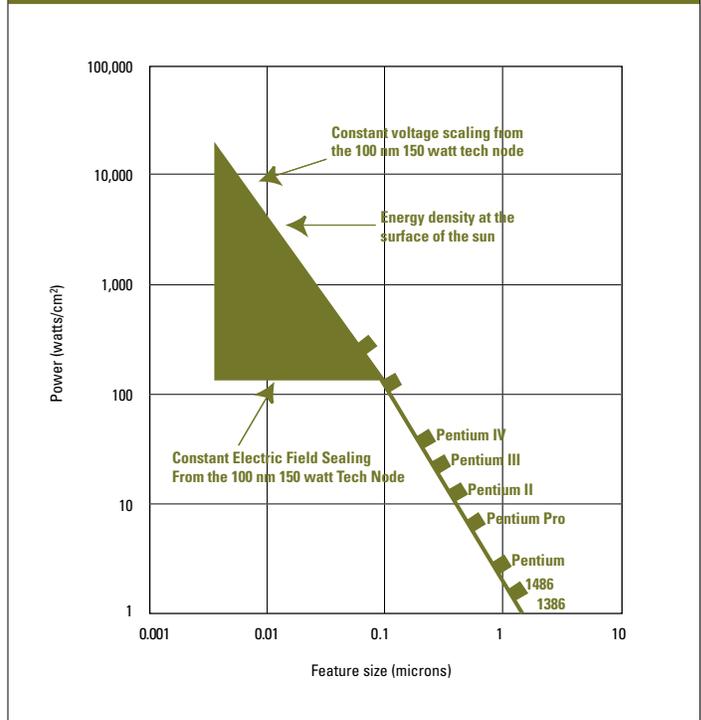
microprocessor would increase to 18 megawatts (MW)/cm<sup>2</sup> for feature sizes of one atom. This exceeds the radiant energy at the surface of the sun and is obviously not an option. One solution that has been applied is to scale voltage down by some factor. For example, if constant electric field scaling (that is,  $\beta = \alpha^{-1}$ ) is used, then table 1 predicts no increase in the power dissipation. This, however, would require that the devices be operated at the millivolt level and that other factors, such as static power dissipation due to tunneling currents, not be a significant factor. While operating voltages are being scaled down (from 5 volts to 3.3 volts to 1.8 volts to 1.0 volt, for example), there are practical and device physics limitations to such very low millivolt supply voltages. Reducing supply voltage for high performance transistors by a factor of 5 (that is, to about 0.5 volts predicted by the 2001 ITRS roadmap in 2013) reduces the power dissipation for our gedanken experiment to ~30 KW/cm<sup>2</sup>—still a very large value.

Power management strategies using circuit architecture will not be sufficient as power dissipation continues to increase. Thus, it is quite likely that power management will become a limiting factor well before the ultimate feature size is reached. Figure 2 presents actual data<sup>4</sup> on the increase in energy dissipation over several recent generations of microprocessors and several additional projected future generations. The two limits of constant voltage scaling and constant electric field scaling are indicated on the figure starting at the 100-nm technology node. Clearly, constant voltage scaling is untenable, and constant electric field scaling is not achievable over the projected range of feature size. Reality will be some intermediate state between the two extremes (see the shaded area in figure 2). These data confirm that power management will become a major problem for the current paradigm in the near future. From only device physics consideration, the limit is likely to be set by thermal dissipation due to leakage current in devices that exhibit quantum tunneling in the gate insulator.

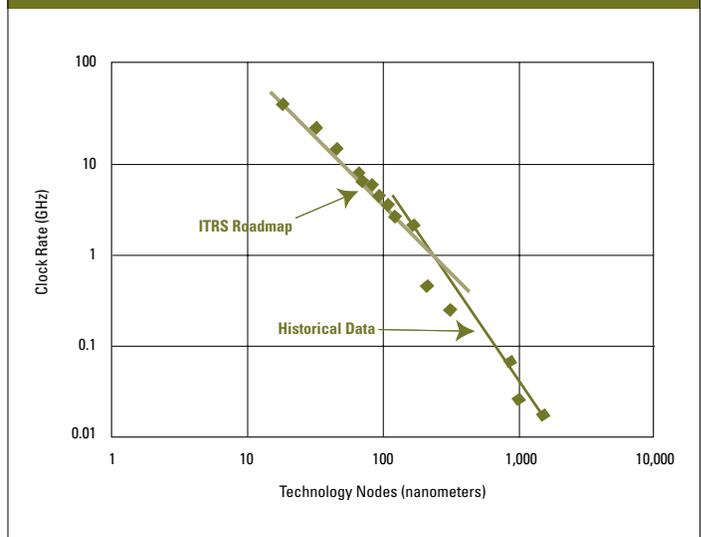
A similar analysis concerning clock rate as a function of technology node is plotted in figure 3. Historical data are taken from the performance of Intel microprocessors to the 180-nm technology node, while projections beyond this point are taken from the 2001 ITRS. The ITRS data start with the year 2001 and extend to 2016. During that period, the clock rate is given as 1.7 GHz in 2001 and projected to reach 28.75 GHz in the year 2016. A simple analysis of the data shows that the ITRS plot has a much lower slope ( $n = 1.52$ ) than the slope of the historical microprocessor data ( $n = 2.3$ ). It appears that the ITRS is projecting a significant slowdown in the rate of growth of the clock speed over historical data. Practical limitations, including power dissipation and circuit limitations, will likely further limit the existing paradigm as suggested in the figure.

To this point, we have confined our discussion to properties that can be attributed to bulk processes in semiconductors. However, more subtle processes are emerging. For example, while the current feature sizes shown in figure 1 are larger than those in which quantum (that is, not bulk) properties come into play, the insulator thickness required by the scaling is now about 20 atoms. This is well into the transition region where quantum tunneling currents are clearly observable. This is a qualitatively different situation from

**Figure 2. Microprocessor Energy Density**



**Figure 3. High Density Microprocessor Clock Rate as a Function of Technology Node**  
(after the ITRS 2001 Roadmap and historical data)



what has occurred in the past and jeopardizes scaling in the near term (over the next 5–10 years).

There may be partial solutions to this particular problem. It should be noted from table 1 that capacitance scales as the dielectric constant. This offers the possibility of obtaining the required gate oxide insulator capacitance per unit area by holding the oxide thickness constant (so as to avoid making the tunneling problem worse) and increasing the dielectric constant of the oxide. Therefore, the

likely near-term solution to the insulator problem will be to find a new material system with a higher dielectric constant than silicon dioxide ( $\text{SiO}_2$ ), so called high- $\kappa$  materials, such that the electrical properties can be scaled without having to thin the insulators further.

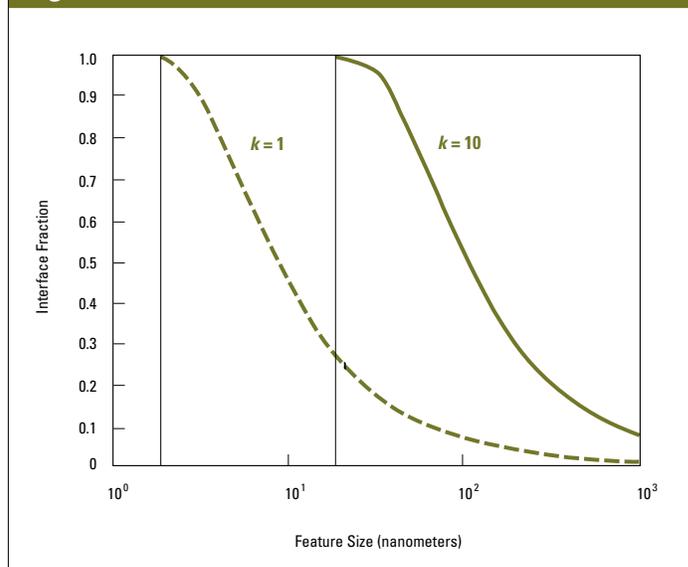
This is easier said than done, since the insulator material system must be compatible with the substrate upon which it is placed. In all likelihood, this problem will be resolved, since large resources will be applied to the solution. It does, however, make the point that the scaling is becoming much more complex than it has been. It should also be noted that this dielectric scaling strategy cannot be employed for more than one or two generations since it will ultimately destroy the geometry of the scaling (that is, the ratio of the channel length to the oxide thickness is typically at least 25 to 1 so that the gate can exercise its control function). Other innovations that will continue in the near term to keep the industry on the Moore curve are strained silicon for higher electron mobility in the active channel, high current/low voltage implantation for shallower junctions, and advances in copper/low- $\kappa$  materials for interconnects, where  $\kappa$  here refers to dielectric constant.

However, one has to work harder and harder to maintain the scaling required by Moore's Law. Another way to get a sense that the situation is now qualitatively different is to estimate the fraction of atoms of a semiconductor feature that reside on the surface to those that reside in the volume (bulk) of the feature. An estimate of this fraction is shown in figure 4, where  $n$  is the feature dimension divided by the effective diameter of the atoms that make up the feature (that is,  $n$  is the number of atoms across the feature). The parameter  $\kappa$  is a measure of the number of atoms over which surface or interface effects manifest themselves. In the case  $\kappa = 1$ , these effects are manifest over only 1 atom thickness. In the case  $\kappa = 10$ , they are manifest over 10 atom thickness.

Today, feature sizes are approaching 100 nm, which corresponds to  $n = 370$ . It is clear from figure 4 that for values of  $n$  much larger than 370 (representing the previous history of solid-state electronics), the interface fraction is very small regardless of which value of  $\kappa$  one uses. For values of  $n$  smaller than 370 (the region into which scaling now enters), the interface fraction rises very rapidly until it becomes dominant. This is a very different situation from the past and will undoubtedly have profound effects on scaling to smaller feature sizes. When these effects occur depends upon the value of  $\kappa$ . If the effects are restricted to within 1 atom of the surface ( $\kappa = 1$ ), they will not become appreciable until feature sizes reach about 30 nm. If the proper choice for  $\kappa$  is 10, then solid-state electronics is already into the domain where it is becoming dominated by interface processes rather than bulk processes. The appearance of quantum tunneling currents mentioned above suggests this case. Of course, this model is elementary, but it does suggest that obtaining another order of magnitude reduction in feature size will be considerably more challenging than it has been to date.

Because it is not possible to present a complete review of the technical literature, we will summarize a few concerns regarding continued scaling of semiconductor electronics. It has been pointed out that when the dimensions of devices approach the mean free path of the carriers (which is now occurring), the bulk transport models that have been used in the past fail. Quantization of the energy levels occurs when dimensions approach the deBroglie

**Figure 4. Interface Fraction**



wavelength of electrons. As dimensions approach the distance between the dopant atoms, small number effects will become important, because depleted layers must be reduced in proportion to the dimensions. Tunneling currents increase rapidly as layers are thinned. The scaling of the thickness of the gate insulation in field effect transistors in proportion to other dimensions of the transistor approaches limits set by tunneling and by the influence of the silicon-silicon dioxide interface on the insulating properties. The resulting power dissipation created by tunneling currents grows substantially and creates significant roadblocks to further higher-level integration. The breakdown voltage of insulating layers decreases. Soft errors, such as those created by radioactive impurities and cosmic rays, are becoming of increasing concern. The interconnect wiring between transistors is becoming a special concern.

Devices in computers are organized into logic circuits made of a few transistors that perform elementary logic functions. The circuits are interconnected to implement more complex functions. The number of connections is the same order as the number of components. The number of connections is now in the many millions and will grow exponentially in the near future. For example, the total length of interconnect wires in a modern microprocessor IC is several kilometers. Making wires narrower to reduce the space that they occupy on chips increases their resistance per unit length and leads to transmission delays limited by the time it takes to charge the capacitance of the wire given as  $1/RC$ , where, again,  $R$  is the resistance and  $C$  is the capacitance of the wire. The wire length per transistor increases faster than the number of transistors. Deleterious cross-talk between more closely spaced interconnects also increases.

It is clear from this simple analysis that the wiring interconnects in ICs do not scale and thereby do create a significant barrier to further integration. All of the above contribute to increasing the complexity of feature size scaling and therefore increase the difficulty of maintaining the performance enhancements predicted by

Moore's Law. These roadblocks are well known to the microelectronics community. For example, the ITRS notes, "Processing dimensions are getting close to the size of photoresist molecules and other physical dimensions associated with exposure and development. Existing techniques for measuring sizes, positions, and defects are becoming difficult to use. In addition, displacement of the equipment's structural parts due to heat and vibration is no longer negligible." Clearly, there will be severe demands for metrology and stability if one is to reduce feature size further.

To accommodate Moore's Law in the near term, the issues discussed above and others must be managed such that the technology node (the ½ pitch size of the metal interconnect line width connecting transistors) approaches 65 nm by 2007. The physical gate length of the transistor for this technology node will be ~32 nm. Much beyond the 65-nm technology node, optical lithography will no longer be viable for additional feature size reduction. This will require that new lithographic technology is introduced if the current paradigm is to be pushed further. The most likely replacement is extreme ultraviolet (EUV) lithography, which operates at a source wave length of about 13 nm. EUV lithography is quite different from optical lithography. For example, it must use focusing mirrors rather than lenses. Also, it is absorbed by almost all materials, making masks very expensive and complex. This technology is likely to be much more expensive than existing optical lithography technologies that use laser sources at 193 nm and 157 nm and will continue the trend of ever more expansive manufacturing facilities.

The increasing costs for state-of-the-art semiconductor manufacturing facilities is also an important consideration that will shape the future direction of this technology. The discussion above has focused on physical limitations, but there is also an economic side, one manifestation of which is known as Moore's Second Law. This law is illustrated in figure 5, which plots the cost per factory as a function of time.<sup>5</sup> This figure illustrates the impact of increasing complexity on cost. Extrapolating the current trend to 2005, the cost per fabrication line will be about \$10 billion, and by 2015 it will be at \$200 billion.

Of course, industry will work to reduce these out year capital investments. Nevertheless, large capital investments clearly will be required to continue feature size scaling. The trend is toward fewer worldwide facilities using ever-larger wafer size (12-inch-diameter wafers are the state of the art today) to achieve economy of scale reductions. A corollary to current cost trends is that the ability to implement a diversity of chip designs into actual ICs will likely be constricted as the cost of a mask set for a given design becomes extremely high. The result for ICs with state-of-the-art features and density will likely be fewer different designs in extraordinarily high volume.

Is the market there to support such an investment, especially in light of the approaching physical limitations that will limit the long-term use of the new capital investment? Will any of the few

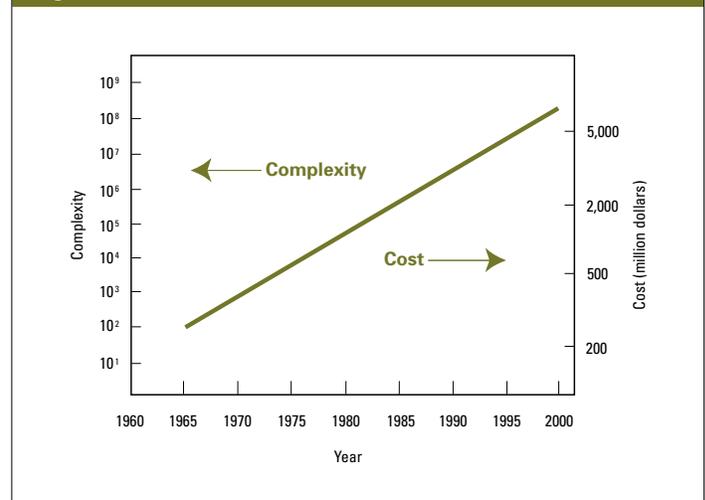
mega-fabs of the future be in the continental United States? Will American companies own any of them? If the answer to either of these last two questions is no, then what are the implications for supply and assured chip functionality for DOD? Within about 15 years, as features approach the size of a few atoms, further miniaturization will not be possible. Will industry find it profitable to push the current paradigm to its limit? It is clear that to continue Moore's Law beyond 10 to 15 years will require the introduction of a new device and a new circuit topology paradigm. While it may be possible to do so, it must be realized that this will no longer be the development path that led to Moore's Law in the first place. Finding this new path, if it exists, becomes the key issue for the science and technology community that supports the IC manufacturing base.

## What Is Next?

It seems clear that solid-state microelectronics will enter a new regime over the next 7 to 10 years in which the current scaling paradigm will no longer hold. Interface and quantum mechanical processes rather than classical processes will dominate the emerging technological regime. Feature size scaling will become more difficult. Indeed, the scaling that has worked so effectively in the past will likely not convey to this new regime. It is reasonable to ask whether DOD should be concerned about this. One approach to coming to grips with this question is to look at where the current paradigm is likely to bottom out. It has been shown experimentally that the gate oxide thickness, which is the thinnest feature of the MOSFET, must be at least five atoms thick for silicon dioxide.<sup>6</sup> The experiments that determined this limit required extraordinary control in the creation of the oxide layer and used techniques that will not scale to mass-produced devices. Nevertheless, the experiments provide valuable guidance regarding how far the present paradigm can be pushed.

**It seems clear that solid-state microelectronics will enter a new regime over the next 7 to 10 years in which the current scaling paradigm will no longer hold**

**Figure 5. Moore's Second Law**



The gate length in the MOSFET is typically 25 times the oxide thickness. This leads to a minimum gate length of  $\sim 125$  atoms, or about 32 nm for a silicon dioxide insulator of about 1.2 nm for the 65-nm technology node expected in 2007. (Industry is prepared to make the investments needed to reach 65-nm feature size, and it should be reached by 2007.) It is logical to ask whether the 65-nm technology node would provide sufficient computer power to meet DOD needs. If this level would suffice, then DOD has no reason for concern. If additional computer power is required, what can be done to move beyond this point? The scaling in table 1 provides some guidance. If a conservative 3-year scaling rule methodology is used, then a feature size of 32 nm would correspond to about 775 million transistors per chip, of which  $\sim 276$  million transistors would be high-performance devices in the core of the main power unit operating at a clock rate of  $\sim 7$  GHz. Such an IC would have the ability to perform  $\sim 30$  Giga FLOPS with a single microprocessor. It would also dissipate  $\sim 190$  watts. This power dissipation, while stressing, is probably manageable, and the computer power is quite substantial.

Is this computer power sufficient for expected DOD applications? To answer this requires some projection of future DOD requirements. A demanding military requirement in this regard is the DOD stated objective to maintain information superiority and total situational awareness. This objective will be accomplished partially by smart sensors and appropriate information networks. Since history suggests that we always need more compute power than we think, it is prudent to employ aggressive examples when making predictions. As an illustrative example, we examine a stressing but not unreasonable implementation of total situational awareness, namely target detection and identification using hyperspectral imagers flying on mini unmanned aerial vehicles (UAVs). The subject of using mini UAVs for such applications was recently addressed by one of the authors.<sup>7</sup>

The advantage of the mini UAV is that it can obtain high-resolution images and would be an organic asset of a local commander (for example, a battalion level commander). If the UAV flies at a 3-kilometer (km) altitude, seeks spatial resolution of about 6 inches, and flies a hyperspectral imager with a 20-degree field of view and 200 spectral bands, then each image looks at about 1 km<sup>2</sup> and generates about  $2 \times 10^8$  pixels per band. For convenience, assume a 16-bit dynamic range. The information content of a single image frame is then about  $10^{11}$  bits. To achieve real-time battlefield assessment, it would be desirable to receive these images at video rates. This results in a bit stream of about  $3 \times 10^{12}$  bits per second. This sensor does not exist for reasons that will become clear shortly, as well as other issues such as the need to achieve the required signal-to-noise ratio. Nevertheless, it is instructive to look at where we stand regarding meeting the computational and data handling requirements necessary to operate on this raw data stream. The electronics to get the data off the focal plane and perform, for example, automatic target recognition (ATR) and data compression will require the image processor to process data at about the same rate that it is collected (that is, about  $10^{12}$  operations per second<sup>8</sup>). This is about a hundred

times the speed of the front side bus expected from a single microprocessor at the 65-nm technology node. One could segment the calculations so that they could be accomplished by multiple processors. This approach would require about a hundred microprocessors and would dissipate on the order of about 10 kilowatts. This is clearly beyond the capability of the mini UAVs, which are power constrained, and, therefore, the mission could not be done with this approach. This would also exceed the payload power available on larger UAVs, such as the Predator ( $\sim 1.8$  KW).

While this calculation is oversimplified, it does make the point that DOD information superiority and total situational awareness objective cannot be met if the effective computer power available to DOD distributed sensors asymptotes at the levels determined by the 32-nm MOSFET at the 65-nm technology node. In making this statement, we assume that the distributed sensors will need on-board processing power that is capable of dealing with the data collection rate. One

could conceive of transmitting the uncompressed data to central facilities where detailed calculations would be done with supercomputers. This does not seem reasonable, however, considering the transmitter power that would be necessary, the data rates involved, and the operational environments in which the sensors would operate. We have also deliberately used the term *effective computer power* since there may be approaches other than brute force number crunching to deal with these high data rate sensor systems.

As mentioned earlier, the feature size of an MOS transistor can be reduced further by employing a gate insulator with a dielectric constant substantially higher than SiO<sub>2</sub> if a robust new material can be identified that has the necessary properties. For example, by doubling the dielectric constant of the gate insulator, a robust transistor with a gate length of 16 nm should be feasible. The resulting processor would still not meet the computing requirements outlined in the mini UAV example described above. Indeed, it appears that one would need a feature size of about 8 nm to do the job. At this point, the ratio of gate length to oxide thickness would be small enough that the device probably would not work. The power handling requirements would also be formidable for the current paradigm. Other DOD computing and data handling requirements can be identified that will require effective computing power that will probably not be achieved within the paradigm that has tracked Moore's Law over the past 40 years.

## What Does the Future Hold?

Research is being conducted worldwide that offers fleeting glimpses of a new paradigm in solid-state electronics at the nanometer scale below 20 nm—the realm of *nanoelectronics*. This long-term research focuses on new materials and new electronic phenomena. For example, nanotubes of carbon and other materials have demonstrated amazing physical and electronic properties. The electronic properties—in some cases a metal and in others a semiconductor—of carbon nanotubes have been demonstrated to be a function of the

## **A demanding military requirement is the DOD stated objective to maintain information superiority and total situational awareness**

chirality of the nanotube and its diameter. Elemental transistor-like switches have been made from single carbon nanotubes. In a completely different research area, advances have been made in quantum dot structures. A zero-dimension quantum dot is a semiconductor structure that confines exactly one electron in all dimensions. These structures, made possible by advances in the deposition and precise control on an atomic level of thin layers of III–V semiconductors, have led to the discovery of so-called qubits—quantum dots that can have several different energy states simultaneously. The possibility of using such qubits in a quantum computer—a computer not based on Boolean logic but instead on a completely different mathematics with computational properties that are theoretically far beyond what exists today or will exist in traditional ULSI in the time horizon described herein—is intriguing.

Yet another area with potential for large impact in future nanoelectronics technologies is magnetic semiconductor materials and the possibility that such materials offer to create switches based upon controlling and sensing the quantum mechanical spin of single electrons. The concept of helical logic devices in which information-encoded single electrons are constrained to move along helical paths formed by a rotating electric field is yet another novel concept for advanced computing. Computing based upon biological implementations using deoxyribonucleic acid is also under intense study. In addition, there are potential breakthroughs in the area of processing algorithms. These examples, and those yet to be discovered, of high-risk long-term research are possible directions beyond the horizon of the present paradigm.

There is no promise, however, that any of these research areas will produce the answer. But if the history of 100 years of technological innovation in electronics is any guide, the prospects are in our favor that a way beyond the looming limitations of scaling and Moore's Law will be found. However, investment in this type of long-term high-risk research is unlikely to be made by the industrial private sector, which has more pressing near-term needs. Also, basic research is by its nature nonproprietary. The free exchange of ideas and results is a critical element of the scientific process. Research is a global enterprise. But there is a definite need to ensure that whatever new scientific breakthroughs occur, they are available first and foremost to the United States and DOD to maintain a technological advantage. The most assured way to have this occur is to nurture long-term research within the United States in the private sector, universities, and Government Laboratories.

## A Course of Action

What is a prudent course of action for DOD? It would not seem productive for DOD to invest resources to help squeeze the most out of MOSFET CMOS scaling. Commercial industry has mastered this area and has the ability—and incentive—to apply large resources toward this problem. There is little that DOD can add except, perhaps, in niche research areas, such as advanced lithography. On the other hand, several fundamental device and circuit architecture issues have been outlined in the discussion above that any new paradigm must address satisfactorily. Among these are excessive power dissipation, very low-voltage operation, and interconnection and

signaling limitations as switching rates increase. These and other related technological issues require new innovations in material science, fabrication, and architectural approaches for their resolution.

A sustained investment in these areas is where DOD can once again make a major impact on future electronics for sensing, computation, and information technologies. The highest leverage in development programs occurs in the early stages of research and development, where investment costs are low and the opportunity for impact is high. This is where DOD science and technology can make significant contributions. Undoubtedly there are many other approaches that have not yet been thought of or surfaced. Clearly there is great opportunity here for DOD science and technology to make major contributions. Also, it is important to keep in mind the discovery that led to the invention of the transistor. Breakthroughs in one area often result from serendipitous discovery in what appear to be unrelated areas. Positioning DOD so that it can maintain the needed broad visibility in the technical community and to be wise enough to recognize important developments/discoveries will be key to success.

## Notes

<sup>1</sup> G.E. Moore, "Cramming more components onto integrated circuits," *Electronics* 38, no. 8 (April 19, 1965).

<sup>2</sup> R.H. Dennard, F.H. Gaensslen, H.N. Yu, V.L. Ridout, E. Bassous, and A.R. LeBlanc, "Design of ion-implanted MOSFETs with very small dimensions," *IEEE Journal of Solid-State Circuits* 9 (October 1974), 256.

<sup>3</sup> Community awareness of this problem is indicated by publications such as J.D. Meindl, ed., "Special Issue on Limits of Semiconductor Technology," *Proceedings of the IEEE* 89, no. 3 (March 2001), and P. M. Solomon, ed., "Scaling CMOS to the limit," *IBM Journal of Research and Development* 46, no. 2/3 (March/May 2002), 117–360.

<sup>4</sup> S. Borkar, "Design challenges of technology scaling," *IEEE Micro* 19 (July/August 1999), 23–29.

<sup>5</sup> E.S. Meieran, "21<sup>st</sup> Century Semiconductor Manufacturing Capabilities," *Intel Technology Journal* (4<sup>th</sup> quarter 1998).

<sup>6</sup> D. Muller et al., *Nature* (June 24, 1999).

<sup>7</sup> Timothy Coffey and John Montgomery, "The Emergence of Mini UAVs for Military Applications," *Defense Horizons* 22 (Washington, DC: National Defense University Press, December 2002).

<sup>8</sup> This number depends on the algorithms used.

Defense Horizons is published by the Center for Technology and National Security Policy through the Publication Directorate of the Institute for National Strategic Studies, National Defense University. Defense Horizons and other National Defense University publications are available online at <http://www.ndu.edu/inss/press/nduphp.html>.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk  
Director

## I-Power: The Information Revolution and Stability Operations

*Franklin D. Kramer, Larry Wentz, and Stuart Starr*

### Overview

Information and information technology (I/IT) can significantly increase the likelihood of success in stability operations—if they are engaged as part of an overall strategy that coordinates the actions of outside intervenors and focuses on generating effective results for the host nation. Properly utilized, I/IT can help create a knowledgeable intervention, organize complex activities, and integrate stability operations with the host nation, making stability operations more effective.

Key to these results is a strategy that requires that 1) the U.S. Government gives high priority to such an approach and ensures that the effort is a joint civilian-military activity; 2) the military makes I/IT part of the planning and execution of the stability operation; 3) preplanning and the establishment of I/IT partnerships are undertaken with key regular participants in stability operations, such as the United Nations and the World Bank; 4) the focus of the intervention, including the use of I/IT, is on the host nation, supporting host-nation governmental, societal, and economic development; and 5) key information technology capabilities are harnessed to support the strategy. Implementing the strategy will include 1) development of an information business plan for the host nation so that I/IT is effectively used to support stabilization and reconstruction; 2) agreements among intervenors on data-sharing and collaboration, including data-sharing on a differentiated basis; and 3) use of commercial IT tools and data provided on an unclassified basis.

Over the past 30 years, the information revolution has had an important impact on the conduct of military operations. In the United States, it has produced what is often called “netcentric warfare” or “netcentric operations”<sup>1</sup>—the combination of shared communications, key data, analytic capabilities, and people schooled in using those capacities—that has enabled enhanced joint activities, integrated distributed capabilities, much greater speed, and more effective maneuver. The result has been that the United States and its allies have been able to conduct very effective combat operations under a range of conditions,

including quick insertion (Panama), maneuver warfare (major combat operations in Iraq), an all-air campaign (Kosovo), and a Special Forces-led effort (Afghanistan).

At the same time that major combat operations have proceeded so successfully, the United States and its allies have undertaken a variety of stability operations in Somalia, Haiti, Bosnia, Kosovo, East Timor, several African countries, Afghanistan, and Iraq.<sup>2</sup> These stability operations generally have included both economic and governance reconstruction and have spanned the full security gamut from nonviolent peacekeeping to full-blown counterinsurgency. Not one of these operations has approached the success achieved in combat operations undertaken in the same period.

This paper analyzes whether a strategic use of information and information technology (I/IT) in stability operations could lead to more successful operations. Certainly, the information revolution has been a dynamic and positive factor in business, government, and social arenas in the Western world. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities of all types. This paper concludes that utilizing the elements of the information revolution in a strategic approach to stability operations would have positive results and sets forth the strategic and operational parameters of such an effort.

### Problems of Stability Operations

Utilizing the fruits of the information revolution for effective stability operations requires a prior understanding of what makes a stability operation effective. As noted above, stability operations have security, economic, and governance reconstruction elements. Yet while it is widely recognized that stability operations go far beyond purely military actions—encompassing security, humanitarian, economic, and governance/rule of law issues—no one has set forth an actual strategic or operational doctrine that promises success in stability operations. As a World Bank staff report put it, “The Bank, like other international partners, is still learning what works in fragile states contexts.”<sup>3</sup>

The problems of stability operations are evident. To begin with, no two circumstances are the same. To say that Haiti is different than Somalia is different than Bosnia is different than Afghanistan is only to hint at the depth and breadth of the complexities. These include the causes of the crisis that occasioned the intervention, the host-nation culture or cultures, the language or languages, the nature of the economies *ante bellum*, the influence of neighbors, and a multitude of other factors. By definition, the state structure has collapsed or is severely impaired. Often there has been significant violence. Internal groups have been factionalized and frequently have each others' blood on their hands. Economies are in disarray. Social mechanisms have broken down. Information is lacking, and communications mechanisms are limited.

Prior to almost all interventions, the international community already will have been significantly present in the form of international organizations, nongovernmental organizations, businesses, bilateral governmental activities, and many more venues. Once there is a major international intervention, complexity increases greatly. Regardless of the initial number of international actors, the number and diversity of participants increase. More importantly, their relative importance increases for such functionality as exists or is created in the host country. Additionally, whereas before the intervention, development often had priority, now there are simultaneous challenges in the security, humanitarian, economic, and governance arenas—and, if social needs may be separated from the foregoing, in the social arena as well. Because of the expanded requirements, there are numerous players. Personnel and equipment stream in from civilian and military components of the governments of the United States and other nations, international organizations, such as the United Nations (UN) and its many agencies, the North Atlantic Treaty Organization (NATO), the Organization for Security and Cooperation in Europe, the African Union, the World Bank, and others. Nongovernmental organizations also are involved, many of them in the humanitarian arena, as well as numerous others that participate in myriad aspects of reconstruction and development. Many businesses also get involved, either as contractors to national and international organizations or as participants in private ventures.

A very important aspect of the complexity is that dealing with the host nation has become more difficult. Governmental functions are broken, and the government is seen by many as illegitimate and not representative of all the people; its reach is generally limited, and it is ineffective in mobilizing domestic human and other resources.

A further complicating factor is that circumstances on the ground change over time in significant part in response to the intervention. (The transformation from liberator to occupier is a well-known problem for intervening forces.) Interventions generally last for years, and a decade is not unusual. Stability operations encompass not only security but also reconstruction, and reconstruction takes time. In addition to actual changes, managing expectations of both the intervenors and the host nation becomes extremely important. For example, there is a so-called “golden hour” of 6–12 months during which actions must support expectations and the local population must experience improvements in quality of life.

---

Franklin D. Kramer ([kramerf@ndu.edu](mailto:kramerf@ndu.edu)) is a Distinguished Research Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University. Larry Wentz ([wentzl@ndu.edu](mailto:wentzl@ndu.edu)) and Stuart Starr ([starrs@ndu.edu](mailto:starrs@ndu.edu)) are Senior Research Fellows in CTNSP.

It is in this context that the question arises whether the application of the tools and content of the information revolution can have a positive effect on the outcome of a stability operation.

## Opportunities for I/IT Strategy

As difficult as the circumstances of a stability operation are, the very complexity provides significant opportunities for the use of an effective information strategy built around the use of information technology. It is worth underscoring at the outset what may be an obvious proposition: that information and information technology have to be used together to be effective. One will not suffice without the other.

At the most basic level, information technology can be used to distribute information to important players in an ongoing stability operation. Making information available can have four important consequences.

First, it can *help create a “knowledgeable” intervention*. Even before the intervention, and certainly as the intervention progresses, the intervenors will need information of many kinds about both planned and ongoing respondent activities and about the host nation. For the latter, population characteristics, cultural dynamics, economic structures, and historical governance issues all can be described and analyzed.

The intervenors will first plan and then undertake many activities, with multiple players in each field of endeavor. While it will not be possible for all intervening actors to have the unity of command that is sought by militaries, the use of I/IT may allow for organizing a more common approach—or at least to reduce inconsistent approaches.

An information strategy supported by information technology provides an opportunity to share information among the stability operation respondents themselves. This sharing of information will facilitate the generation of a common approach and can help in the effective use of scarce resources. As an example, the allocation of health care resources might be usefully rationalized once there is at least a working sense of what types of resources are available from the respondents. Also, intervenors working on the rule of law in different sections of the country will be more effective if they adopt closely aligned approaches than if they use significantly different approaches, even if each is valid in and of itself.

A second key element of the strategy will be using I/IT to *help organize complex activities*. Normally, a stability operation will be undertaken on a countrywide basis. For even the smallest countries, this means a significant geographic arena, with all the difficulties of maintaining connectivity. The intervention also will undoubtedly extend over a significant timeframe, and I/IT will be necessary to maintain an updated approach as conditions on the ground change.

Complexity also will be manifested in the requirement to deal simultaneously with security, humanitarian, economic, and governance issues. Many intervenors will be involved in only one or some of these actions, but actions in one field often have consequences for another. Moreover, knowledge of what is happening in each is important for the development of an overall strategy capable of achieving an effective host nation. Even in a single sector, information supported by effective information technology would allow for more effective in-country coordination; and distributed players would be better able to take focused effective actions. Furthermore, knowledge is an important element in building trust and commitment among different stability operations players, which can be a key element in enhancing effectiveness.

The third key use of distributed information will be to *integrate the stability operation respondents with the host nation*. It bears stating more than once that the objective of a stability operation is not a “good intervention” but rather an “effective host nation” as a result of the intervention. To accomplish this difficult task, given that the host nation is likely fragmented, disrupted, and not very effective, the intervenors need to stay connected to the host nation so that the results are adopted and adoptable by the populace on whose behalf the effort is being undertaken. An I/IT strategy needs to involve the host nation (likely in numerous manifestations) in the ongoing activities of the intervention.

The fourth use of I/IT is to *integrate the host nation and make it more effective*. Effectiveness can be enhanced by using I/IT to identify key requirements and target scarce resources. Information for a budget process is an important example. I/IT will also be able to facilitate informed senior decisionmaking well beyond budget and budget-type decisions. For example, how best to bring previous warring factions to work together will involve important social and economic issues whose resolution can be enhanced by good information.

Host-nation capacity can also be created by the use of I/IT. Government operations can be reestablished with the proper use of information technology. Both the information systems and the training to use them will be required, but information capacity can be generated far more quickly than other infrastructures—and can enable other effective actions.

## Key Questions for the I/IT Strategy

An important question in analyzing an I/IT strategy for stability operations is how such a strategy relates to what else is happening in the intervention. As noted by the World Bank staff, no one has developed a truly knowledgeable approach to stability operations, which, in World Bank parlance, is one type of activity in fragile states. There are, however, some principles that have been adopted by the international community and the United States that are worth noting here.

First, the international community, through the Organisation for Economic Co-operation and Development (OECD) and otherwise, has emphasized the importance of the principles of harmonization and alignment. *Harmonization* refers to having the outside intervenors work in a generally coordinated fashion. As the OECD Development Co-operation Directorate has stated, “Harmonisation is taken to refer to common arrangements amongst the donor community, rationalized procedures and information sharing between donors . . . related to the goal of greater coherence between and among donors.”<sup>4</sup> *Alignment* refers to having the outside intervenors align their activities with the interests of the host nation. Again, as the OECD Development Co-operation Directorate stated, “Alignment has been defined . . . as a set of practices according to which donor organizations use recipient country strategies, policies, and practices . . . as a guide for their assistance programs.”<sup>5</sup> Both these principles are embodied in the so-called Rome Declaration on Harmonization of 2003 and subsequent actions and statements of the major multilateral and bilateral donor entities and countries, including the United States.

I/IT can have an important, positive impact on both harmonization and alignment. Coordination among intervenors is one of the key achievable results of an effective information strategy implemented by information technology. Likewise, an I/IT strategy is an important element

to ensure that the host nation is effectively integrated into the decision-making and implementing actions of the outside intervenors.

A second question is the relationship between an I/IT strategy and strategies for security, humanitarian needs, economic development, and governance/rule of law. The U.S. Government, and particularly the Department of Defense (DOD), has often talked about using all elements of national power for success in stability operations, often citing diplomatic, informational, military, and economic (DIME) power as key aspects of the types of power brought to bear by outside intervenors.

This so-called DIME paradigm is a useful model, although it is not meant to be exhaustive. For example, host-nation civil society may be affected by outside, nongovernmental, civil organizations that nonetheless are important elements of an intervenor’s national power. Social issues also must be considered, and, unless “diplomatic” is read to mean all contacts other than military or economic, there will be important nondiplomatic interactions on matters such as rule of law. What the DIME paradigm shows most importantly, however, is that information needs to be considered in an overall context, just as the principles of harmonization and alignment indicate.

There is a sterile debate as to whether information only supports other activities or is an activity in and of itself. Certainly, information supports other activities. Military, economic, and governance activities all operate on the basis of information. Conversely, certain aspects of information, such as the establishment of technical structures, can be undertaken apart from other activities. As an example, think of the building of towers to create the infrastructure for a cellular network. Overall, however, information, as every other action in a stability operation, is designed for one purpose: to serve the objective of making the host nation effective. That is the overall context in which to consider I/IT and to determine whether and how to undertake a particular effort.

The broad challenge for an I/IT strategy for stability operations is to help create effective results from the multitude of players and actions that will be found in a particular situation. No one should think that information is a panacea. If a faction within a country resists working with another faction even after all information is exchanged, then that is a political problem and probably will not be solved by further information. But given that information is not a universal solution to all problems, the question is whether the information revolution can help harmonize, align, and make more effective the outside military and civilian governmental intervenors, international and nongovernmental organizations, businesses, and, especially, host nation in all its manifestations.

## Elements of an I/IT Strategy

Five key elements are required to generate an effective I/IT strategy for the United States to use in stability operations.

*Element 1.* The first requirement is for the U.S. Government to make the fundamental decision that such a strategy is a key mandatory element of all stability operations. That is no small statement, because the reality is that the United States has never—in any of its many stability operations—made such a decision. But the rationale for such a conclusion is clear: information and information technology are crucial elements to the success of stability operations, supporting effectiveness, harmonization, and alignment goals.

A coherent U.S. Government I/IT strategy is essential to produce the needed results. This means that the effort has to be truly

interagency—and, most importantly, be accepted as a key element by both DOD and the State Department (including USAID, the U.S. Agency for International Development). While some individuals have acknowledged this point, no such government-wide I/IT strategy exists, although a potential framework for one has been created.

Released by the President in December 2005, NSPD-44, “Management of Interagency Efforts Concerning Reconstruction and Stabilization,” articulates the basic framework for interagency cooperation. It assigns primary responsibility for stabilization and reconstruction operations to the Secretary of State (through the Office of the Coordinator for Stabilization and Reconstruction) and mandates close coordination with DOD to integrate stabilization and reconstruction contingency planning with military planning, when relevant and appropriate. The Director of Foreign Assistance, who reports directly to the Secretary of State, also serves as the Administrator of USAID, where several offices have been created or restructured to deal with stabilization and reconstruction challenges.

At DOD, the framework was supported in November 2005 by the release of Directive 3000.05, “Military Support for Stability, Security, Transition and Reconstruction Operations,” which affirms that such activities represent a core DOD mission and are given a priority comparable to combat operations.

Within this framework, however, the focus on I/IT has been limited. USAID, recognizing the potential of I/IT in stability and reconstruction operations, has taken some steps to include I/IT as a sector and development tool. USAID strategy states that it seeks to leverage I/IT in conflict management and mitigation missions and in humanitarian assistance operations. USAID also seeks to promote global access to IT and to assist development through several ongoing projects such as the Leland Initiative for Africa, the Digital Freedom Initiative, and the Administrator’s Last Mile Initiative.

Some important embassies have also taken I/IT steps. The U.S. Embassy in Afghanistan created the position of Senior Telecom Advisor to facilitate coordination among both military and civilian U.S. Government elements in country. In Iraq, DOD established the Iraq Reconstruction Management Office within the Embassy structure, and it, too, has a telecommunication advisor to unify I/IT efforts. These efforts are the beginning of a coherent U.S. Government approach to I/IT. A complete strategy would, however, require the Department of State/USAID to make I/IT a key element of strategy in stability operations. These I/IT initiatives are a good start, but are not an integrated strategy. They do, however, provide a basis on which to build.

*Element 2.* Although the problems of stability operations go far beyond military, the second element of an effective I/IT strategy recognizes that, doctrinally, the military requires an I/IT strategy as part of the planning and execution of any stability operation. Accordingly, in both joint and Service documents—plans and the rules and guidance for the development and execution of plans—an I/IT strategy is a required element.

As noted above, this approach is fully consistent with the military analysis of the DIME paradigm. The key point here is that military planners and operators need to include an I/IT strategy in their approaches. A subsidiary—but crucial—point is that an I/IT strategy is *not* a traditional function of the J-6 (the technical information officer on a military staff, the chief information officer in business terms). Rather, I/IT has to be a function of both J-3 and J-5: that is, built into plans and implementation and policy. The J-6 will be in a supporting/implementing role to help

execute the strategy. There is no reason why the J-6 cannot help develop the I/IT strategy, but it cannot be developed apart from the policy, plans, and execution of the larger effort. This is not a technical problem; it is a strategic effectiveness problem to accomplish host-nation harmonization, alignment, and effectiveness.

The U.S. military has already taken some important steps in terms of using I/IT as part of a stability operation. Warfighting information technology is available if and when military operations are a required part of the stability operation. This paper does not deal with those issues and instead focuses on the issue of joint stability operations activity writ large—that is, joint within the U.S. Government and combined with other non-U.S. partners. On the latter, DOD has undertaken some very worthwhile efforts under the Combined Enterprise Regional Information Exchange System (CENTRIXS) program.<sup>6</sup>

CENTRIXS is a Web-based network, developed with both commercial off-the-shelf and government off-the-shelf tools. It is designed to provide information among coalition partners in activities in which the U.S. military is involved. For example, U.S. Central Command uses CENTRIXS to support coalition military coordination and information-sharing for the Multinational Force in Iraq and the International Security Assistance Force in Afghanistan. CENTRIXS operates on military classified networks, so it is not broadly available to all participants in a stability operation. It is, however, quite useful for information exchange among coalition militaries and is a good step in the direction of using information in stability operations.

*Element 3.* The third element of an I/IT strategy for the U.S. Government for stability operations is to pre-establish I/IT partnerships with key stability operations participants. It is important to underscore the word *key*. It is not possible, and would not be effective, to try to establish pre-existing partnerships with all of the many players who will be involved in a stability operation. But there are some very key players from the government perspective.

A few countries can be expected to participate in many and even most operations that the United States does. The United Kingdom is one; Australia is another. Certain key international organizations likewise will be there. The UN certainly would be involved—though dealing with the UN requires dealing with a variety of UN groups and agencies, since it does not act as a single entity. Thus, planning will be important with the Office for the Coordinator of Humanitarian Affairs, the UN Development Program, the UN Department of Peacekeeping Operations, and perhaps the UN Children’s Fund. NATO is often a player, as well as the European Union. Major nongovernmental organizations will also regularly be engaged in stability operations. In fact, these organizations will generally be there in advance of the U.S. military. The fact that preplanning only includes some players is meant to allow for creation of a useful framework. An effective I/IT strategy will include many others, and there may be conferences, meetings, and workshops of a broader nature. But real planning will be enhanced by a more limited approach.

*Element 4.* The fourth element of an effective information strategy is to focus on the host nation. The importance of establishing host-nation effectiveness has already been emphasized. Informing host-nation decisionmaking, enhancing governmental capacities, and supporting societal and economic development are all crucial elements of an information strategy. Working with I/IT as discussed below can help generate important progress in security, humanitarian, economic, and governance/rule of law arenas. The recognition by the

international community of the harmonization and alignment goals is important. However, when information technology is considered, all too often harmonization with respect to the intervenors becomes emphasized as compared to alignment and effectiveness of the host nation. This is backwards. An effective I/IT strategy is one that makes the host nation effective. Nothing else will do. Thus, a critical element of the strategy is an I/IT business plan for the host nation and an intervenor support strategy that aims to enable the host-nation business plan.

*Element 5.* The last element of an I/IT strategy will be to work with others to use the key technical capabilities to support the effectiveness, harmonization, and alignment goals. The specifics are discussed below, but a crucial point is that generating the technical part is far less about invention—the information revolution has given us and continues to give us broad capabilities—than it is about developing ways to use those brilliant inventions in an overall effective, collaborative fashion. The planning aspects of the strategy are crucial to effective use of the tools. Common choice can create highly effective capabilities. Divergent choices can undercut well-meaning strategies.

## Operationalizing the I/IT Strategy

It is one thing to have a strategy; it is quite another to implement it effectively. The discussion below sets forth how to implement an operational I/IT strategy. A key point is to remember that both the end goal (creating an effective host nation) and the strategic context (the I/IT strategy itself) must be developed and implemented inside an overall approach of harmonization and alignment that supports enabling the host-nation security, humanitarian, economic, and governance activities.

To effectuate those tasks, the U.S. Government needs to adopt an information business model with multiple key elements. Those who have responsibility for the I/IT strategy, which ideally will be a joint effort led by the Department of State (including USAID) and DOD, will need to run the business model in a focused, long-term fashion; otherwise, achievement of the strategic aims will be jeopardized.

The business model breaks down into two broad elements: harmonization among outside intervenors, and effectiveness and alignment for, and with, the host nation.

*Harmonization.* On the harmonization side, a good place to start operational analysis is to recall the complexity of the problem and the number of intervenors. As discussed above, an important element of the strategy is to undertake preplanning with key partners. There are four important elements of preplanning to achieve harmonization.

First, joint civil-military information planning will be critical. In the first instance, this needs to be done between the Department of State and DOD, but most importantly it needs to be done between the U.S. Government and other major intervenors to harmonize their interventions. It is not an impossible task to keep others informed and aware, but it is difficult. Issues arise immediately as to what data can be provided and how information can be exchanged. With respect to the latter, development of agreed management and data standards can fundamentally enhance the provision of information. Pre-event planning and face-to-face meetings can enhance trust and provide important education about others' methods. While the myriad actual stability operations have provided some reasonable knowledge about different key actors, on-the-job learning is necessarily more difficult because of the requirement to

do one's "day job." Accordingly, some common training, exercising, and/or education away from a stability operation can create potentially significant opportunities to enhance harmonization. None of this will occur unless an element of the government, preferably a joint Department of State-DOD element, focuses on the requirement for preplanning.

Second, improved collaboration depends on both better processes and use of available technical means. The process issue is perhaps the most crucial. As noted above, it is important to decide how, with whom, and how much data are shared. There is a general tendency, particularly at DOD, to come at the problem through a classified lens. That is, since DOD is used to treating data as classified, the question is often framed as how such data can be made available. Often, the answer is given in binary terms: information either can be made available or it cannot. This all too often becomes a least common denominator approach because the judgment is made that if the data are not available to some, it cannot be available to any.

A much better approach would be to recognize that, in stability operations, most relevant data are broadly available from other than classified sources—though often not broadly collected. Furthermore, and most importantly, data can be shared on a differentiated basis. For example, information provided to Japanese civilian officials can be differentiated from information provided to World Bank officials, which can be differentiated from information provided to Red Cross officials. Groups that have engaged in preplanning and have built up trust will find it easier to share information than groups that meet only in the circumstances of the stability operation. Differentiation is one key element to enhancing data-sharing—and working differentiation as an effective operational approach will depend on preplanning.

A second important step to better data-sharing will be better use of technical means. For example, the Internet has become a mechanism for unclassified collaboration and sharing of information among civilian and military elements responding to crisis operations. Furthermore, commercially available collaboration tools and other tools, such as video teleconferencing and Web-cams, are being used by them on the Internet. Technologies are improving quickly to enhance data-sharing. In the civilian arena, the growth of Web logs (blogs), file-sharing, Wikipedia, MySpace, and similar sites all attest to the possibilities of sharing, if the desire to use the mechanisms is there. Many organizations already run sites to make information available (for example, the UN-sponsored ReliefWeb). However, the collaborative aspects of these sites are limited.

U.S. Joint Forces Command (USJFCOM) has taken strides to enable the sharing of unclassified information with nontraditional partners. The command has conducted several exercises that explore this challenge, and Multinational Experiment 4 specifically addressed it. The command is also standing up a nonmilitary domain portal outside its firewall that takes an approach more akin to that of a relief organization—many of which are linked to it—than a military one. The portal (<http://harmonieweb.org/>) enables people and organizations who are participating in a relief effort to obtain and post information that may be valuable in providing the needed assistance.<sup>7</sup>

Additionally, the United States is encouraging the development of an open-source, collaborative arena, tentatively called "the hub," that would use blogging, file-sharing, and Wikipedia-type approaches to create an open space for collaborative sharing. It is not clear as of this writing what the outcome of that effort will be. However, even assuming its success, it seems probable that a combination of both a fully open site (the hub or some variant) and a more directed

approach (for example, NATO–UN–World Bank collaborative sharing) might be useful. Remember the point about differentiation: to try to use only one tool or one kind of approach to allow for all types of collaboration is not necessarily the most successful approach. Transferring the CENTRIXS in some modified form for collaboration among key civil-military players while generating a broader open-source approach is likely to be a useful effort.

The third element required to achieve harmonization is the development of an implementation strategy. Whatever the precise mechanism for improved collaboration, it can be fairly confidently stated that improvements will not occur absent a strategy that designates elements within the government to make such improvements happen. At the moment, there are good but separate efforts. The Office of the Secretary of Defense is working on the hub effort. USJFCOM is seeking to support elements of the Department of State and, through experimentation, is developing new civil-military coalition processes for improved collaboration and information-sharing and assessing commercial information technology tools for enabling the processes. The recent DOD directive on stability operations requires development of a collaborative information-sharing mechanism.<sup>8</sup> But there is no overall directed effort—and this key element is crucial. Otherwise, the efforts will be personality-driven and ad hoc. Such approaches are way better than nothing but not likely enough to be effective.

An improved approach to collaboration includes broad agreement on the information needed to be collected and exchanged; standards for collection and exchange; technical mechanisms for each that work together; processes; and some education and training together. The final important element of collaboration is the ability to improve data usability. As noted above, it is probably useful to think about data in two broad types of collaborative forums: a more limited network among key partners, and a broader, more open network. In each, capacities for search, aggregation, storage, and retrieval are useful and potentially important. In each, the issues of quality control and information assurance will arise, as will the issue of dissemination.

Technical improvements in recent years have significantly increased the ability to aggregate different types of data, such as the ability to put written information on photographs and to integrate geographic material with other data. That said, there needs to be some data-management group that will determine for the collaborating activity just what kind of capacities will be created—or allowed. For example, it is possible to add to a photograph the names of the people in the picture, but in certain circumstances, adding names might be very hazardous for the individuals identified. An ongoing data-management effort to create rules and manage the activity will be necessary. There is, of course, a technical aspect to this, but some of the key issues will turn out to be policy issues, so the group will need to engage both technicians and policymakers.

Information power derives from a combination of people, content, and technical capabilities. In the technical arena, there is a whirlwind of ongoing activity and innovation. A very useful capability would be to have an “information toolbox” that maintains lists of:

- key information partners, including businesses with technical capabilities
- information and data-management tools
- other key tools, such as collaboration and translation.

For the effort that we are focusing on here, commercially developed tools are essential because government-generated tools will often not be available to important partners. There will be debates between open-source and proprietary tools, and those debates need to be resolved in actual context, based on what the effort is intended to establish. The case will probably be that the broader the activity, the more desirable the use of open-source—but even that statement needs to be evaluated in the particular circumstance.

The Center for Technology and National Security Policy at the National Defense University has generated a first order “tool kits and best practices” analysis in its recently published *ICT Primer*.<sup>9</sup> That discussion includes, inter alia, review of telecommunications capabilities such as satellite communications, creation of a civil-military information environment, data and information management, and best practices. Maintaining and updating such an activity is an important element of an overall strategy.

*Effectiveness and Alignment.* The fundamental task of an I/IT strategy is to enhance host-nation capacity. That is the critical result for which the stability operation is undertaken. To accomplish that result in an effective fashion, the strategy will need to accomplish two tasks, each familiar to the international community: first, assess the host nation and, second, establish a goal toward which to build. To put it more in the vernacular, a cure without a diagnosis will be improbable; directions without destination will be random. In short, an effective approach will require an information business plan for the host nation.

The assessment phase of an information business plan should begin before the intervention. It must include analyses of both information requirements and available information technology. Unlike humanitarian interventions, such as the relief effort for the December 26, 2004, tsunami, stability operations generally have long build-up periods, so there is time to prepare. An assessment would consider the pre-intervention state of information technology and information usage in the host nation. It is important to recognize that baselines will differ in different host nations. What can be accomplished in a country with an austere, pre-crisis baseline is likely considerably different from what can be accomplished in a more built-up, moderately established country. As an example, Bosnia is different from Afghanistan in terms of establishing an information business plan. Different baselines will generate different goals, and there will be no “one-size-fits-all” approach.

Some key elements of an information assessment will include evaluation of the host nation’s telecommunications laws and regulations and communication infrastructures—land line telephone system, cell phone capacity, and Internet availability. It should also address usage patterns, language and literacy issues, technical training of locals, and financial resources.

Once an assessment has been undertaken, goals will need to be set for operationalizing the information business plan. Generally, it will be useful to time-phase the goals into an initial deployment phase, a middle phase (getting-things-going phase), and a long-term (exit-by-intervenors) phase. A critical point throughout is that the intervenors’ information business plan goals need to be in support of the overall goals for the host nation, and the host nation as promptly as possible will need to help generate those goals.

The initial deployment phase will require the intervenors to consider what deployable capabilities will be useful to help establish a host-nation element or elements. There are both structural information

capabilities, such as deployable cell phone capacities and the use of satellites, and functional capabilities, such as “health care in a box,” that need to be considered.

The virtue of preplanning is that key intervenors can rationalize their capacities in the early, usually chaotic days of an intervention by considering which capabilities each might focus on. Equally important is to undertake such a discussion remembering that, first, numerous entities will already be in country with some capacities that can be utilized and that, second, host countries will likely have some capacity, and perhaps some significant capacity. Over the entirety of the intervention, the implementation of the information business plan likely will mean that the lead on different aspects of the plan will change. Broadly, one might expect a move from outside military intervenors to outside civilian intervenors to host nation, although the reality is likely to be more coordinated and complex. The transitions will occur over time, so there will be overlaps that need careful management. If it is understood from the beginning that there will be transitions in the way the plan is implemented, it will make for a more realistic and effective approach.

The middle phase of an information business plan for the host country will focus on five key elements. First is to *align the host country so that it is connected to the collaborative mechanisms used by the intervenors in some fashion*. While the key intervenors likely can use high-tech means, it may be that the host country will not be able to do so. An important task of an information business plan will be to allow for low-tech to high-tech connectivity. As an example, in Afghanistan, the literacy rate is so low that Internet use is necessarily limited and cell phone connectivity may be much more important. In fact, in Afghanistan, the cell phone is the lifeline communications capability. These points can be more broadly generalized: if the information business plan is to succeed, it must take account of the host nation’s information culture and the related information technology culture.

A second element is to *help establish working government agencies*. Depending on the overall strategy, these could be central ministries or local/provincial offices. Information technology can be used to improve ministry effectiveness, especially to allow for an analytic approach through budgeting and transparency of expenditures. Those are crucial functions for the establishment of legitimate governance, and information technology can help each.

A third element for many stability operations will be to *increase connectivity between the central government and provincial/local governments*. Information technology can enhance this connectivity through, for example, the two-way flow of data and finances. Often, the cause of the crisis will have been differences between the central government and a region of the country, and working to bring warring elements together will be important. An information business plan can be an effective part of an overall effort.

A fourth element will often be to *provide certain important greater functionalities in government services to the populace*. While an information business plan may not be able to improve all functionalities significantly, health and education are two arenas of consequence in which such a plan can make an important difference. In the health arena, information technology can be used to build up local centers of health care, such as hospitals; support training of health care workers; and provide valuable functionalities, such as health surveillance systems. In the education arena, information technology can support curriculum establishment and the provision of instruction, as well as the training of teachers.

The fifth element is to *provide for the private-sector development of information capabilities*. Two of the most important issues are informed regulatory mechanisms and useful seed financing. An overly constrained regulatory environment will make it difficult for private enterprise to operate at a profit. A properly structured set of incentives can help create an environment in which profit-making companies can contribute importantly to economic reconstruction. Seed money may be very important, especially in the early days of a stability operation, particularly to get local involvement in the development of the information business plan.

The middle phase of the plan often may be the equivalent of the medical “golden hour” for establishing a framework for effective use of I/IT for the host nation. While the information flow may be limited, meeting expectations of the host government and population during this middle phase will be very important to longer-term success for the intervention and the host nation.

The middle phase will naturally flow over into the long-term phase for the host nation and the exit strategy for the intervenors. That part of the information business plan strategy should have at least three key elements. First, as noted above, the private sector should become a key element. Creating an environment in which there are commercial opportunities for information technology and information firms will help seed economic revitalization. Second, the host nation will need to consider what role it will play in the development of a national information technology infrastructure. Models range from full privatization to early phase ownership to ongoing involvement. Third, as part of their effort in country, intervenors will have established IT capabilities. Such facilities and datasets should not be automatically dismantled as the intervenors leave. Rather, they should be built as leave-behinds for local partners, both governmental and nongovernmental, whether commercial or nonprofit.

An I/IT strategy includes people, content, and technology. In a stability operation, the information needs—the content of what must be provided in addition to the connectivity—of the host nation require consideration. Broadly speaking, those information content needs will fall into the categories of security, humanitarian, economic, governance/rule of law, and social.

In analyzing how such information needs should be fulfilled, an I/IT strategy will recognize that the information element will support functional strategies for each of these arenas—all of which will have significant subparts. For example, the establishment of prosecutorial, court, and prison functions will have security and rule of law/governance aspects. Significant programs will be under way to help create each of these elements as part of a stability operation. Responding to the information needs of those programs has to be an affiliated strategic effort—or, to use the terms of the international community, needs to be aligned with the overall aims of the functional programs.

The specific needs may be provided with the use of information from one or more of the intervenors. In a variety of ways, information technology can be utilized to provide expert assistance. A simple example is maintaining an online list of experts. More sophisticated efforts can be established, such as a call-in center for the provision of various kinds of information. Research arrangements can be set up online, as can connectivity with key national and international organizations, both governmental and nongovernmental, that are willing and able to provide assistance.

As is true for the technology itself, information needs change over time. In fact, the ability to provide information may become more important as the host nation develops its own capacities. The capacity to access such information may be developed in two parallel fashions. First, in a traditional approach there could be an office to help facilitate access to expert management. More recently, a distributed approach, such as Wikis and blogs, may be able to make a great deal of expert information available without a specific data manager, if the right information tools are provided. Issues of trust and reliability will arise, but the community approach to providing information via the Internet has been very powerful in other arenas, and its use in stability operations should be encouraged.

The discussion of the management of information needs raises the important question of how to manage the I/IT strategy in the course of the stability operation. Adoption of a strategic approach and even operational activities will be greatly facilitated by the establishment of a forward field organization. Ideally, this would be a joint Department of State-DOD function with the job of carrying out the information strategy in country. In a stability operation, the organization likely would be collocated with the military command activity.

The role of the organization would include carrying out the U.S. Government aspects of the I/IT strategy. In addition, the organization would collaborate with the organizations with which preplanning took place, including key countries, the UN, and major nongovernmental organizations. As promptly as possible, the organization will want to begin to work with the host nation, though precisely what that means will depend on the circumstances of the operation. As a forward community of interest is being set up, the organization will want to create mechanisms that add to the effort entities that have not been part of the preplanning. As discussed above, a hub type approach may be very valuable, as may more structured relationships. In addition, the organization will want to work with the public affairs office to facilitate interaction with the media and, most importantly, information for the public at large.

## Conclusion

I/IT can be important components for success in stability operations. Achieving successful results requires that a purposeful strategy be adopted to use these capabilities to the desired end of building up the host nation and to develop operational activities that effectively implement the strategy. A strategic approach causes coalition participants to undertake five key activities:

- conduct pre-event activities with partners
- implement improved collaboration
- ensure improved data usability
- develop an information toolbox
- create a forward field information office.

Also, creating an overall focus to generate an effective host-nation information business plan consists of four actionable items:

- assessing host-nation information capacity
- building a host-nation information goal
- creating immediate, medium, and long-term information capacities
- analyzing information needs and developing methods to fulfill those needs.

These activities and items can generate an environment in which the information revolution can help create success in stability operations.

## Notes

<sup>1</sup> *Net-centric warfare*, as defined by the Department of Defense Functional Capabilities Board, refers to: warfighting that networks all elements of an appropriately trained joint force; integrates their collective awareness, knowledge, and experience in order to rapidly create new capabilities, make superior decisions, and achieve a high level of agility and effectiveness in dynamic and uncertain operational environments.

<sup>2</sup> Department of Defense (DOD) Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*, Section 4.2, provides: "Stability operations . . . immediate goal . . . is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and a robust civil society." In this paper, the term *stability operations* is used per the DOD Directive to mean the full-spectrum of stabilization and reconstruction activities.

<sup>3</sup> World Bank, Operations Policy and Country Services, *Fragile States—Good Practices in Country Assistance Strategies*, December 19, 2005, vii, available at <[www-wds.worldbank.org/external/default/WDSContentServer/1W3P/IB/2005/12/22/000090341\\_20051222094709/Rendered/PDF/34790.pdf](http://www-wds.worldbank.org/external/default/WDSContentServer/1W3P/IB/2005/12/22/000090341_20051222094709/Rendered/PDF/34790.pdf)>.

<sup>4</sup> Organisation for Economic Co-operation and Development, Development Cooperation Directorate, Senior Level Forum on Development Effectiveness in Fragile States, Harmonisation and Alignment in Fragile States, December 17, 2004, 14, available at <[www.oecd.org/dataoecd/20/56/34084353.pdf](http://www.oecd.org/dataoecd/20/56/34084353.pdf)>.

<sup>5</sup> Ibid.

<sup>6</sup> Jill L. Boardman and Donald W. Shuey, "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-Wide," available at <[www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf](http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf)>.

<sup>7</sup> Robert K. Ackerman, "Unclassified Information New Key to Network Centrality," *SIGNAL Magazine* (September 2006), available at <[www.afcea.org/signal/articles/templates/SIGNAL\\_Article\\_Template.asp?articleid=1185&zoid=52](http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1185&zoid=52)>.

<sup>8</sup> DOD 3000.05, Sections 5.1.9, 5.7.1.

<sup>9</sup> Larry Wentz, *An ICT Primer: Information and Communication Technologies for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction*, Defense and Technology Paper 31 (Washington, DC: Center for Technology and National Security Policy, July 2006), available at <[www.ndu.edu/ctnsp/Def\\_Tech/DTP31%20ICT%20Primer.pdf](http://www.ndu.edu/ctnsp/Def_Tech/DTP31%20ICT%20Primer.pdf)>.

Defense Horizons is published by the Center for Technology and National Security Policy. CTNSP publications are available online at <http://www.ndu.edu/ctnsp/publications.html>.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk  
Director

# Strategic Fragility: Infrastructure Protection and National Security in the Information Age

by Robert A. Miller and Irving Lachow

## Overview

Modern societies have reached unprecedented levels of prosperity, yet they remain vulnerable to a wide range of possible disruptions. One significant reason for this growing vulnerability is the developed world's reliance on an array of interlinked, interdependent critical infrastructures that span nations and even continents. The advent of these infrastructures over the past few decades has resulted in a tradeoff: the United States has gained greater productivity and prosperity at the risk of greater exposure to widespread systemic collapse. The trends that have led to this growing strategic fragility show no sign of slowing. As a result, the United States faces a new and different kind of threat to national security.

This paper explores the factors that are creating the current situation. It examines the implications of strategic fragility for national security and the range of threats that could exploit this condition. Finally, it describes a variety of response strategies that could help address this issue. The challenges associated with strategic fragility are complex and not easily resolved. However, it is evident that policymakers will need to make difficult choices soon; delaying important decisions is itself a choice, and one that could produce disastrous results.

## Faustian Bargains

Developed societies around the world face an unexpected paradox: though wealthy beyond the dreams of earlier generations and able to call forth vast resources and project influence across the globe, they face threats and dangers that did not exist a few decades ago. During the past half-century, global integration has accelerated significantly. A growing number of nations and regions have been incorporated into the international economy, which now depends on a set of intercon-

nected critical infrastructures that in many cases extend far beyond national boundaries and are controlled by an increasingly elaborate information grid. Information has become both instantaneous and ubiquitous; it often seems that very little happens anywhere that is not known within a few hours everywhere. In many cases, these critical infrastructures are the keys to our prosperity. We depend on them. But they can break—or be broken.

The development of these linked infrastructures and interdependencies has taken place with astonishing rapidity. They have emerged, seemingly out of nowhere, within the past few decades. The result is revolutionary.

An excellent example of this change is in merchant shipping. For many, the word *seaport* conjures up an image of sailors and longshoremen swarming over cargo-strewn piers, but that world no longer exists. Almost all of the longshoremen are gone, as are most of the merchant sailors. Many once-bustling ports have shrunk, their piers replaced by office buildings, condominiums, entertainment centers, restaurants, parks, and other amenities of the modern city.

The major reason for this transformation has been the advent of containerized shipping.<sup>1</sup> Almost unknown half a century ago, containers are now the primary method for moving finished goods around the world. In a sense, containers have made globalization possible. Not so long ago, the cost of transportation was a significant part of the total cost of any product, which was why so many factories were located near their ultimate customers. Now, the cost of transportation has dropped precipitously and businesses can move their operations far from customers—even across a continent or ocean—and still be competitive with businesses only a few miles from the point of sale.

Within little more than a generation, the old way of handling freight—break-bulk loading of goods stacked on pallets onto small merchant ships by gangs of longshoremen—has become as antiquated

as oxcarts and almost as rare. Approximately 90 percent of the world's trade in non-bulk goods is transported in cargo containers. In the United States, almost half of incoming trade (by value) arrives in containers piled high on very large, specialized ships. Millions of these containers arrive at U.S. seaports each year.<sup>2</sup> To be efficient, though, these new container ships have to operate through large, carefully designed, highly automated, and extremely capital-intensive ports of call.<sup>3</sup> The inevitable result is that a growing percentage of traffic is routed through a few large ports. By 2003, just five U.S. seaports carried 60 percent of America's total container traffic.<sup>4</sup>

Coupled with concomitant improvements in intermodal transportation, end-to-end supply chain operations, and information-based logistics management systems, containerization has brought radical improvements in efficiency. These changes have permitted huge increases in capability and profitability. By putting more eggs into a smaller number of baskets, companies have cut costs across the board. Our just-in-time world hums along more and more efficiently—until one of these baskets breaks or is broken.<sup>5</sup>

Two conspicuous examples of this pattern of concentration and the resulting vulnerability are electric power grids and air traffic control systems. Today's interconnected, continent-wide power grids are much better than their local and regional predecessors at providing cheap and reliable power, and they are significantly less prone to local breakdowns. But when they do crash, the consequences are far greater than those of the more frequent and more localized failures of past decades. Similarly, the highly integrated systems that control air traffic are much safer and more efficient than the disjointed regional systems of half a century ago, but when the system seizes up, the effects are far more immediate and widespread.

Everyday life offers many more examples of growing system dependencies and tight linkages. Consider traffic signals. Ubiquitous, unremarkable, and essential to traffic flow in every city, these signals were once controlled individually by mechanical devices. They were almost impossible to reset quickly in response to changing conditions. Now, traffic signals in an increasing number of locales are operated through centralized traffic-management networks. The result is that traffic management is much more flexible, easy to modify when conditions warrant—and vulnerable to widespread disruption if the system is compromised.<sup>6</sup>

The preceding examples illustrate the situation that we call *strategic fragility*. Without fully realizing it or planning it, modern societies have created a world dominated by fewer, more highly concentrated, more efficient, and more ubiquitous networks. These networks now govern our daily lives. Radical improvements in systems, processes, and operations have stimulated significant increases in global productivity by squeezing slack and redundancy out of systems and improving process effectiveness. However, these changes have also reduced local and regional resilience and diminished spare capacity available in an emergency. In some cases, they have increased exposure to potentially catastrophic failures and runaway system collapses.<sup>7</sup>

**Robert A. Miller and Irving Lachow are Senior Research Professors in the Information Resource Management College at the National Defense University. The authors can be reached at millerr@ndu.edu and lachowi@ndu.edu, respectively.**

Thus, modern societies have made an unintentional Faustian bargain that brings increases in operational efficiency and capability at the cost of greater susceptibility to widespread catastrophic failures. Most people probably would not want to reverse this bargain even if they could. Whatever doubts one may have about the globalized, interconnected planet of the early 21<sup>st</sup> century, few among us truly yearn for the slower, less efficient, more expensive world of a few decades ago. However, we must recognize that our society faces new kinds of vulnerabilities and risks. The challenge is to decide how to manage those risks in a cost-effective manner.

## Critical Infrastructures

The term *infrastructure* originally referred to physical networks that supported cities and included things such as roads, water and sewer utilities, power cables, and telecommunications lines. The contemporary concept of critical infrastructures goes beyond physical structures to interconnections and functions that enable a society to survive and thrive (see table). The working definition used by the U.S. Government defines *critical infrastructures* as “assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.”<sup>8</sup> The term also includes the virtual networks that link information assets together in cyberspace.<sup>9</sup>

### Critical Infrastructures Identified by U.S. Government

Agriculture and food	Commercial facilities (including theme parks and stadiums)
Defense industrial base	Dams
Energy	Emergency services
Public health and health care	Commercial nuclear reactors, materials, and waste
National monuments and icons	Information technology
Banking and finance	Telecommunications
Drinking water and water treatment systems	Postal and shipping
Chemicals and hazardous materials	Transportation systems
Government facilities	

*Source:* U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2006), 20. It is summarized in U.S. Government Accountability Office, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan* (Report GAO-06-672, June 2006), table 1, 9–10. The listing does not represent any attempt to rank infrastructures by importance or vulnerability. Other nations and regions have similar lists. See the *CRN International CIIP Handbook* (Zurich, 2006). T.D. O'Rourke has suggested using a simplified grouping of these infrastructures into six “lifeline systems”: electric power, gas and liquid fuels, telecommunications, transportation, waste disposal, and water supply. See O'Rourke, “Critical Infrastructure, Interdependencies, and Resilience,” *National Academy of Engineering Publications* 37, no. 1 (Spring 2007), available at <[www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-6ZQQRH?OpenDocument](http://www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-6ZQQRH?OpenDocument)>.

One of the hallmarks of critical infrastructures is that they are complex, adaptive systems that are far more capable and complicated than the sum of their physical components.<sup>10</sup> They also rely heavily on scale-free networks such as the Internet.<sup>11</sup> As one analyst has noted in summarizing current research on the topic, “while these types of networks are very resilient to random failures, they are very vulnerable to targeted attack. . . . [S]elf-organizing competitive networks are highly efficient, but have the negative externality of systemic vulnerability.”<sup>12</sup> In other words, these networks are adept at dealing with scattered outages but susceptible to well-targeted, systematic, repetitive attacks on key nodes.

The interdependencies between infrastructures and their reliance on the information infrastructure as a control mechanism make the consequences of failures in any given area unpredictable and hard to manage. In many cases, economic factors—notably, the capital costs of building facilities on the scale needed to operate and compete in a globalized marketplace—continue to create pressures toward having fewer, larger, and more geographically concentrated infrastructures. While this trend is not new, the push toward consolidation has intensified in recent years. One consequence is that in many economic areas we are seeing a smaller number of larger facilities, each of which commands a larger share of its market. A number of examples of this trend can be found in the United States:<sup>13</sup>

- nearly one-third of waterborne container shipments pass through the twin ports of Los Angeles and Long Beach
- over 36 percent of freight railcars pass through Illinois, primarily around Chicago
- about 25 percent of pharmaceuticals are manufactured in Puerto Rico, mostly in the San Juan area
- over 31 percent of naval shipbuilding and repair facilities are in or near Norfolk, Virginia.

A related trend is that various infrastructures are increasingly dependent on a few key providers of products and services. In the past, most organizations had their own unique sets of internal systems and processes. Increasingly, however, these systems and processes are being outsourced to a few companies that provide third-party logistics and supply-chain management services. In addition, many of the firms that still manage their own logistics processes have come to rely on a limited number of system integrators and application providers for core systems. The result is that many organizations that think of themselves as relatively autonomous are in fact highly reliant on a small number of contractors and suppliers, such as United Parcel Service or Federal Express (FedEx), and on information systems developed and supported by a few large vendors, such as Electronic Data Systems or IBM. As in other areas, this trend has typically brought significant increases in not only operational efficiency but also new kinds of vulnerabilities. If FedEx runs supply-chain operations for 50 firms, multiple operating systems are replaced by a single one. The one may be more effective, and even inherently more secure, than most of the 50 were, but hackers now can concentrate their attacks on one target.

### **attacks on critical infrastructure and key resources can have both direct and indirect consequences**

Looking ahead, it is likely that the next few years will see the emergence of de facto standards for the supervisory control and data acquisition systems that govern many physical infrastructures and operations. This trend is accelerating as individual companies consolidate and infrastructures are knit together firmly. More Faustian bargains are on the way.

## **Implications**

The implications of the growing dependence of modern societies on vulnerable critical infrastructures and just-in-time operations have been recognized and widely discussed for many years. Three features of these critical infrastructures increase the potential consequences of their failure: the increasing reach of individual infrastructures that in many cases span countries and continents; the interdependence of infrastructures (so that, for instance, a failure in the electric power grid will disrupt regional water and sewer infrastructures); and the increasing importance of the cyber infrastructure as a control mechanism for the others.<sup>14</sup> As the Department of Homeland Security has pointed out, attacks on critical infrastructure and key resources can have both direct and indirect consequences. Focused attacks on key assets, systems, and networks can immediately disrupt critical functions. Attacks can also have indirect effects by creating disruptions that cascade through the government, society, and the economy. Infrastructure failures stemming from natural disasters or other causes can have similar impacts.

## **Role of Public Confidence**

Most of the analyses of critical infrastructure failure emphasize (for good reason) the tangible consequences that would ensue if these infrastructures were to fail. However, the intangible factors may be at least as important. Civilized societies depend on public confidence in the stability and durability of social arrangements. There are different ways to characterize this attribute. The simplest is to define it as the general expectation that tomorrow will resemble today and that events are generally predictable and controllable by public authorities. In other words, the working assumption that most people have is that the world will remain relatively stable. If things go wrong, public confidence can be shaken and, eventually, broken. History has made it clear that a breakdown in public confidence can lead to a rapid collapse of law and order, anarchy, and a “war of all against all.” Something of this

sort occurred in the aftermath of Hurricane Katrina.

The public’s growing dependence on mass media for information about what is going on has two consequences. If communications are operational during a crisis, the media will likely *amplify* and *accelerate* the sense of crisis and dislocation (as was seen during Katrina). But what happens when these communications media are put out of commission? Many of the mediating authorities that were on hand in the past to mobilize community actions and dampen fear-mongering are less available and less effective than they once were. If the media become unavailable

because of infrastructure collapse, media-reliant individuals will feel a sense of dislocation and confusion that may leave them susceptible to rumors and misinformation.

This fact of life in the information age makes public confidence, human perceptions, and the media prime targets for hostile attack. Attempts to manipulate an enemy's morale and political support are not new, but the growing importance of the media in shaping public perceptions means that information operations have become potent strategic weapons. When combined with directed attacks on other critical infrastructures, these operations can become even more powerful.

## Threat

Threats to critical infrastructure and key resources (CI/KR) fall into three general categories: natural disasters, "normal accidents,"<sup>15</sup> and deliberate attacks. The first two are fairly common and infrastructures are generally resilient from their effects, though not always to catastrophic events such as Katrina. Deliberate attacks, while less frequent, are potentially more worrisome for two reasons. First, adversaries can study CI/KR to identify critical nodes. This is important because much of American CI/KR exhibit the attributes of scale-free networks: resilient to random attacks but susceptible to targeted attacks against key nodes. That is one reason why natural disasters and normal accidents do not usually cause long-term strategic damage to CI/KR; unless they happen to randomly take down a key node, the system as a whole will be able to recover quickly. Humans can change that. If they can identify key nodes in a given infrastructure network (the ease of which depends on the characteristics of the infrastructure in question and the capabilities, resources, and motives of the attackers), adversaries might be able to take down the whole thing in one fell swoop.

Another key factor that we can affect is the duration and/or frequency of an outage. A single incident is not likely to cause long-term damage. Infrastructures are generally built to be resilient to all but the most catastrophic events. Even if a major failure occurs, the system will likely return to operating capacity in relatively short order. However, one significant difference between natural disasters and deliberate attacks is that the former tend to be one-off events—they are unlikely to occur multiple times in a short period. In contrast, human attackers may choose to mount sustained attacks against key nodes (in one or more infrastructures) that could cause lasting damage to the Nation. The good news is that such sustained attacks are not easy to carry out. They take extensive planning and intelligence-gathering, large numbers of highly skilled people who can keep their activities secret for months or years, significant financial resources, and access to advanced test beds for rehearsal and experimentation with attack methodologies. The bad news is that the number of groups (or countries) that could undertake such operations is growing, and the trends (technological, demographic, and economic) do not bode well for defenders of CI/KR.

Exactly what kinds of attacks are adversaries likely to perpetrate against CI/KR? The answer to that question is the typical analyst's response to any query on a complex topic: it depends. To gain some insights into the problem, we need to look at both means and ends. To begin with the latter: what exactly are the attackers trying to accomplish? Do they wish to create a sense of horror and panic among a civilian population? If so, they will likely want to destroy things or kill people in a violent and spectacular way. This is best accomplished through high explosives or weapons of mass destruction. An examination of the long list of terrorist activities planned or executed since 9/11 reveals exactly such a pattern of attacks. It is not difficult to imagine a scenario where terrorists attack an infrastructure with explosives to cause massive casualties.<sup>16</sup> In fact, such scenarios are both easy to devise and difficult to prevent; they clearly deserve attention. The downside of such attacks is that they will undoubtedly cause a massive response on the part of the attacked nation. In some cases, such a response may be an intended outcome; in others, it may not. Either way, a direct attack on a nation's infrastructure will likely be interpreted as an act of war, with all of the attendant consequences.

Some attackers may have different goals in mind. They may want to disrupt a nation's infrastructures without causing mass casualties or creating conditions likely to provoke a massive response. The most common scenario fitting this description is one where an adversary disrupts U.S. logistics and transportation infrastructures in order to slow a

**by focusing on the threat from  
manmade attacks, the government has  
diverted attention from the risks  
posed by both natural disasters and  
industrial accidents**

possible American response to an attack on a third party.<sup>17</sup> Because the goal in such scenarios is disruption rather than destruction, and because these attackers may not wish to be identified, the use of cyber attacks is much more likely in these cases. Cyber attacks can be con-

ducted in ways that make attribution difficult. For example, commonly available hacker tools and techniques could be used either to deny the availability of critical infrastructures or create uncertainty in the minds of decisionmakers about the reliability and dependability of the infrastructures.

Finally, it is important to point out that the attack mode is not "either/or." An adversary could certainly use both physical and cyber attacks to achieve desired ends. The most likely goal in such a scenario would be to use cyber methods to enhance the effect of physical attacks. For example, someone could attempt to disrupt the computer or communications systems of first responders just after a large explosion in an urban area. This strategy would probably be used when the goal is massive destruction or disruption. Because physical attacks are part of this approach, and such attacks leave evidence trails, they are not likely to be carried out by parties who wish to remain anonymous.

## Policy Issues and Options

At the risk of oversimplifying a complex subject, we will group all possible response options into three broad categories: prevention and protection; resilience; and deterrence.

**Prevention and Protection.** This category includes all actions taken to either prevent an incident from occurring or minimize the impact that an incident will have on a given CI/KR. If the incidents in question are natural disasters or normal accidents, the response options generally focus on prediction and safety measures. If the incidents are manmade, the response options may include things like border security, counterterrorism, intelligence-gathering, and military operations.

Since 9/11, the United States has focused the bulk of its energy and resources on trying to prevent terrorist-sponsored infrastructure attacks. Such efforts are absolutely necessary, but they are not sufficient; it is practically impossible to prevent some kind of terrorist attack in the United States. In addition, by focusing on the threat from manmade attacks, the government has diverted attention from the risks posed by both natural disasters and industrial accidents, neither of which can be prevented by antiterrorism measures. For both of these reasons, the Nation should weigh the costs and benefits of initiatives that go beyond purely preventive measures and explore ways to increase the resilience of critical infrastructures.

**Resilience.** History has clearly demonstrated that infrastructure failures are inevitable. The goal of decisionmakers should be to minimize the impact that such failures will have on the Nation as a whole. Recent disasters such as Katrina have shown that one critical factor in restoration of infrastructure performance and maintenance of public order is the ability to mount a rapid, coordinated, and well-planned response. This can be accomplished through a variety of resilience programs. Such programs could involve a number of ideas: better insurance, continuity of operations capabilities, investments in redundant capabilities for vulnerable single points of failure, and the creation of coordinated and trained rapid-response teams similar to Germany's *Technisches Hilfswerk*. While such resilience programs can be extremely effective, funding them can be difficult because they impose short-term costs and benefits are unpredictable. However, a resilience-based approach is helpful for all types of infrastructure incidents and is almost certainly cheaper than a strategy of simply waiting for events to occur and then paying for the resulting damage. It can also save lives.

**Deterrence.** Although deterrence could be viewed as a prevention measure, we believe that it is sufficiently different from the usual range of prevention and protection options to deserve a separate analysis. Deterrence refers to the development of retaliatory capabilities to dissuade adversaries from launching an attack against U.S. assets. It is a psychological approach built upon the premise that if the costs of an attack outweigh its potential benefits, the attack will not be carried out. One can affect this calculus by increasing the likely costs of an attack (usually through the threat of retaliation) and/or by reducing the potential benefits of an attack (usually through defensive measures that fall under both protection/prevention and resilience).

The United States is already acting to prevent attacks on its CI/KR by a range of adversaries. Hopefully, it will also take additional steps to improve the resilience of its infrastructures. The deterrence issue raises another policy question: should the United States develop plans, pro-

cesses, and capabilities to threaten potential adversaries with retaliatory, infrastructure-focused operations to deter them from attacking in the first place? This is not a simple question to answer. Deterrence will not work unless the following conditions exist: we must be able to identify the adversary; the adversary must know that we have the capability to cause them great harm as well as the willingness to use that capability; and the adversary must wish to avoid the harm we can cause.

When it comes to infrastructure attacks, it is not easy to satisfy all four of these preconditions. This is especially true if an adversary uses cyber attacks. Such methods can make identification of the attacker uncertain. Will the United States be willing to retaliate in kind if it is not sure about who has attacked it? Also, what kind of response would the United States be willing and able to use in response to a cyber attack? Would that response be sufficiently robust to prevent adversaries from attacking in the first place?

To complicate matters further, some of the adversaries that the United States may wish to deter include powerful national states such as China and Russia. Is the United States prepared to convince these countries that it has the means and will to cause great harm to their infrastructures if the United States is attacked? With what capabilities will the United States threaten them credibly? How can the United States signal to these and other countries that it has specific capabilities without giving away its attack plans or escalating tensions? (This is a major problem with cyber attacks.)

Finally, transnational groups such as al Qaeda may be difficult to deter for two reasons: they may not provide easy targets for retaliatory actions, and they may not be afraid of the U.S. response. In fact, they may want the

United States to attack their assets in Muslim countries to further their goal of convincing Muslims that the United States is a great enemy.

Deterrence options do pose challenges. However, a deterrence strategy could also prove useful in some situations. Decisionmakers need to analyze the advantages, disadvantages, and obstacles associated with developing a deterrence strategy for critical infrastructures and/or cyberspace. A full discussion of the implications of such a strategy is beyond the scope of this paper but seems likely to become an increasingly important part of national security thinking in the future.

## The Private Sector

Finally, the fragility question poses new issues for public-private coordination. In many societies, including the United States, most of the critical infrastructures are owned and/or operated by private firms. This arrangement has its advantages; the private sector is usually far more flexible and adaptive, quicker to innovate, and more efficient than the public sector. However, it also carries several challenges, especially in terms of homeland security. For example, because no single private entity is responsible for an entire national or global infrastructure, and there are at least 17 critical infrastructures in the United States alone, the task of developing and mounting a coordinated private-sector

## **U.S. leaders focused on national security policy will need to confront the possibility that sustained attacks on national infrastructures could potentially limit American ability to project power**

response to threats or incidents requires dozens if not hundreds of companies to work together (not to mention that cooperation with local, state, and Federal government agencies is also required). These firms often show an admirable sense of civic obligation and patriotism, especially in times of emergency.

Nonetheless, for a variety of legal, financial, and competitive reasons, full cooperation among companies is unlikely. In addition, firms will naturally put their own business interests ahead of broader, vaguer public interests; after all, they have a fiduciary responsibility to their shareholders. Thus, while individual companies may take steps to improve their own security (which may make good business sense), it can be difficult for competing enterprises to cooperate effectively to reduce national vulnerabilities in homeland security.

If private firms lack market incentives to deal with cross-cutting infrastructure risks, society faces a dilemma—either tolerate the situation or create new incentives for cooperative efforts. These incentives could include rewards to encourage desired behaviors, such as accelerated tax write-offs or grants, and/or penalties for undesirable behaviors, such as levies that would help fund reinsurance risk pools. Determining what incentives the government should offer, how such incentives would be implemented, and how their efficacy would be measured is a vexing problem with no easy solution.

If incentives fail to produce the desired outcomes, policymakers must then decide if at least a few critical infrastructures should be regarded as public goods that the government has a responsibility to protect from “market failures.” A number of policy options flow from this perspective, ranging from government ownership of selected CI/KRs (such as the Nation’s air traffic control system) to terrorism risk insurance to legal and regulatory actions. The fundamental policy dilemma facing the United States is whether to leave things as they are and accept a higher degree of vulnerability or try to reduce vulnerability by tackling constitutional, political, and economic issues that have their own huge costs. This is an issue that deserves further debate.

If one accepts that the forces pushing advanced societies toward strategic fragility are likely to persist and accelerate, then one comes face to face with a range of difficult policy issues. For example, U.S. leaders focused on national security policy will need to confront the possibility that sustained attacks on national infrastructures could potentially limit American ability to project power. In a broader sense, policymakers will need to think about the best ways to manage the Faustian bargains that shape our societies by mitigating risks and creating more resilience to guard against the inevitable slings and arrows of outrageous fortune. None of this will be easy, fast, or cheap. But inaction will inevitably impose its own costs, and they are likely to be higher than those exacted by prudent foresight.

Defense Horizons is published by the Center for Technology and National Security Policy. CTNSP publications are available online at <http://www.ndu.edu/ctnsp/publications.html>.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk  
Director

## Notes

<sup>1</sup> For a description of the evolution and impact of containerization, see Marc Levinson, *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger* (Princeton: Princeton University Press, 2006); and Brian Cudahy, *Box Boats: How Container Ships Changed the World* (New York: Fordham University Press, 2006).

<sup>2</sup> Most liquid and dry-bulk cargos continue to move in noncontainer ships. In 2003, container ships made up 30.5 percent of vessel calls to U.S. ports. See Congressional Research Service, *Port and Maritime Security: Potential for Terrorist Nuclear Attack Using Oil Tankers*, Report RS 21997 (Washington, DC: Congressional Research Service, December 2004), 1.

<sup>3</sup> The implications of the switch to container traffic were recognized as early as the 1970s.

<sup>4</sup> The five seaports are Los Angeles, Long Beach, New York, Charleston, and Savannah. Such long-established ports as Boston, San Francisco, Baltimore, and Philadelphia barely register on the list. See *Plunkett's Transportation, Supply Chain and Logistics Industry Almanac* (Houston: Plunkett Research Limited, 2004), 32. Similar trends are evident in other sectors.

<sup>5</sup> The security issues raised by concentrations of container traffic are discussed in Michael J. Babul, “No Silver Bullet: Managing the Ways and Means of Container Security,” U.S. Army War College Strategic Research Project (2004), 1. See also Jon D. Haveman and Howard J. Shatz, ed., *Protecting the Nation's Seaports: Balancing Security and Cost* (San Francisco: Public Policy Institute of California, 2006), 2.

<sup>6</sup> U.S. Department of Transportation, *Intelligent Transportation Systems for Traffic Signal Control*, FHWA–JPO–07–004, January 2007, 2, available at <[www.its.dot.gov/ipodocs/repts\\_te/14321.htm](http://www.its.dot.gov/ipodocs/repts_te/14321.htm)>.

<sup>7</sup> On this point, see Charles Perrow, *Normal Accidents: Living with High Risk Technologies*, 2<sup>d</sup> ed. (Princeton: Princeton University Press, 1999), and *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* (Princeton: Princeton University Press, 2007), as well as Stephen Flynn, *The Edge of Disaster* (New York: Random House, 2007).

<sup>8</sup> U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2006), 103, available at <[www.dhs.gov/xprevprot/programs/editorial\\_0827.shtm](http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm)>.

<sup>9</sup> *Ibid.*, 103.

<sup>10</sup> On this point, see Steven Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” *IEEE Control Systems Magazine*, December 2001, 13, 24.

<sup>11</sup> For a good discussion of scale-free networks, see Albert-Laszlo Barabasi, *Linked* (New York: Plume, 2003).

<sup>12</sup> Sean Gorman, *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection* (New York: Elgar, 2005), 8.

<sup>13</sup> Congressional Research Service, *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, Report RL 33206 (Washington, DC: Congressional Research Service, December 21, 2005), 4.

<sup>14</sup> The 2006 National Infrastructure Protection Plan (NIPP) defines the *cyber infrastructure* as including “electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition systems, and networks such as the Internet are all part of cyber infrastructure.” 13. Although other definitions differ slightly in terminology, there is general agreement on the basic parameters of this definition. Note that the cyber infrastructure in this definition includes both the mechanisms—the systems and networks—and the content of the information. It also includes 2 of the 17 critical infrastructures (information technology and telecommunications) identified in the NIPP.

<sup>15</sup> See Perrow.

<sup>16</sup> For an interesting discussion of the threats posed by non-nation-states, see John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (New York: John Wiley and Sons, 2007).

<sup>17</sup> For a description of such a scenario, see James C. Mulvenon and Richard H. Yang, *The People's Liberation Army in the Information Age*, CF-145–CAPP/AF (Santa Monica, CA: RAND, 1999).

## Cyber Influence and International Security

by *Franklin D. Kramer and Larry Wentz*

### Overview

Cyber influence is an ongoing source of power in the international security arena. Although the United States has an enormous cyber information capacity, its cyber influence is not proportional to that capacity. Impediments to American cyber influence include the vastness and complexity of the international information environment, multiplicity of cultures and differing audiences to which communications must be addressed, extensiveness and significance of contending or alternative messages, and complexity and importance of using appropriate influential messengers and message mechanisms.

Enhancing the influence of the United States in cyberspace will require a multifaceted strategy that differentiates the circumstances of the messages, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers.

To improve in these areas, the United States must focus on actions that include discerning the nature of the audiences, societies, and cultures into which messages will be delivered; increasing the number of experts in geographic and cultural arenas, particularly in languages; augmenting resources for overall strategic communications and cyber influence efforts; encouraging long-term communications and cyber influence efforts along with short-term responses; and understanding that successful strategic communications and cyber influence operations cannot be achieved by the United States acting on its own; allies and partners are needed both to shape our messages and to support theirs.

The United States is an information superpower, estimated to produce annually about 40 percent of the world's new, stored information and a similar share of telecommunications.<sup>1</sup> U.S. dominance in information production might be expected to create commensurate influence, yet numerous opinion surveys show that approval of the United States is declining almost everywhere, as is American influence. In 2006, the Pew Global Attitudes Project found that "America's global image has again slipped" and that in only 4 of 14 countries surveyed did the United States have at least a 50 percent favorable rating as compared to 7 of 10 in 1999–2000.<sup>2</sup> A British Broadcasting Corporation (BBC) poll of some 26,000 people in 24 countries (including the United States) published in 2007 likewise confirmed that the "global perception of the U.S. continues to decline," with the populace of only 3 of the 24 countries surveyed saying the United States had a mainly positive impact on world affairs.<sup>3</sup> The mismatch between U.S. information capabilities and the actuality of U.S. influence is obvious.

This essay analyzes the factors that affect the generation of influence through cyber capabilities in the international security arena. For the United States to be more effective, a three-part cyber strategy must be developed that combines:

- psychological and marketing expertise in the application of the principles of influence
- domain expertise in the geographic, cultural, linguistic, and other arenas where the principles are to be applied
- technical and management expertise in the use of cyber capabilities and tactics.

Even with such capacities, however, U.S. cyber influence will be affected by numerous factors, including the nature of the

information environment, the multiplicity of entities undertaking communications, the actions and policies of the relevant parties (including competing communications strategies of our adversaries), and the impact of culture, belief, and emotion.

## Cyberspace Considerations

*Cyberspace* is “an operational domain characterized by the use of electronics and the electromagnetic spectrum to create, store, modify, and exchange information via networked information systems and associated physical infrastructures.”<sup>4</sup> In cyberspace, information communications technologies are used to create and transmit information and thereby generate influence. The capacities of the different technologies overlap, especially as technological convergence continues through ever-greater reliance on digitization, computers, and the Internet. A look at the technologies reveals both their overlapping natures and their particular virtues.

Classic telecommunications were built on voice-grade, circuit-switched “plain old telephone service,” which was oriented to end-to-end connection. Many of these features are now found in or transmitted by wireless platforms and capabilities, such as cell phones, WiFi and WiMax, faxes, smart phones (such as Blackberry and Treo), text messaging, and voice-over-Internet protocol. The dominant feature of the phone is speed of communication and, in its newer versions, a close approximation to “anywhere/anytime” contact.

Radio and television are top-down, one-way, broadcast communicators, divided among local, regional, or national systems and increasingly available on a continuous, often global basis through the use of satellite, cable, and streaming audio and video via the Internet. The dominant feature of radio and television is the capability to reach broadly over an area and, accordingly, provide information simultaneously to a very large audience.<sup>5</sup>

The Internet can be a one- or two-way (or more) channel that can have targeted or broad reach. The Internet can create focused groups, establish social networks, engage large populations, and allow for organization across borders. It tends to be a bottom-up, interactive, and instantaneous means of communicating. Its characteristics include “viral distribution” (the quick movement from one or a core to many through the capacity of message recipients to

become message distributors), a capacity to search for and provide useful information for action and/or education, and an ability to create influence through the communications empowerment of individuals or groups.

Telecommunications, radio and television, and the Internet have all been enhanced by digitization and the creation of capacities for multiple sources of information—no longer limited to professionals—from cameras, camcorders, iPods, compact discs, digital video discs, and video and audio tapes. User-generated content—and a sort of collective intelligence—has become one of the dynamic and influential aspects of cyberspace via capabilities such as blogs and Wiki sites.<sup>6</sup>

In sum, the ability to use cyber capabilities to communicate in the modern world is substantial and increasing, but communication does not necessarily translate into influence.

## From Communication to Influence

Translating communication into influence, particularly in the international arena, requires a full understanding of the factors that bear on the reception and interpretation of the message.

### Complex Environment

The international information environment is vast and complex. Multiple messages are being sent and received by multiple entities, simultaneously and generally in an uncoordinated fashion. Even apart from the Internet, in the United States alone, each day there are more than 12 billion display and 184 billion classified advertising messages from newspapers; 6 billion messages from magazines; 2.6 million commercial (radio) messages; 330,000 television commercials; and 40 million direct-mail pieces.<sup>7</sup>

Worldwide, in 2002, 18 exabytes (10<sup>18</sup> bytes) of new information were produced through electronic channels (telephone, radio, television, Internet)<sup>8</sup> and 5 exabytes of new information were produced by print, film, magnetic, and optical storage media.<sup>9</sup> This translates to 800 megabytes of recorded information produced globally per person in 2002.<sup>10</sup> Worldwide, an estimated 25 billion emails per day were sent in 2006—not including spam messages, which account for 60 percent of all email.<sup>11</sup>

Of course, bytes are not the only or best way to measure the information flow. Video generates more bytes than text; all of Wikipedia will fit on a 100-gigabyte hard drive, which would store less than one day’s worth of one channel of broadcast-quality TV programming. Another indicator of information flow is the more

**the ability to use cyber capabilities  
to communicate in the modern world  
is substantial and increasing, but  
communication does not necessarily  
translate into influence**

Franklin D. Kramer is a Distinguished Research Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University (NDU). Larry Wentz is a Senior Research Fellow in CTNSP at NDU.

than 1.2 billion landline telephones and 2.1 billion cell phones that are in use worldwide.<sup>12</sup> Over 1 billion people (18.9 percent of the world's population) use the Internet.<sup>13</sup> From 2000 to 2007, Internet use jumped 244.7 percent globally, with the greatest percentage increases seen in Africa (874.6 percent) and the Middle East (920.2 percent).<sup>14</sup> More than 50 million blogs are maintained worldwide, a number that has doubled every 6 months for the past 3 years.<sup>15</sup>

As the foregoing suggests, the world is awash in information and means of communication, and the market for attention is highly complicated and competitive. The actors are diverse, ranging from individuals to private entities of all types to governments to supranational entities. The topics include economic, social, governmental, and all forms of human intercourse. Information overload and "noise" are serious problems that contribute to the masking of messages.

Information is continually circulating. Multiple perspectives are regularly presented, and access can be limited in certain areas by, for example, government action.

In such an arena, even so substantial an entity as the U.S. Government is only one player. The information environment is not one in which "information dominance" or "information superiority"—in the sense of overwhelming the other players—is likely to be achieved.<sup>16</sup> "Information effectiveness," on the other hand, is achievable.

### Target-side Analysis

Communication influence is, of course, intended to affect a target or targets, whether one person or many, similar or divergent. But creating that influence requires much more than aiming communication at targets. Some key factors are considered below.

First, and most importantly, "Communication cannot be conceptualized as *transmission*. . . . The sense people make of . . . messages is never limited to what sources intend and is always enriched by the realities people bring to bear."<sup>17</sup> So, instead of a target or an audience, the other party should be considered an active participant. Hence, understanding the target participants is critical to creating the influence the communicator seeks to achieve.

Effective communication in the international arena is more difficult than communication in a familiar culture. Understanding values and belief structures, truly comprehending the language, and being knowledgeable about the information culture are key factors. One has a good feel for one's own culture, but it takes work to achieve a similar feel for another culture. For example, is the culture one where focus on the individual is the best approach, or is the group or the family more of the key influence mechanism? What is the power of the rumor mill and informal networking? What perceptions and biases should be

anticipated? All these and many other cultural factors affect the influence of an international message.

Even though culture is a good starting point in thinking about how to create influence, culture is not everything. Interest issues—the political, social, and economic imperatives—also will have huge impact. So, too, will the role of the sources of influence in the society, including key individuals, trusted advisors, and influence networks.<sup>18</sup> The mindset and behavior of such individuals and networks will have significant impact on the interpretation of the message and, hence, on its influence.

In short, the communicator's problem is how to address simultaneously multiple communication partners. This problem is familiar in the context of U.S. political campaigns, where the

communicators must reach the political base, the swing vote/ neutrals, and the opposition, as well as pundits all at the same time. This problem is heightened in an international context. In the targeted nation or nations, there will be government officials, other key leaders, both political and private (for example,

business and nongovernmental groups), and the population at large, which likely will be divided along racial, cultural, religious, and other lines. In addition, for many international messages, and certainly for the most important, other nations will be interested. That "group," of course, is also likely to be highly divergent, including friends and potential allies, neutrals, and potential or actual enemies. Moreover, the message we deliver to others also will be delivered to ourselves—to the affected portion of the government, the Congress, and the population at large.

Finally, whether the target partners are influenced by the message will be significantly affected by the fact that "research has shown that people inform themselves primarily at moments of need."<sup>19</sup> This has been found to be true in the context of American commercial and domestic political messaging campaigns. The issue of need requires evaluation in the context of an international geopolitical influence effort. Determining the need for information—and therefore the basis for influence—in a different society brings the communicator back to the importance of understanding that society, culture, interests, and entities.

### Message Delivery

Understanding the target participants is only part of the communicator's challenge. A second key aspect is the delivery side of messaging: How are the contents of the message chosen? How are the delivery means chosen? How are the messengers chosen?

With respect to content, the most important understanding the communicator must achieve is that what he says is only part of the content. Already noted is the fact that the recipient will participate in shaping the message. Also of crucial importance,

## **effective communication in the international arena is more difficult than communication in a familiar culture**

however, is what might be called the “message-facts relationship.” In speaking of the importance of information as a part of counterinsurgency warfare, David Galula, in his classic book on the subject, points out that “facts speak louder than words”; “[the counterinsurgent] is judged on what he does, not on what he says”; and “nothing could be worse than promising reforms and being unwilling or unable to implement them.”<sup>20</sup>

Counterinsurgency is far from the only circumstance in which international messaging will be undertaken. The point, however, is universal: words can only go so far in the face of real-world evidence that undercuts them or is otherwise more influential.

One important aspect of which the communicator must be aware is the nonverbal message, which often is more influential than the verbal message. As an illustration, Colonel Ralph Hallenback, USA (Ret.), who operated in Iraq as a Coalition Provisional Authority (CPA) civilian, observed, “There has been much subsequent handwringing about CPA’s lack of strategic communication with the Iraqi people. [But] a lot of people had no electricity but could look across the river and see the CPA all lit up at night. And that was the way we really communicated.”<sup>21</sup> If the nonverbal message is not considered, unintended consequences may overwhelm the intended impact of the message.

Assuming that the message content will not be overwhelmed by the message context, the message must still be chosen to have the desired effect, given the nature of the target audience and the environment. Messages can be delivered directly or indirectly, and sometimes an indirect message may be more effective than a direct one. What might be considered a logical argument may have limited impact because the target participants have strongly held positions for cultural, emotional, or psychological reasons. For example, a campaign for the rule of law may be seen as undercutting the position of elders in a tribal society.

Few new messages have immediate impact, and the role of repetition must be considered—as must the role of timing and whether the message will fill an information need. Direct, hard-hitting confrontational messages also may be appropriate, depending on the results sought. But some messages will not work at all in some environments, although the desired effects may be achievable with a different message.

Different means of delivering messages will achieve different results. Cell phones were the great factor in Ukraine’s Orange Revolution. User-generated content such as blogs and digital pictures have had great impact, most notoriously in the Abu Ghraib scandal. Television has had a decided impact on the world’s view of the ongoing conflict in Iraq. Such cyber mechanisms, of course, can be complemented or outrun by simple

word of mouth—rumor probably is the greatest factor in the views held by many in the Arab world as to who was responsible for the 9/11 attacks. For example, there is continued doubt in the Arab community that Muslims were involved, even after the release of the video in which Osama bin Laden takes credit for the attacks. The effective communicator will analyze the full spectrum of potential message arenas from word-of-mouth discussions, print media, cell and telephone capacities, data networks, including portals and messaging, and radio, television, and movies—all of which are complementary, and many of which are converging because of technological advances.

Different delivery means also may imply different messengers, and the choice of messenger is surely important.<sup>22</sup> A messenger may appeal to an audience for many reasons ranging from trust and respect to common interest to celebrity “buzz” to fear. The importance of the culturally attuned messenger is implicit in another point made by Galula, who stresses the importance

of finding and organizing the “favorable minority.”<sup>23</sup> In his analysis, that minority, working with the outside intervening power, has an important capacity to help resolve the insurgency issue. The reasons, of course, include the minority’s understanding of the context for the insurgency and the ability to involve the rest of the country in its resolution. The lesson for the international communicator, more

generally, is that communications undertaken with the help of knowledgeable, favorable, local messengers will have a greater chance of success,<sup>24</sup> both because third-party communications are often more effective than those of intervening outsiders, and because the knowledgeable local can help make outsiders more effective.

## U.S. Cyber Capacities

The U.S. Government uses a variety of mechanisms to create influence in international cyberspace. For example, public affairs offices at the White House, the Department of State (DOS), the Agency for International Development (USAID), and the Department of Defense (DOD) all use television and radio appearances and maintain Web sites to deliver messages. The information is immediately available worldwide, generally circulated without charge by private media, and increasingly available for review on the Internet. The government’s public affairs capacity is enhanced by numerous additional offices and multiple sites. Every Embassy has a public affairs activity, as do numerous DOD commands, and there are many Internet capabilities.

**the effective communicator will analyze the full spectrum of potential message arenas—all of which are complementary, and many of which are converging because of technology advances**

In addition to public affairs, the United States undertakes formal public diplomacy led by the Undersecretary of State for Public Diplomacy. The Public Diplomacy office emails fact sheets, news, event announcements, and electronic journals, and DOS experts are even made available electronically. Embassies also use cyber means, and Embassy Web sites present substantive material.

A third area of U.S. cyber capability is the Broadcasting Board of Governors (BBG).<sup>25</sup> Since October 1, 1999, the BBG has been the “independent federal agency responsible for all U.S. government and government sponsored, non-military, international broadcasting.”<sup>26</sup> According to the BBG:

every week, more than 100 million listeners, viewers, and internet users around the world turn-on, tune-in, and log-on to U.S. international broadcasting programs. . . . [D]ay-to-day broadcasting activities are carried out by individual BBG international broadcasters: the Voice of America (VOA), Alhurra [television], Radio Sawa, Radio Farda, Radio Free Europe/Radio Liberty (RFE/RL), Radio Free Asia (RFA), and Radio and TV Martí, with the assistance of the International Broadcasting Bureau (IBB).<sup>27</sup>

A fourth use of cyber capabilities by the U.S. Government is what DOD calls *information operations*, which include “electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities.”<sup>28</sup> A key function of information operations is “influencing the way people receive, process, interpret, and use data, information, and knowledge.”<sup>29</sup>

DOD also makes good use of cyber capabilities to create close partnerships with other countries as part of an overall information campaign. The Partnership for Peace Information Management System was established by DOD in 1996 to support the North Atlantic Treaty Organization’s (NATO’s) Partnership for Peace members and still seeks to “facilitate collaboration and strengthen relationships in the Euro-Atlantic and Partnership for Peace community.”<sup>30</sup>

The Asia-Pacific Area Network was created in 1998. Hosted by U.S. Pacific Command, it is a “World Wide Web portal offering information resources and a collaborative planning environment as a means to greater defense interaction, confidence-building, and enhanced security cooperation in the Asia-Pacific Region.”<sup>31</sup> DOD also uses its cyber capacity to plan, support, and conduct exercises on line to work with and influence others.<sup>32</sup>

As the foregoing suggests, the U.S. Government makes extensive use of cyber capacities, particularly the Internet. At State, for example, the USInfo site presents a large amount of information on a daily basis, not only in English, but also in Spanish, French, Russian, Chinese, Arabic, and Persian. State also runs ejournalUSA, which has articles in five thematic areas—Economic Perspectives, Global Issues, Issues of Democracy, Society and Values, and Foreign Policy Agenda—and is available in the same seven languages, plus Portuguese. DOD sponsors

a number of information and online news Web sites. Some sites, such as ones maintained by U.S. Central Command, produce information relevant to some of the most difficult issues, particularly the war in Iraq. Others, such as the Southeastern European Times (published in nine languages) and Magharebia (published in three languages) provide “regional news,” and “in-depth analysis” for their respective areas.<sup>33</sup> DOD networks also add to the government cyber use.

Creating a more effective U.S. Government use of cyberspace will involve more than simply getting more information online. To provide the right information at the right time and place to help achieve the desired effect, the government needs a comprehensive strategy and plan to focus on the target audience, including the audience’s information culture and needs.

## Issues for Cyber Effectiveness

As a general proposition, U.S. Government cyber communications focus on a “mass messaging” approach, seeking to enhance and increase information flow. Mass messages have an important function. It is a very big world, and the government has interests all around it. Simple practicality calls for the use of mass messages.

The downside of mass messages is that they are in transmission mode. As previously discussed, however, virtually no communication is received without the audience “being involved in creating meanings.” Moreover, the meanings created will importantly reflect the target’s culture. Thus, the issue that arises for the United States is what is often described as *segmentation*, dividing the mass audience to focus on specific receiver needs. Creating segmentation in a real world of multiple, overlapping audiences is a difficult, though not impossible, proposition.

It is not likely that the government will abandon the mass messaging approach. The White House Web site, the daily DOS Washington briefing, and numerous similar activities will continue. Segmentation, and a focus on the culture of less than an “all-world” mass audience, will need to be done by different message channels.

## Evaluating U.S. Cyber Influence Effectiveness

One obvious way to segment messages would be through the Embassy posts. There, however, the Government Accountability Office (GAO) has found government performance deficient, stating that posts did a “poor job of answering [the] basic question of whether to direct . . . communications efforts at a mass audience or opinion leaders.”<sup>34</sup>

A second problem for creating effective messages arises from what can be called the “problem of multiplicity,” almost always an issue for U.S. Government strategic messaging. For any communicator working on behalf of the government, it is important to recognize that the United States has multiple goals and operates in a very complex world. The profusion of messages that the government generates reduces its capacity to have a single, focused message on any particular topic.

A multiplicity of message follows from a multiplicity of policy, and a multiplicity of policy means that, sometimes, policies must be prioritized and even apparently inconsistent policies must be followed. Multiple policy objectives can create difficulties for consistent messaging. To take two obvious examples, the United States seeks good relations with both Japan and China. Because these two countries sometimes are at odds, positive messages to one can be seen as negative messages to the other. A similar messaging dilemma has occurred in the context of the Middle East peace process.

As noted earlier, it may be possible to help resolve the problem of multiplicity of messages by focusing on a regional or country basis. As a real-world matter, however, the GAO found that U.S. Embassies “did not have a core message or theme to direct their communications efforts.” In fact, of the posts reviewed by GAO, none had a detailed communications plan.<sup>35</sup> This absence of thematic messaging is evident in the headline links of Web pages of American Embassies. The entries are perfectly reasonable topics for a Web page, but the pages lack thematic consistency and the pages simultaneously present very different kinds of messages. Part of the reason is that the Embassies are undertaking both long- and short-term messaging. Long-term efforts seek to build credibility and trust sufficient to sustain dialogue even amidst policy disputes. The focus is values-driven, and the expectation is that objective presentation of information will ultimately put the United States in a favorable light. This can be a reasonable function for mass messaging approaches. By contrast, short-term messaging is advocacy- and event-driven and seeks to build support for discrete U.S. policies. It is very unlikely, given the various audiences, values, interests, and actions relevant to a policy, that mass messaging will regularly produce short-term effects. A more tailored approach will be important.

### **public affairs messaging, particularly from the United States, is not a place where tailoring for a non-U.S. audience is easily undertaken**

U.S. status as an information superpower has not translated to international influence. Both the Pew poll published in mid-2006 and the BBC poll published in January 2007 underscore the declining international perception of the United States. The United States currently has this low standing despite a variety of efforts to improve its standing and regular use of the Internet and other communications means to make its points.

The problems associated with mass messaging, multiplicity of messages, and lack of core themes were discussed above. Other impediments to influence were addressed 60 years ago in the seminal research article, “Some Reasons Why Information Campaigns Fail.”<sup>36</sup> To understand better how to “promote the free flow of ideas by word and image” on a worldwide basis, the authors focused on the “psychological barriers to the free flow of ideas.” Based on the research, they reached some important conclusions.

First, there “exists a hard core of chronic ‘know-nothings’”—persons who have little information about events. The study points out that “there is something about the uninformed which makes them harder to reach, no matter the level or nature of information.”

Second, “interested people acquire the most information.” Noting that “motivation” to acquire information is key, the study also recognizes that large groups in a population will have little or no interest and “such groups constitute a special problem which cannot be solved simply by ‘increasing the flow of information.’”

Third, the study found that “people seek information congenial to prior attitudes.”<sup>37</sup> They also “avoid exposure to information which is not congenial.”<sup>38</sup> The study’s important conclusion is that “[m]erely, ‘increasing the flow’ is not enough, if the information continues to ‘flow’ in the direction of those already on your side.”

Fourth, “people interpret the same information differently. . . . It is . . . false to assume that exposure, once achieved, results in a uniform interpretation and retention of the material. . . . [I]t has been consistently demonstrated that a person’s perception and memory of materials shown to him are often distorted by his wishes, motives, and attitudes. . . . Exposure in itself is not always sufficient. People will interpret the information in different ways, according to their prior attitudes.”

Fifth, and perhaps most importantly, “information does not necessarily change attitudes”:

The principle behind all information campaigns is that disseminated information will alter attitudes or conduct. There is abundant evidence in all fields, of course, that informed

people actually do react differently to a problem than uninformed people do. But it is naïve to suppose that information always affects attitudes, or that it affects all attitudes equally. The general principle needs serious qualification. There is evidence . . . that individuals, once they are exposed to information, change their views *differentially*, each in the light of his own *prior* attitude.

Sixth, and in light of the foregoing, the authors reached the conclusion that the “above findings indicate clearly that those responsible for information campaigns cannot rely simply on ‘increasing the flow’ to spread information effectively.”

The implications of these conclusions for the effectiveness of U.S. cyber influence are substantial. Information will tend to be accepted and understood in light of prior attitudes; those already supportive of U.S. positions will be most likely to accept information from the United States. Some groups simply will not accept information. If it is important to change their attitudes, more than a direct information approach will be necessary. Determining how to change the positions of those in opposition is more difficult, since these people may interpret the information provided quite differently than intended, according to their prior attitudes.

## Enhancing U.S. Cyber Influence

Enhancing the influence of the United States in cyberspace will require a multifaceted strategy that differentiates the circumstances of the message, the key places of delivery, and the sophistication with which the message is created and delivered, with particular focus on channels and messengers.

A useful starting point is to distinguish among three different analytic circumstances. The first might be called the *general condition* under which the United States will have a great many messages on a great many topics that it is regularly delivering. Those messages are normally delivered by the public affairs functions of the government, as exemplified by the DOS spokesperson’s briefings. Even though the messages are focused on international topics, quite often the intended first recipient of the message is the American public. For example, at a DOS briefing, numerous U.S. media entities will be present, and they will pass on the message to the American public. Of course, international media are also present, and the messages also will be presented internationally—but the message will always be intended to make sense to the American public.

The key conclusion from this analysis is that public affairs messaging, particularly from the United States, is not a place where

tailoring for a non-U.S. audience is easily undertaken. Messages delivered in American English will have a “made in America” tenor. This is not a “bad” result; in fact, it is a “good” result because the American people should have a full understanding of government policy. But it does mean that public affairs undertaken from the United States cannot easily take account of the multiple factors that make international messaging difficult.

Often, in discussions of the effectiveness of U.S. international messaging, there are suggestions that one strategic message should be undertaken top to bottom—so to speak, from

the President to the junior Foreign Service Officer and the Army private. But Presidential addresses on international matters are almost always, first and foremost, statements to the American people. Such statements obviously will be the substantive heart of the international message. But they will not be tailored to the inter-

national audience. For Presidential addresses and for building on public affairs messages in general, additional international messaging will be necessary for, among other things, reaching the uninformed, those who do not already agree with the substance of the message, and those whose prior attitudes will affect how they understand the message; being part of an influence effort to affect the views of those who will not change their minds simply because of exposure; and generating effective communication with key leaders and organizations.

The second circumstance is what might be called the *focused, non-wartime problem*. Some examples of topics are global warming, responding to radical militant Islam, and promoting free trade in Asia. These problems are focused in that they need to be considered. They are non-wartime in the sense that the violent use of force is not ongoing (or at least not as a major factor). The assumption is that, in a war, the impact of combat generally will overwhelm the use of words.

Effective cyber influence in a focused, non-wartime problem requires taking account of numerous considerations and constraints. The complexity of the environment and the numerous messages can be somewhat simplified because of the focus on particular messages. A good first step would be for the United States to create an “international map” of individuals and entities important to influence. Not all the world is critical in the same way on every issue. Not only will the messengers be different, but so will the opposition affected by prior attitudes and/or ignorance whose concurrence with U.S. views will be necessary or valuable.

With this map in hand, a cyber influence campaign can be planned. The next step will be to understand the culture in which influence is sought—how will those who get messages view and respond to them? In thinking through message presentation, some

## **understanding the psychological and marketing issues inherent in influence campaigns is crucial**

questions can be key (and the particular culture may make others important). The following are examples:

- What is the desired effect?
- Should focus be on the individual, or is the group (for example, the family) more the key influence mechanism?
- Will negative messaging work?
- What is the role of religion, and how does that affect messaging?
- What is the meaning of success (for example, is it better for an individual to stand out, or to support another)?
- How do you pretest messages and determine what has been successful?
- Who is the correct messenger? Would a third party be more effective?

Likewise, the interests and nature of key entities must be considered. How does the U.S. message, if adopted, affect the political, social, and economic imperatives of the target audience? Who are the important sources of influence in the society, including key individuals and trusted advisors and influence networks? Galula's point about building on the favorable minority surely must be considered.

None of the foregoing can be undertaken effectively unless experts in the geographic and cultural areas where influence is sought (including some experts with a deep understanding of the language) are heavily involved in the development of the message. Those experts can help build the map and describe the culture and relevant interests, as well as the individuals and entities of influence.

Such domain expertise is necessary but not sufficient for effective cyber influence. Understanding the psychological and marketing issues inherent in influence campaigns is also crucial. The insights of "Some Reasons Why Information Campaigns Fail" are good examples of the psychology behind an influence campaign. Marketing expertise likewise should be understood. These matters, however, raise the crucial factor of intercultural expertise. What is true in the United States in terms of psychology and marketing may not be true in

another culture. It is the rare person who will combine cultural and geopolitical expertise with psychological and marketing expertise. An interdisciplinary team is needed.

The interdisciplinary team also will need a member with a third expertise, namely, in the use of cyber techniques—how to make effective use of radio and TV, what can be accomplished by cell phone messaging, how to use the Internet. In the international context, this type of expertise will necessarily have to be combined with cultural, language, and psychological expertise to be effective. As the team generates its approach, it also will need to consider how cyber and noncyber activities interact.

A final point on the focused, non-wartime message is that the concept of focus deserves much more attention. If everything is equally important, it is very hard to give focus. But, as the discussion of the Embassy Web sites suggests, the United States has made few attempts to focus its messages in the international arena. In fact, that is the point of the GAO study, which stated that U.S. Embassies "did not have a core message or theme to direct their communications efforts." Of the posts reviewed, none had a detailed communications plan.

The DOS Office of Public Diplomacy has recognized the importance of focus and has identified three key themes: support the President's Freedom Agenda with a positive image of hope, isolate and marginalize extremists, and promote understanding regarding shared values and common interests between Americans and peoples of different countries, cultures, and faiths.<sup>39</sup> If these are to be the key themes, it will be important not only for a Washington office to assert them, but also for posts abroad to do so. It is also important to ask *when and where the themes are relevant*. In some situations, the themes, though most important to Washington and presumably to a number of other countries, may not be the best messages for some target countries. The need to decide the key themes, and when and where to implement them, leads to a requirement for a strategic plan. As the GAO study indicates, such plans are required. For the most part, they are not undertaken. That is a crucial failing—and until it is corrected, it is unlikely that U.S. influence cam-

paigns, including cyber influence campaigns, will become more effective.

The last analytic circumstance to be considered is cyber influence in the *wartime situation*, that is, where the use of violence is a major consideration. The ongoing situations in Iraq and Afghanistan are examples, as is the introduction of the military into so-called stability operations (including counterinsurgency, peace enforcement, and peacekeeping).

Military involvement does not mean that influence is not a critical factor. Clausewitz's observation that war is a continuation of

**the three types of expertise—  
geographic and cultural,  
psychological and marketing, and  
cyber technical—necessary for  
effective cyber communications  
need to be organized and  
coordinated with the military**

politics by other means emphasized the importance of the intended political outcome over the particular means employed to achieve it. In a wartime situation, a dominant factor in generating influence will be the use or threat of violence. The impact of the normal influence channels, including cyber influence, will be relatively less because the impact of violence will be so great. However, the generation of cyber influence is still applicable, though more complex. A domain expertise in three arenas—geographic and cultural, psychological and marketing, and cyber technical, including planners and implementers—is still needed. But in addition, the interface with the military must be considered. In this regard, several points deserve consideration.

First, the public affairs efforts of the U.S. Government are going to continue in a wartime situation. Those efforts, first and foremost, will be directed toward providing information to the American public. There is no point in asking for such messages to be focused on the theater of operations because, for the most part, that will not happen.<sup>40</sup> What can happen, however, is for the public affairs personnel to be highly aware of the theater requirements and, at a minimum, communicate and, when possible, coordinate messages. As an example, in the Kosovo campaign undertaken under NATO auspices, both interagency and international communications groups undertook such efforts.

Second, the three types of expertise—geographic and cultural, psychological and marketing, and cyber technical—necessary for effective cyber communications need to be organized and coordinated with the military. To accomplish this, two fundamental shortcomings of the current system must be overcome.

The first shortcoming is that the necessary expertise does not exist in sufficient capacity or at high enough levels in the government. A much greater capacity in both DOS and DOD is necessary. Achieving that level of capacity and expertise can involve a combination of permanent personnel, reserve personnel, and contractors—but the first step is recognizing that we are not even remotely close to the level of expertise we need.

The second shortcoming is that we do not make good use of the capacities we do have. In a wartime situation, the military undertakes to do the best it can in terms of influence operations. A very impressive example is set forth by Colonel Ralph Baker, USA, in his discussion of how he used information operations as one of his “vital tools” to “favorably influence the perceptions of the Iraqi population” in his area of operations.<sup>41</sup> But Baker’s story is one of improvisation, not of a strategic campaign effort. As he says, the “traditional tools in my military kit bag were insufficient to successfully compete” in the influence environment.

## **while neither a cyber nor any other influence campaign can provide magical results, an effective use of cyber capabilities can do much**

Unfortunately, it is not only the lone brigade commander who lacks the tools. DOS generally is not an effective player in influence operations in the theater situation, and DOD does not have adequate theater capacity—or, as Baker makes clear, tactical capability.<sup>42</sup> Contractors have been used, but the results on the whole have not been satisfactory. For example, it is generally agreed that, after the end of major combat operations in Iraq in 2003, it took far too long to generate

a U.S.-supported television capability. Achieving better results will require a more coordinated, effective, interagency approach. Up to now, the United States has not been able to accomplish that, even though it is engaged in several wartime situations.

The final point is that even though violence or the threat of violence has a major influence impact, there is also an extremely important role in influencing target populations as to what the impact of violence should mean to them. As an example, in the Israeli-Hizballah conflict in 2006, both sides mounted intensive influence campaigns designed to show they were winning and that they deserved the support of several audiences—their own people, allies, potential intervening states, sympathetic populations and countries, and the world at large. Whenever war will not be fought to a conclusion of unconditional surrender or destruction (and perhaps even then), the method and consequences of conflict termination will be affected by more than one combatant. Hence, influencing the perceptions and consequent actions of relevant target audiences is of greatest importance to the combatants.

## **Conclusion**

Cyber influence is an ongoing source of power in the international security arena. Although the United States has an enormous cyber information capacity, it has less cyber influence than might be desirable. While neither a cyber nor any other influence campaign can provide magical results, an effective use of cyber capabilities can do much. A considered approach that recognizes the context in which cyber capabilities will be used; understands the principles of making influence campaigns effective; and provides personnel expertise in the technical management of cyber capabilities, in the domains—particularly cultural and geographic—where they will be applied, and in psychological and marketing expertise relevant to the use of cyber capabilities, should be an important component of international security activities for the United States.

In light of the foregoing, the following actions are offered for consideration as possible ways to help make U.S. cyber influence more effective in the international security arena.

First, and perhaps most importantly, greater focus must be placed on the nature of audiences and of the societies and cultures into which cyber-transmitted messages will be delivered. In the first instance, the intended recipients of messages need to be clear. For example, in the context of a counterterror effort, there likely will be a difference among messages to populations at large—those who do not support terrorists, those who are terrorist sympathizers, those who are active supporters of terrorists, and those who are terrorists. Moreover, those varying audiences might well be reached by different types of communications—for example, television for broader audiences and Web sites for potential terrorist recruits. In this context of differentiated messaging, a further important consideration needs to be an understanding of the types of persons who have influence with the message recipients and the types of contexts in which that influence will be most effective.

Second, and implied by the first, it will be necessary to increase the number of experts in geographic and cultural arenas, including a greater expertise in languages. Such expertise can help build a societal/cultural map of influencers, key communications nodes, and cultural communications patterns to guide strategic communications and influence operations. Added to these cultural experts should be experts in psychology and marketing who can help generate messages and ensure that communications are effective. Finally, experts are needed in the use of television, radio, the Internet, and cell phones. In short, an interdisciplinary approach is required.

Third, leaders must realize that while there may be a consistent base message, that message will be presented in multiple theaters. These areas will differ significantly, and one should expect that, to be effective, messaging will likewise differ. To use an example, the society, culture, and influential persons in Indonesia are significantly different from those in Pakistan, and both are significantly different from those in Egypt. It is also worth noting that the Internet has created coherent, nongeographic communities. Numerous studies and reports document the Internet's effectiveness in transmitting messages that sympathize with, give support to, and recruit for terrorist efforts. The Internet must be a focused arena for strategic communications and influence operations.

Fourth, greater resources must be given to the overall strategic communications and influence efforts. For example, expanding the capacities of the Broadcasting Board of Governors, the Embassies, and other outlets of the State Department would be enormously valuable. As noted, the Internet is a key mechanism. DOS runs Web sites, but a broader and more multifaceted Internet strategy—both globally and regionally—would be highly desirable. The GAO has found that while Embassy posts are supposed to

have a strategic communications plan, they are generally ineffective, with little focus and not enough resources.<sup>43</sup> Enhancing U.S. Government capabilities is a critical requirement.

Fifth, long-term communication efforts must be encouraged along with short-term responses. It is possible to change attitudes over time. As an example, consider the American attitude toward smoking, which has changed significantly over the last 30 years. In the battle of ideas, the U.S. Government is seeking a long-term change—and so there is a need to adopt long-term policies. As examples of useful approaches, the DOD Web sites,

Southeast European Times, and Maghrebia mentioned earlier provide news, analysis, and information that are productive, long-term approaches that will not affect attitudes immediately but can have significant consequences over time.

Sixth, the dictum “facts speak louder than words” must be fully appreciated. Some policies generate significant opposition, and strategic communications and influence operations are not panaceas that can overcome all real-world actions. In the earliest planning stages, the communications consequences of actions must be discussed. In conflicts, such as Iraq and Afghanistan, the impact of violent activities will very significantly change the views of the world—not only of those immediately impacted but of those who are indirectly affected and those to whom those impacts are communicated. Every battle commander in these irregular wars soon finds out that the communications battle is critical—because the center of gravity for success is the population. But all too often, our commanders have to learn this on the ground. Especially in this globalized world of instant communications, tactical actions can have strategic consequences. Cyberspace is a creative and cultural commons defined by information, perception, cognition, and belief, and it is becoming the preeminent domain of political victory or defeat. Increased support for training and resources for cyber-enabled communications will be critical elements of effective counterinsurgency and stability operations. As Galula argued, communication—to one's supporters,

**greater focus must be placed on the nature of audiences and of the societies and cultures into which cyber-transmitted messages will be delivered**

Defense Horizons is published by the Center for Technology and National Security Policy. CTNSP publications are available online at <http://www.ndu.edu/ctnsp/publications.html>.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk  
Director

to the population at large, and to the opposition—is of crucial importance. The government needs resources and training for our people on these issues, and these must be undertaken not only by DOD, but also in a joint DOD-State context.

Seventh, the U.S. Government should not expect to be successful at strategic communications and influence operations acting solely on its own. Rather, it should use an alliance and partnership approach, both to expand capacities and increase effectiveness. In the business world, it would be the rare American company that would seek to enter another country without the guidance and support of local business, whether as partners, joint ventures, or advisors—and often all three. In military and diplomatic arenas, our allies and partners are recognized as enormous sources of strength. In the strategic communications and influence operations arena, we need to develop those alliances and partnerships, both to shape our own messages and support theirs.

## Notes

<sup>1</sup> University of California Berkeley, *How Much Information? 2003*, Executive Summary, available at <<http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm>>.

<sup>2</sup> Pew Global Attitudes Project, available at <<http://pewglobal.org/reports/display.php?ReportID=252>>.

<sup>3</sup> BBC, World Service Poll, available at <<http://news.bbc.co.uk/2/hi/americas/6288933.stm>>.

<sup>4</sup> Daniel Kuehl, "Cyberspace—Cyberpower—Cyberstrategy: Their Influence on (Future) History," National Defense University Center for Technology and National Security Policy (forthcoming).

<sup>5</sup> The proliferation of channels in some areas has allowed for greater market segmentation and somewhat less "mass" mass marketing.

<sup>6</sup> Wiki is server software that allows users to freely create and edit Web page content using any Web browser. Wiki supports hyperlinks and has simple text syntax for creating new pages and crosslinks between internal pages on the fly.

<sup>7</sup> Michael Pfau and Roxanne Parrott, *Persuasive Communication Campaigns* (Boston: Allyn and Bacon, 1993).

<sup>8</sup> Two exabytes equals the total volume of information generated in 1999; 5 exabytes equals all words ever spoken by human beings. *How Much Information? 2003*, table 1.1.

<sup>9</sup> *Ibid.*, Summary of Findings I.1.

<sup>10</sup> *Ibid.*: "It would take about 30 feet of books to store the equivalent of 800 MB of information on paper."

<sup>11</sup> Ferris Research, available at <<http://www.ferris.com/research-library/industry-statistics>>.

<sup>12</sup> *The World Fact Book* (Washington, DC: Central Intelligence Agency, 2007), available at <<https://www.cia.gov/cia/publications/factbook/geos/xx.html>>.

<sup>13</sup> Internet World Stats, accessed at <<http://www.internetworldstats.com/stats.htm>>.

<sup>14</sup> *Ibid.*

<sup>15</sup> Technorati, accessed at <<http://www.sifry.com/alerts/archives/000436.html>>.

<sup>16</sup> *Information superiority* is "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." *DOD Dictionary*

*of Military and Associated Terms*, April 12, 2001, as amended through April 14, 2006, available at <<http://www.dtic.mil/doctrine/jel/doddict/data/i/02656.html>>. See generally, Martin Libicki, "Information Dominance," *Strategic Forum* 132 (Washington, DC: National Defense University Press, November 1997), available at <<http://www.ndu.edu/inss/strforum/SF132/forum132.html>>.

<sup>17</sup> *Persuasive Communication Campaigns*, 53.

<sup>18</sup> See generally Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston: Back Bay Books, 2002).

<sup>19</sup> *Persuasive Communication Campaigns*, 54.

<sup>20</sup> David Galula, *Counterinsurgency Warfare: Theory and Practice* (London: Praeger, 1964), 14, 104.

<sup>21</sup> Quoted in Thomas Ricks, *Fiasco: The American Military Adventure in Iraq* (New York: Penguin Press, 2006), 326.

<sup>22</sup> Malcolm Gladwell describes different types of influential messengers based on the category of what they are doing: *mavens*, who validate the message; *connectors*, who link dif-

ferent parties and groups; and *salesmen*, who are effective at marketing. All of these may play roles in the international influence arena.

<sup>23</sup> *Counterinsurgency Warfare*, 75–77.

<sup>24</sup> Gladwell, 219: "Simply by finding and reaching those few special people who hold so much social power, we can shape the course of social epidemics." Local assistance can help in both pretesting messages and assessing their impact.

<sup>25</sup> The BBG was created by the 1998 Foreign Affairs Reform and Restructuring Act (Public Law 105-277).

<sup>26</sup> BBG Online, available at <[http://www.bbg.gov/bbg\\_aboutus.cfm](http://www.bbg.gov/bbg_aboutus.cfm)>.

<sup>27</sup> *Ibid.*

<sup>28</sup> Joint Publication 3–13, *Information Operations* (Washington, DC: Office of the Joint Chiefs of Staff, February 13, 2006), GL–9.

<sup>29</sup> *Ibid.*, 1–9.

<sup>30</sup> Partnership for Peace Information Management System, available at <<http://www.pims.org>>.

<sup>31</sup> Asia-Pacific Area Network, available at <<http://www1.apan-info.net/About/tabid/54/Default.aspx>>.

<sup>32</sup> *Ibid.* The home page lists several exercises supported by the Asia-Pacific Area Network.

<sup>33</sup> Southeast European Times averages 5 million hits a month, with average visits exceeding 20 minutes. Charles F. Wald, "The Phase Zero Campaign," *Joint Force Quarterly* 43 (4<sup>th</sup> Quarter 2006), 72.

<sup>34</sup> Jesse T. Ford, Director, International Affairs and Trade, "U.S. Public Diplomacy, State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges," testimony before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, House Committee on Appropriations, GAO-06-707T (Washington, DC: U.S. Government Accountability Office, May 2006), 21; available at <<http://www.gao.gov/new.items/d06535.pdf>>.

<sup>35</sup> *Ibid.*, 20, 21, 24, 26.

<sup>36</sup> Herbert H. Hyman and Paul B. Sheatsley, "Some Reasons Why Information Campaigns Fail," *The Public Opinion Quarterly* 11, no. 3 (Autumn 1947), 412–423.

<sup>37</sup> *Ibid.*, 417.

<sup>38</sup> *Ibid.*

<sup>39</sup> Ford, 27.

<sup>40</sup> Public affairs activities at the local and regional level, for example, at Embassies, that can be focused on the theater of operations.

<sup>41</sup> Ralph Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006), 13.

<sup>42</sup> In a forthcoming companion piece to this article, Stuart Starr discusses how tactical influence operations might be improved.

<sup>43</sup> Ford, 20.

## **Other recent titles from NDU Press**

### **After the Surge: Next Steps in Iraq?**

*Judith S. Yaphe*

(Strategic Forum No. 230, February 2008)

### **Organizing for National Security: Unification or Coordination?**

*James M. Keagle and Adrian R. Martin*

(Center for Technology and National Security Policy, Defense Horizons 60,  
January 2008)

### **Strategic Fragility: Infrastructure Protection and National Security in the Information Age**

*Robert A. Miller and Irving Lachow*

(Center for Technology and National Security Policy, Defense Horizons 59,  
January 2008)

### **The European Union: Measuring Counterterrorism Cooperation**

*David T. Armitage, Jr.*

(Strategic Forum No. 229, November 2007)

### **Trans-American Security: What's Missing?**

*Luigi R. Einaudi*

(Strategic Forum No. 228, September 2007)

### **The Country Team: Restructuring America's First Line of Engagement**

*Robert B. Oakley and Michael Casey, Jr.*

(Strategic Forum No. 227, September 2007)

### **The Comprehensive Approach Initiative: Future Options for NATO**

*Friis Arne Petersen and Hans Binnendijk*

(Center for Technology and National Security Policy, Defense Horizons 58,  
September 2007)

### **Privatizing While Transforming**

*Marion E. "Spike" Bowman*

(Center for Technology and National Security Policy, Defense Horizons 57,  
July 2007)

### **China's ASAT Test: Motivations and Implications**

*Phillip C. Saunders and Charles D. Lutes*

(INSS Special Report, June 2007)

### **Responding in the Homeland: A Snapshot of NATO's Readiness for CBRN Attacks**

*Michael Moodie and Robert E. Armstrong with  
Tyler Merkeley*

(Center for Technology and National Security Policy, Defense Horizons 56,  
June 2007)

### **Counterintelligence and National Strategy**

*Michelle Van Cleave*

(School for National Security Executive Education Report, April 2007)

### **Sino-Japanese Rivalry: Implications for U.S. Policy**

(INSS Special Report, April 2007)

### **Preventing Balkan Conflict: The Role of Euroatlantic Institutions**

*Jeffrey Simon*

(Strategic Forum No. 226, April 2007)

For on-line access to **NDU Press** publications, go to: [ndupress.ndu.edu](http://ndupress.ndu.edu)

# **Information and Communication Technologies for Reconstruction and Development**

## **Afghanistan Challenges and Opportunities**

Larry Wentz, Frank Kramer, and Stuart Starr

**Center for Technology and National Security Policy  
National Defense University**

**January 2008**

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

---

**Larry Wentz** is a Senior Research Fellow at the Center for Technology and National Security Policy (CTNSP), National Defense University, where he consults on command and control issues. He is the author of *Lessons from Bosnia: The IFOR Experience* and *Lessons from Kosovo: The KFOR Experience*.

**Franklin D. Kramer** is a Distinguished Research Fellow at CTNSP. Mr. Kramer was Assistant Secretary of Defense for International Security Affairs from March 1996 to February 2001.

**Stuart H. Starr** is a Distinguished Research Fellow at CTNSP and President, Barcroft Research Institute, where he consults on command and control issues.

### **Acknowledgements**

A number of persons have been important to the research in this report, but special thanks goes to James Craft, the first Senior Telecom Advisor (STA) at the Afghanistan Reconstruction Group (ARG) U.S. Embassy Kabul and sponsor of the April-May 2006 trip to Afghanistan to collect the insights needed for the research on this paper, and to Ed Smith, ARG Chief of Staff, for his support of the activity. Jim's insights, guidance, and support were a key to the success of the research effort. James Baker, the current STA, has continued to support our research effort. Others in Afghanistan and the United States who made important contributions to the research effort were: Spanky Kirsch, ASD NII (now at DHS); Bob Kinn, ASD NII; Capt Joe Verastegui, USA, at CFC-A CJ9; Capt Will Brown, USA; LTC Aaron Johnson, USA; LT Chris Simpson, USN; LT Don Beish, USN at CFC-A CJ6; Michelle Parker, USAID Jalalabad PRT/ISAF DA (USAID); Lane Smith, USAID Kabul; Alane Regualos, USAID Khost PRT; Cmdr John Wade, USN, Khost PRT Commander; Oliver Dziggel and Tony Loda, BearingPoint Kabul; and Tom O'Neil and Greg Romano, Globecomm System Inc. The support of Minister Sangin and Aimal Marjan of the Afghanistan Ministry of Communications and Mr. Bhat, Afghan Telecom, was also most appreciated.

Defense & Technology Papers are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at <http://www.ndu.edu/ctnsp/publications.html>.

## Contents

Introduction.....	1
ICT as a Sector and Cross-sector Enabler.....	4
Afghanistan.....	7
The Country .....	7
Governance .....	7
Culture and Diversity.....	8
Security and the Battle of Confidence .....	8
ICT and the Challenges of Recovery .....	10
ICT Governance and the Road to Recovery .....	11
ICT—Putting the Pieces Together .....	14
Private-Sector GSM Networks and Services .....	15
Private Internet Cafes and ISPs.....	17
Public Fixed Line and Wireless Local Loop Services .....	18
Afghan Telecom Network and Services .....	19
Public and Private-Sector Transmission Networks.....	23
ICT Support to Cross-Sector Reconstruction .....	24
ICT Capacity Building.....	26
Cyber Security and Electric Power Challenges .....	27
A Continuing Success Story .....	28
Community Radio.....	30
Coordination and Information Sharing.....	31
Other Reconstruction Challenges .....	36
ICT-Related Lessons from Afghanistan .....	39
The Way Ahead .....	41
Conclusion .....	48
References.....	49



# Introduction

---

The term *information and communication technologies* (ICTs) encompasses the range of technologies for gathering, storing, retrieving, processing, analyzing, and transmitting information that are essential to prospering in a globalized economy. Advances in ICTs have reduced the costs of managing information and introduced innovations in products, processes, and organizational structures that, in turn, have generated new ways of working, market development, and livelihood practices.

Internationally, ICTs are viewed as a basic enabler of informal social and economic discourse, leading to a strengthening of civil society and the promotion of economic activity. The importance the United Nations (UN) attaches to ICTs as enablers of economic, governance, security, education, healthcare, and social well-being reconstruction and development is evident in sponsorship of two international summits, the 2003 and 2005 World Summit on the Information Society (WSIS). These summits documented steps on how to establish and organize the Information Society, and their reports referenced the importance of ICT by frequently citing the phrase, “ICTs as a tool for social and economic development.”<sup>1</sup>

While there is little doubt that ICTs are an engine for social and economic development, quantifying their impact is difficult. Evidence remains largely anecdotal, and the link between ICT deployment and reconstruction and development remains vague. The National Defense University (NDU) Center for Technology and National Security Policy (CTNSP) recently completed a study, known as the I-Power study, which looked at using information and ICTs to achieve success in stability and reconstruction (S&R) operations. The study results suggest that the strategic use of information and ICTs can increase significantly the likelihood of success in affected-nation, cross-sector reconstruction and development—if they are engaged at the outset as part of an overall strategy that coordinates the actions of outside interveners and focuses on generating effective results for the affected nation. This has certainly been the pattern in business, government, and social arenas in the Western world, where the information revolution has been a dynamic and positive factor. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities throughout the world.

Experiences from recent U.S. government (USG) and coalition interventions in the Balkans, Afghanistan, and Iraq repeatedly have demonstrated that ICT activities supporting stabilization, reconstruction, and development operations in an affected nation can be problematic. These activities suffer from a lack of adequate understanding of the affected-nation information culture and ICT business culture. There is no clear mapping of responding stakeholder organizations roles and responsibilities. Program development, project coordination, information sharing, and ICT implementation are largely uncoordinated and non-standard. No agreed architecture or plan is in place for affected-nation ICT reconstruction.

---

<sup>1</sup> Information on both summits is available at <<http://www.worldsummit2003.org/>>.

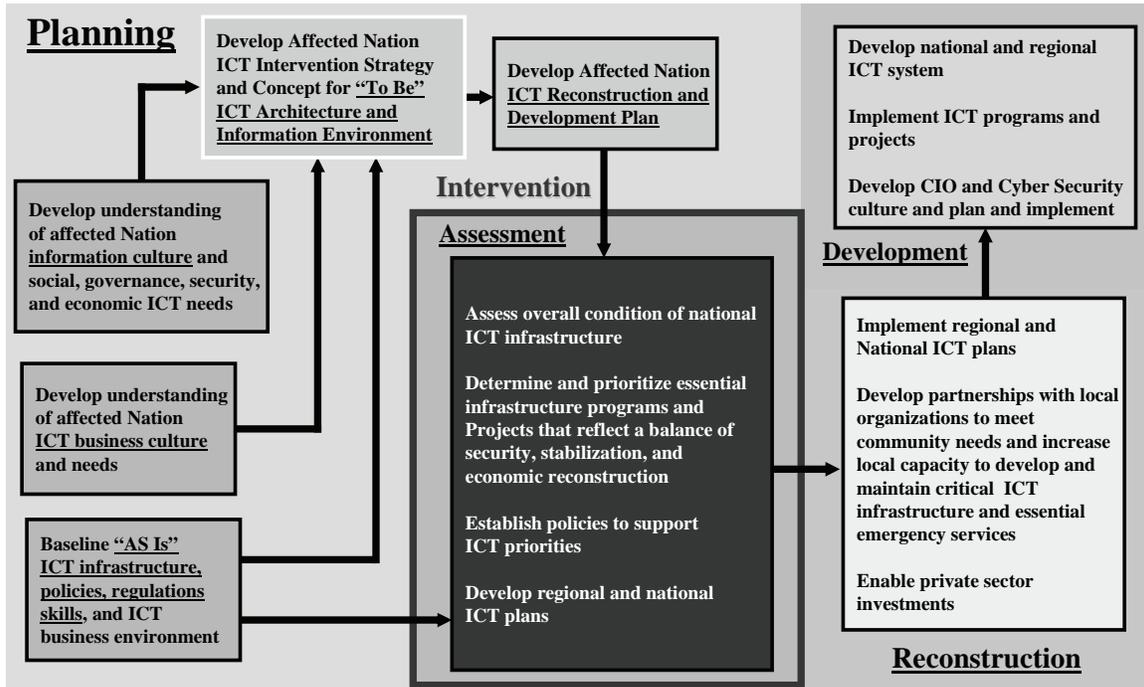
A coherent civil-military ICT strategy and plan for intervening coalition military forces, responding-nation civilian elements, international organizations (IOs), and non-governmental organizations (NGOs) is also lacking. No agreed mechanisms or procedures are in place to enable effective civil-military coordination and information sharing among participants and with the affected nation. Interveners consistently do not view ICT as a reconstruction and development priority equal to roads, power, and water or as an enabler of cross-sector reconstruction and development. Consequently, senior leadership has no framework to make investment decisions and track ICT-related reconstruction and development progress.

The situation on the ground also complicates the challenges of failed-state interventions in all regards, including ICT. Civil and military responders usually encounter spoilers interfering with the intervening forces; refugees and internally displaced persons (IDPs) requiring humanitarian assistance; buildings requiring reconstruction; roads, power, water, telecommunications, healthcare, and education systems disrupted or dysfunctional; absence of a functioning government as well as laws, regulations, and enforcement mechanisms; widespread unemployment and poverty; and a shortage of leaders, managers, administrators, and technical personnel with 21<sup>st</sup>-century information and ICT management, operations, and technical skills.

An ICT business model along the lines of the one depicted in figure 1, coupled with the smart use of information and ICT, could be employed to help create a knowledgeable intervention; facilitate appropriate integration of intervener ICT reconstruction and development initiatives with the affected-nation ICT strategy and plans; organize complex activities; and enable coordination, information sharing, and implementation activities among interveners and with the affected nation, making the latter more effective. Additionally, ICT can be used to link constituent parts of an integrated multinational reconstruction and capacity-building effort; help multiple sectors, such as, security, governance, education, health, agriculture, finance, and commerce simultaneously; and enhance situational awareness (SA) of cross-sector reconstruction and development activities.

Real world experience suggests that ICT can be (and is being) used to generate social, economic, cultural, and political changes, but, as noted earlier, it is difficult to quantify the impact of ICT initiatives and separate the influence of ICT from that of other factors, such as civil security stability, governance, or economic growth. Furthermore, internationally agreed indicators to measure and compare country experiences are lacking. Some countries are certainly doing much better in exploiting ICTs and adopting more effective ICT policies and strategies than others, but there is no agreed and uniform way to measure and compare. Although a growing body of anecdotal evidence suggests that ICTs have a real macro-economic impact, it is not clear to what extent ICTs have helped to directly reduce major reconstruction and development concerns, particularly those of the UN Millennium Development Goals, such as poverty, hunger, and sickness. Much work remains to be done to measure and comparatively assess the effectiveness of ICT as an enabler of cross-sector reconstruction and development.

**Figure 1. ICT Business Model**



The intent of this report is to raise awareness of the importance of the role of ICT in failed state intervention and follow-on reconstruction and development. Afghanistan is used as a case study to examine and highlight, by example, successes and some of the challenges encountered in trying to rebuild a war-torn country’s telecommunications and IT infrastructure and to use it to enable other sector reconstruction and development.

A discussion of ICT as a sector and enabler of cross-sector reconstruction and development is introduced to set the context for a discussion of Afghanistan experiences. An overview of Afghanistan the country and the ICT environment follows to help the reader better understand and appreciate the initial conditions and related cultural, infrastructure, skill base, and implementation challenges. Some of the related coordination and information sharing challenges encountered by the multinational civilian and military participants are discussed, along with approaches used to address these challenges. Finally, a snapshot of the public and private ICT infrastructure is presented as well as some examples of ICT use in the education and healthcare sectors.

Afghanistan ICT has truly been a success story emerging from a country left dysfunctional after 23 years of war. ICT lessons derived from this success are highlighted, as are some thoughts on making more effective use of the ICT infrastructure in the future. Findings and observations of successes and challenges are based on visits by one of the authors to Afghanistan in April and May 2006 to research the rebuilding of Afghanistan telecommunications and IT and their use as enablers of cross-sector reconstruction and development.

## **ICT as a Sector and Cross-sector Enabler**

---

ICT can be a powerful enabler of reconstruction and development goals. It is both a sector and an enabler of cross-sector reconstruction and development. As a sector, ICT supports national capacity building and export market focus and plays a critical role in reestablishing basic economic linkages by relieving communication bottlenecks from financial, governmental, and cultural information flows. As an enabler, it supports global positioning focus and adoption of cross-sector strategies that can be used to harness the uniqueness of ICT to accelerate a wider reconstruction and development process. It is also an essential enabler for boosting productivity by helping to establish a climate for job creation, investment, and sustainable growth. The real benefits lie not in the provision of technology per se, but rather in promoting creation of powerful social and economic networks by dramatically improving communications and the exchange of information.

ICT is pervasive and cross-cutting, can be applied to a full range of activities from personal use to business and government, and is multifunctional and flexible, allowing for tailored solutions to meet diverse needs. Using ICT, governments can improve the quality and responsiveness of their organizations as well as the services they provide to citizens by expanding reach and accessibility of services—and thereby enhancing government legitimacy. This can be facilitated through the use of e-government applications that provide government services and information to citizens over the Internet and other communication networks. E-government also can be used to help reduce corruption and enhance transparency in governance and thus offers an opportunity to positively influence attitudes of the leadership and general population.

ICT connects individuals, local communities, and businesses with information and resources beyond their geographic boundaries, encouraging information dissemination and exchange as well as communication. In developing nations, where it may take hours of travel to have face-to-face meetings between local and regional leaders, ICT can enable communications between and among such leaders in a matter of minutes. Additionally, in hostile environments where personal security is a concern, ICT can be used to connect leaders and other personnel without necessitating their travel through high-threat areas. Local communities can gain access to outside information sources, which often can alleviate the effects of insurgent propaganda and increase mutual understanding in the local community.

ICT contributes to a market economy by making it possible for users to acquire products and services directly from the original provider, reducing the need for intermediaries. By generating opportunities for employment, ICT can contribute to poverty reduction. Through the creation and expansion of networks, ICT can transcend cultural and linguistic barriers by providing individuals and groups the ability to live and work anywhere, allowing local communities to become part of the global network economy without regard to nationality, and challenging current policy, legal, and regulatory structures within and between nations.

ICT can facilitate the improvement of healthcare delivery by allowing access to remote consultation and diagnosis, medical databases and libraries, epidemic alerts, and treatment. Medical facilities can streamline processes and automate patient record systems. ICT also can improve the efficiency, accessibility, and quality of the learning process. Distance learning can be employed for higher level education as well as technical and vocational training, while primary and secondary education can access educational material, collaborate, and explore interactive learning techniques. Alliances can be formed between learning institutions within the affected nations as well as with off-shore institutions to facilitate capacity building.

Through its many roles, ICT extends the influence of the central government and can serve to revolutionize economic and social development, especially in rural areas. In rural areas it can be used to provide local access to government services; increase the visibility of government; spawn local entrepreneurs; help business owners identify market opportunities and find reliable and safe ways to transport goods and services; provide means for electronic funds transfer or other mobile commerce using cell phones and Internet banking; provide remote access to health services and information; and facilitate distance learning as well as other educational opportunities.

ICT is being used today in many developing countries to enable governance and security and to revolutionize economic and social development in urban and rural areas. Innovative implementation of ICT capabilities has done wonders for the poor around the world by creating new jobs and new ways of reducing the cost of doing business. Mobile phones (GSM, CDMA, GMPCS), data (EVDO, GPRS, Internet), satellite access (VSAT, INMARSAT RBGAN, and BGAN terminals), wireless networking (WiFi and WiMax), Public Call Offices (individuals selling cellular voice calling and Internet access service), and Internet Cafés and Telekiosks (voice and Internet access) are all used to provide instant communications in urban and rural areas. Such communication enables access to market, education, and healthcare information and also provides greater contact and improved relationships among families within a country and abroad. In rural areas, ICT such as cell phones, can be used to help the population communicate, gain access to information and advice and find job opportunities. ICT can be used to train and educate through the use of graphics and pictures combined with soundtracks or video on laptops.

Prime examples of the innovative use of ICT can be found in India, Africa, Bangladesh, Cambodia, Peru, and other parts of the world where cell phones, wireless ICT, and access to the Internet have become some of the best tools for poverty reduction and economic recovery. ICT benefits not only the rich but those who are less fortunate. For example, at the village level in rural areas, beneficiaries can be local entrepreneurs who make money selling phone services to villagers on a per-call basis; poor youth or small business owners selling pre-paid phone cards; and Internet cafe owners who offer Internet access service. Cell phones can be used creatively to gain market advantages and provide business and employment opportunities. Businesses can use cell phones to gain access to information about their domains of interest and reach subject matter experts for advice and counseling.

However, the poor cannot benefit from globalization without active involvement from the public and private sectors and without access to products and services that represent global standards. The rural area provides new growth opportunities for the private ICT sector and a forum for innovation. The global ICT industry has been addressing the more sophisticated market for some time, but recently has discovered a new market—the world’s poor—and has risen to the challenges of lack of power, poor telecom coverage, dusty environments, and low literacy to innovate and provide easy-to-use, low-cost, and energy-efficient ICT options with features focused on rural area needs. Industry innovations include ultra-low-cost cell phones and longer-life batteries, bicycle-powered chargers, dustproof keypads, and booster antennas for areas with poor coverage; solar-powered WiFi wireless networking; easy-to-use, low-cost and energy-efficient laptops, voice over internet protocol (VoIP) for use on wireless networks, portable and fixed satellite access arrangements, cell phone access to Internet, and cell phones with built-in FM radios.

The providers of service in rural areas also have been extremely creative. In India, the wireless pony express of Daknet (a rural internet service provider) uses thousands of buses equipped with WiFi transceivers to pick up and deliver email wirelessly from village kiosks, providing the equivalent of a store-and-forward email service. Young men on bicycles carry mobile phones and go village to village selling calling service to the locals. In Afghanistan, government-run telekiosks and public call offices run by ex-soldiers and women as well as private Internet cafes with remote satellite access are used to sell both voice and Internet services to the local population. Discussions also are underway about micro-financing establishment of local community towers as a way to attract private cellular providers to put antennas on the towers, thereby extending cell service to rural areas. This creates both direct and indirect job opportunities and local income through leasing space on the towers and selling calling service and related cellular phone support services to locals. Local community and warlord buy-in adds an element of physical security protection for the cellular providers. In Cambodia, the “Motoman” project uses WiFi equipped motorcycles and a satellite connection to deliver emails to remote villages. Affordable, solar-powered, easy-to-install ICT systems for building Internet and telecommunications networks in rural areas with little or no access to electricity or affordable communications infrastructure are now available as off-the-shelf, prepackaged products.

Extending voice and Internet services to the rural areas is not a technology issue. Technology is an enabler. The challenges are assessment of rural community needs and constraints of the environment; development of a strategy and plans for providing service; identification of an appropriate portfolio of ICT capability packages to employ; and finding the funding to invest in public-sector initiatives and enable local entrepreneurs while providing incentives to the private sector to extend needed ICT services to rural areas.

# Afghanistan

---

## The Country

The Islamic Republic of Afghanistan encompasses approximately 652,000 square kilometers and is slightly smaller than the state of Texas. It is a landlocked plateau between Iran and Pakistan that also shares borders with China, Tajikistan, Turkmenistan, and Uzbekistan. High mountains, which are part of the Hindu Kush system, cover much of the country and small glaciers and year-round snowfields are common.

Afghanistan is one of the world's poorest and least developed nations. Because of years of fighting, roads, power, water, telecommunications, healthcare, and education have been disrupted or are dysfunctional. One in five children dies before the age of 5, mostly of preventable diseases. Life expectancy is about 42 years for males and 43 for females. The literacy rate is 36 percent in urban areas (51 percent for males and 21 percent for females) and even lower in rural areas. About 32 percent of the children are in school, but only 3 percent of girls attend school. Many schools for girls have been burned, and teachers and families of the girls going to school have been threatened or even murdered by insurgents.

Until recently, the country lacked a functioning government as well as laws, regulations, and enforcement mechanisms. Poverty and unemployment remain widespread; currently about 40 percent of the population is unemployed. The lack of skilled workers and administrators is also a pressing problem for labor. The Afghan economy largely depends on growing poppies and producing illicit drugs. Ninety percent of the world's opium is derived from Afghanistan, which has raised concerns that the country is in danger of becoming a full fledged narco-state. A growing insurgency is fueled by the booming drug economy.

## Governance

Administratively, Afghanistan is divided into 34 provinces, which are further divided into 365 districts. Kabul, the capital, is located in east central Afghanistan at an elevation of about 5,900 feet. The major economic centers are Kabul, Herat, Kandahar, Jalalabad, Khost, Mazar-e-Sharif, and Kunduz. The population of the country is around 30 million (16 million females/14 million males), and 45 percent are under the age of 15 years. About 22 percent live in urban areas—more than 3 million live in Kabul alone.

Afghanistan is governed under a constitution that went into effect in 2004, but warlords continue to use militias to control their areas. President Hamid Karzai was elected in October 2004. The current parliament was elected in 2005. Among the elected officials are former Mujahadeen, Taliban, communists, reformists, and Islamic fundamentalists. Some of the early provincial governors were former warlords. Corruption and organized crime exist at all levels of society, including government elements and ministerial level involvement in the illegal narcotics trade. The constitution established an independent judiciary, but no laws may be passed that are contrary to Islamic law (Shari'a). Law is

administered on an intermittent basis according to a mixture of codified law, Shari'a, and local customs.

Although the Afghan National Police (ANP) are responsible for maintaining civil order, they are viewed by the average Afghan in many areas as a source of danger rather than security—they have been accused of improper treatment of the local population and have been ineffective in controlling crime. Interestingly, however, many Afghans in high-threat areas feel police presence does provide some degree of security protection. The emerging Afghan National Army (ANA), on the other hand, is widely considered a success as a multi-ethnic national institution with its young recruits, good training, and modern equipment. Outside Kabul, local and regional military commanders continue to exercise control. Often the military needs to respond to an incident because police are unable, largely due to lack of training and equipment.

Following the removal of the Taliban, international intervention and investments in Afghanistan have been substantial. However, 75 percent of reconstruction and development spending has been outside the Government of Afghanistan (GOA) channels without formal, centralized oversight. Seventy percent of spending has been in Kabul, where only 10 percent of the population lives. This has significantly impacted the ability of the GOA to establish legitimacy outside of Kabul.

### **Culture and Diversity**

Afghanistan is still largely a tribal culture with a variety of social ills, such as poverty, interethnic strife, inequality of women, and widespread thievery, kidnapping, and banditry. Afghan women still rank among the worst off in the world; most are illiterate, many have no access to healthcare, and child and forced marriages are common.

Extremely close bonds exist within the family, which consists of the members of several generations. The oldest man or patriarch is the head of the family, and his word is law for the whole family. Family honor, pride, and respect toward other family members are highly prized qualities. Twenty-five percent of primary school-aged children work to support the family.

Afghanistan has long been known as the crossroads of Asia, and this is reflected in the country's linguistic and ethnic diversity. The official languages are Dari (50 percent) and Pashto (35 percent), but other spoken languages, such as Uzbek and Turkmen, are considered official in the areas in which they are primarily spoken. Religion is the strongest common bond with the majority of the population being Muslim—84 percent are Sunni and 15 percent Shia Muslim.

### **Security and the Battle of Confidence**

The security situation in 2007 is tenuous and will likely impact the ability to conduct reconstruction and development, particularly in the southern, southeastern, and eastern regions. During the winter of 2006, the UN World Food Program reported the security situation remained relatively tense. In March 2007, the situation deteriorated significantly, with major and frequent incidents of improvised explosive device (IED)

attacks, suicide bombings, rockets, mine explosions, and riots. Violence in Afghanistan has been on the rise; in 2006 it was four times more intense than it was in 2005. Suicide attacks jumped from 27 in 2005 to 139 in 2006, and the use of IEDs doubled. International aid and reconstruction workers have been targeted, setting back reconstruction and development efforts in the hostile areas. The traditionally secure areas in the north and west also have been affected. Even Kabul started experiencing IEDs. In September 2006, just 50 yards from the landmark Massood Square that borders the main gate to the U.S. Embassy compound, a vehicle was detonated next to a U.S. military convoy, killing 16 people, including two U.S. Army reservists, and wounding 29 others.

No major attacks have targeted the ICT infrastructure, probably because the insurgents use it, too. There have been a few isolated incidents, such as the Taliban news announcement in May 2007 threatening attacks on the private cell phone provider Roshan if they did not stop dealing with U.S. and coalition forces. So far nothing has happened. Some criminal elements target ICT equipment to steal, especially at isolated, remote sites. For these reasons alone, ICT facilities are protected 24x7, using both fencing and hired armed guards. Private-sector estimates show that security costs are on the order of 10–20 percent of the cost of doing business. ICT contractors have had staff kidnapped and murdered, and informal reports suggest that government ICT staff manning Afghan Telecom facilities have been threatened. The security threats are a significant deterrent for contractors, consultants, government workers, and related reconstruction and development activities, especially in the provinces along the Pakistan border where ICT reconstruction largely came to a halt at the end of 2006. Additionally, it has been reported by ICT contractors working in the high-threat areas that they are finding it increasingly difficult to get Afghans not only to work for them openly but to work for them on more than one job. Hiring Afghan workers is becoming a one-shot deal in many areas.

Although progress has been made, some 6 years after the fall of the Taliban, many of those assessing and working Afghanistan reconstruction and development are beginning to perceive that the USG, the international community, and the Karzai government may be losing the "battle of confidence" among the Afghan people. Factors influencing these perceptions include the precipitous increase in Iraqi-like suicide bombings (a doubling over the last year), the unprecedented rise in hostility toward Westerners (many Afghans believe Westerners are afraid of them because Westerners do not go out of the protected compounds to meet freely with them), and the rising number of Afghans who are "on the fence" on the question of whether to support the government or the Taliban (recent military actions against the Taliban have resulted in the unfortunate killing of innocent civilians, which does not help win hearts and minds). With the window of opportunity to change direction (return to being viewed as a liberator and enabler of change rather than occupier) rapidly shrinking, the United States and the international community need to take dramatic steps to spur the delivery of governance, security, economic growth, healthcare, education, and social wellbeing services to stabilize Afghanistan. The general feeling is that only by injecting the country with much-needed resources and building local Afghan capacity can the United States and the international community help the government in Kabul establish its legitimacy and win back support from the Afghan people.

## **ICT and the Challenges of Recovery**

After 23 years of conflict, under-investment, and neglect, the ICT infrastructure was left in disrepair with no national or international connectivity. Pakistan country codes were used in many border areas, and Afghans had to travel to neighboring countries to make and receive phone calls. Because music, TV, and Internet had been forbidden by the Taliban, these capabilities were largely non-existent.

ICT culture and skills had evaporated—most of the population with the needed skills left the country during the war years. Hence, there was (and still is) a serious shortage of Afghan leaders, managers, administrators, and technical personnel with 21<sup>st</sup> century, IT-oriented business and technical skills in the civil service, the private sector, and higher education institutions. Key skill areas of concern include business management and practices, project management, telecom and IT, and English language. In regard to English, most software applications and use of IT systems, including the Internet, requires some working knowledge of the English language.

Following the fall of the Taliban at the end of 2001 and the absence of any public and/or private national telecom sector operators, the Ministry of Communications [in March 2007, the MoC was renamed the Ministry of Communications and Information Technology (MCIT)] took over operation of what was left of a limited and outdated, analogue, fixed-line ICT infrastructure with fewer than 40,000 telephone lines for a population of more than 25 million. About 60 percent of the active lines were provided by a few fixed switching exchanges in Kabul with the rest in the cities of Herat, Mazar e Sharif, Kunduz, and Jalalabad. These exchanges were not interconnected and the service was unreliable. In April 2002, Afghan Wireless Communication Company (AWCC), who operated a limited ICT network during the Taliban era, began operation of a stand-alone Global System for Mobile Communications (GSM)—a digital cellular phone technology based on time division multiple access techniques—that provided communications capability to about 11,000 cellular subscribers largely in the Kabul area, plus some limited coverage in Herat and Mazar e Sharif. Coverage and quality of service were marginal, but the network was a start, and it allowed limited telecom access to the outside world.

Due to damage to the backbone satellite, microwave, and cable networks, Afghanistan did not have a functioning long distance network to support national or international service. The MCIT made early efforts to restore some long distance connectivity and establish international access. For example, a few Very Small Aperture Terminal (VSAT) satellite links were planned to connect the legacy switching exchanges in Kabul with those in other cities. Limited international access was available using the international gateway owned by AWCC, which employed a satellite link to route international calls through Guam. Direct inbound calls to Afghanistan were routed internationally using the +93 country code. International and some in-country, long distance calls could be made using satellite phones, such as Thuraya, Globalstar, Iridium, and International Maritime Satellite (INMARSAT). A number of UN agencies and NGOs provided VSAT sites that supported humanitarian assistance activities during the Taliban era and continued to operate after the fall of the Taliban. Many are still operating today. These facilities

provided basic voice and Internet access through their own IT systems and international satellite gateways. Public calling and Internet access were almost non-existent during the Taliban era. After the fall of the Taliban, the MCIT initially contracted with private companies to provide some limited Internet services for selected government agencies.

### **ICT Governance and the Road to Recovery**

The Afghanistan transitional government established in December 2001 recognized that ICT would be critical to the success of the planned national elections and to facilitating communications among the central government and regional authorities. ICT was also recognized as important to the collection of taxes and customs duties, establishing a national banking system, and enabling other political, security, governance, judicial, social, and economic recovery actions.

The transitional government moved reasonably quickly to initiate the actions necessary to put a telecom and Internet policy and ICT strategy and plan in place to enable Afghanistan to become part of the global information society. In June 2002, the Afghan transitional government appointed a new Minister of Communications and designated the MCIT to have the leadership role to enact policies to create an environment conducive to private-sector investment. In October 2002, the Minister of Communications published a national telecommunications development strategy that outlined key ICT infrastructure development initiatives and set the conditions for developing an Afghanistan Telecommunications and Internet Policy.

In October 2003, the Telecommunications and Internet Policy was approved. The policy encouraged private investment through the introduction of measured competition; established Afghan Telecom as a state-owned corporation to operate the public ICT network with the right to accept private investment; and supported rapid expansion of telecom and Internet services at the local level. Additionally, the policy aimed to enable the rapid growth of affordable communications to all of the Afghan people so they might experience the Information Age; establish a fully functioning and affordable telecom infrastructure; and encourage the private sector to grow and take over these networks over time. The MCIT objectives included wide adoption of ICT to improve all aspects of Afghan life, including education, healthcare, employment, and access to information; growth of the local ICT industry to foster investment and employment; and use of ICT to increase government efficiency and effectively deliver improved social services. The policy was used to prepare the right legal framework and create a transparent regulator.

In 2005 the GOA published the Afghanistan National Development Strategy (ANDS), which articulated an interim strategy for achieving security, governance, economic growth, and poverty reduction. The ANDS five-year strategic benchmark for telecommunications stated that by the end of 2010, a national telecommunications network was to be put in place so that more than 80 percent of Afghans would have access to affordable telecommunications, and public revenues of more than \$100 million U.S. dollars would be generated annually. Additionally, it stated that the government would establish a telecommunications regulatory system to raise investor confidence and

create a public telecommunications backbone on which the private sector could build, to ensure that economic and social discourse extended to rural areas.

A five-year MCIT development plan was issued in 2005 and has served as the guiding document for ICT-related initiatives. The ICT strategy promulgated focuses on two major thrust areas. First, use of the private sector and appropriate regulations to help jump start economic recovery through enabling private-sector investments in the rapid expansion of mobile voice services and introduction of Internet services (direct on-line and dial-up access and Internet cafes) in the urban areas. Second, use of the government to develop the public ICT for governance and make affordable ICT services accessible to the broader population. Hence, the private sector is driven by density and return on investments, and the public sector is driven by the need to extend government influence to the provincial level, improve public security and governance at all levels, and provide ICT access to the district level. Ultimately, the intent is to extend telecom and IT access to the citizens in all of the 6,000 villages nationwide and to use both public and private systems to do this. The driving theory behind this strategy is that communications provides the foundation for security, economic development, good governance, and improved social well-being. The plan also addressed the development and privatization of the public service provider, Afghan Telecom, and the development of the public ICT sector, including capacity building of the MCIT, other ministries' staff, and the public in general.

The government, public, and private ICT networks that have emerged from this strategy are described later. They include the Government Communications Network (GCN), Provincial Governor's Communication Network (PGCN), District Communications Network (DCN), Village Communications Network (VCN), Cellular GSM providers, Internet Service Providers (ISPs) and Internet Cafes, CDMA-Wireless Local Loop network and expansion, Fixed Line network (including local copper cable) and expansion, Local Fixed Service Provider (LFSP) licenses and the National Fiber Ring. A number of parallel initiatives were begun by donors and NGOs to use ICT as an enabler of reconstruction in other sectors, such as healthcare and education. Examples of these are cited later.

Although not discussed in this paper, independent ICT networks are being established by the Ministry of Defense (MoD) and Ministry of the Interior (MoI) to support the ANA and ANP respectively. These networks use a mix of fixed, satellite-based VSAT networks, tactical military ICT capabilities, GSM cellular, a digital trunked radio system [Terrestrial Trunked Radio (TETRA)], and other fixed and mobile ICT capabilities. The ANA network has an interface with the GCN hub in Kabul. There also may be selected subscriber access to GCN/DCN services in the future.

In December 2005, President Karzai signed the Telecom Law, replacing the Laws on Regulation of Telephone Services 1964, 1968, and 2000 and establishing an independent regulatory body, the Afghanistan Telecom Regulatory Authority (ATRA). Salient new features of the law include provisions for regulating tariffs of operators with "significant

market power” and for ATRA oversight of the Telecom Development Fund (TDF).<sup>2</sup> ATRA was created by merging the Telecommunications Regulatory Board and the State Radio Inspection Department of the MCIT. The Telecom Law was published in the Official Gazette on May 27, 2006. ATRA became fully responsible for all regulatory functions in the telecom sector: licensing and compliance, spectrum planning and assignment, numbering, ensuring network interconnection, promoting competition, and consumer protection, among other things. Five board members were appointed in June 2006, and organizational build up was initiated and continues. In fact, today ATRA is actively monitoring and controlling the telecom sector to ensure compliance with the law and license conditions.<sup>3</sup>

The MCIT established an ICT Directorate and an official MCIT web site.<sup>4</sup> The +93 country code has been recognized by international and regional carriers. The Afghanistan “.af” domain name was recovered. The Afghan Network Information Center (AFGNIC) manages the country code top level domain and National Internet Registry of Afghanistan and also serves as the Internet Exchange Point for Afghanistan.

At the outset of the intervention into Afghanistan, the international, coalition military, and USG interests and investments in public Afghanistan ICT reconstruction and development were problematic. There appeared to be a general lack of understanding of the Afghan information and related ICT business culture. Donors shunned providing telecom reconstruction funds for public services (largely influenced by the so-called “Washington Consensus” championed by the World Bank), and even the USG took a largely hands-off approach to underwriting Afghan ICT, despite the obvious need for emergency support following the war. In 2003, Afghanistan was able to clear its debt to the World Bank, in part with the help of Japan, the UK, Sweden, Norway, and Italy, which contributed to a trust fund for this purpose. Additional funds from the multi-donor Afghanistan Reconstruction Trust Fund (ARTF), which is administered by the World Bank, helped to clear the remaining arrears, allowing Afghanistan to become eligible for loans for projects designed to help meet the country's longer-term development needs. As a result, in early 2004 the World Bank and USAID became engaged and granted money to the Afghanistan MCIT to create a national telecommunications system to connect the central government with the country's 34 provinces and create public access centers for Internet and telephone communications at the district level. Subsequently, China, India, and Iran expressed investment interest, but outside of the USG, UN, and World Bank investments there was little interest from other Western nations or IOs.

---

<sup>2</sup> The TDF was based on a 2.5 percent tax on private sector operator revenues and used to fund telecom development projects that may not be undertaken on commercial grounds by these operators.

<sup>3</sup> The official ATRA web site is <[www.atra.gov.af](http://www.atra.gov.af)>.

<sup>4</sup> The official MCIT web site is <[www.MCIT.gov.af](http://www.MCIT.gov.af)>.

## ICT—Putting the Pieces Together

---

An early initiative to provide government communications support for governance and emergency communications was a 2003 USAID-funded CODAN HF Radio network that linked the Kabul-based Afghan government with its 34 provincial government elements. Until the international community, GOA, and private investments enabled implementation of a nationwide ICT network, the HF network was the primary means for supporting governance and emergency communications to the provincial capital level. The CODAN network is still operational today with the base stations located in the MCIT buildings in provincial capitals.

Other early communications capabilities employed, even during the era of the Taliban, were over 100 VSAT nodes (providing access to International voice and Internet service) operated by NGOs and the UN and the Global Mobile Personal Communications by Satellite (GMPCS) phones. For some time, the VSAT nodes and satellite phones were the only means for accessing international communications and long distance communications within Afghanistan, and they are still used to a lesser extent today. Due to high costs, the satellite phones were (and are) not used by the common Afghan: the phones themselves are expensive and satellite-based phone calls frequently run over a \$1 per minute for a voice call and over \$5 per minute for low data rate calls. The GMPCS users tend to be foreign military; national government elements, such as Embassies and national aid organizations; IOs, NGOs, and foreign business representatives. GMPCS phones that have been used are Globalstar, Iridium (used by USG elements), Thuraya, and INMARSAT. ATRA has issued licenses to New Ansari Ltd. for Thuraya and AWCC for INMARSAT use throughout Afghanistan.

The main objective of the GOA Telecommunications and Internet Policy is to modernize and rapidly expand ICT networks and services and to achieve universal access to telephone and Internet across the country. The MCIT vision, strategy, and early efforts to establish a regulatory authority and policies enabled, with the help of the international community, significant progress to be made in the evolution (some might argue revolution) of Afghan ICT. The rapid introduction of ICT has served to help jump start the economy in the urban areas, extend ICT support to governance from Kabul to the provincial level, and establish telecoms and Internet access for the broader population at the provincial and some district levels. A good public-private partnership has proven to be the key to the success of the rapid growth of private cellular services and the early introduction of Internet services in urban areas.

Although at the outset the GOA, international donors, military, and private sector had no agreed, overarching ICT architectural framework to make investment decisions, there was a MCIT-led vision, strategy, and plan that influenced subsequent investment and implementation activities, resulting in the emergence of the “default” ICT architecture illustrated in figure 2. Investment and implementation activities of the MCIT/ATRA with support from international donors, such as the World Bank, USAID, and coalition military and investments of the private sector, such as the cellular providers, Internet

Service Provider (ISPs), and related Internet Café owners formed the basis for the public-private ICT networks that emerged. Additionally, coalition military and national government investments, supported by the MoD and MoI, formed the basis for the ANA and ANP ICT networks. The remainder of this section discusses the evolution of the ICT elements that form the basis of the default ICT architecture. Details of the ANA and ANP networks are not addressed.

### **Private-Sector GSM Networks and Services**

As early as December 2001, private-sector efforts began to build a phone system in a country still emerging from more than two decades of war. Battling logistical problems, political instability, and physical insecurity, the Afghan Wireless Communications Company (AWCC) launched a new wireless operation in April 2002 in Kabul with plans to quickly extend to four additional cities (Herat, Mazar-i-Sharif, Kandahar, and Jalalabad) by the end of the year. An international gateway was established to provide international phone service, and during the April 6, 2002, ceremony to launch the GSM network, Afghanistan's interim leader, Hamid Karzai, placed the first call to an Afghan émigré in Germany.

AWCC, which is 80 percent owned by Telephone Systems International (TSI), a U.S.-based company, and 20 percent by the MCIT, was awarded the first nationwide GSM mobile license in January 2003. The Telecommunications Development Company of Afghanistan (TDCA)—doing business as “Roshan”—was awarded the second nationwide GSM mobile license that same month. Roshan is 51 percent owned by the Aga Khan Fund for Economic Development (AKFED)—the development arm of the Aga Khan Development Network (AKDN); 37 percent by Monaco Telecom International (MTI); and 12 percent by MTC. Areeba, owned by Investcom (Lebanon), was awarded the third nationwide GSM mobile license in September 2005. The United Arab Emirates (UAE) based, Etisalat, was awarded the fourth nationwide GSM mobile license in May 2006.

Although at the outset the GSM network performance was fragile in terms of coverage and quality of service (dropped calls and poor voice quality) and costs to use it were high, by the end of 2006 four licensed GSM operators were providing cellular phone service to major urban areas, quality of service had improved and costs had decreased substantially. The customer base grew to more than 2 million subscribers and is still growing. Of the four independent networks, AWCC and Roshan are nationwide and the other two plan to be. AWCC has about 900,000 subscribers and the most extensive terrestrial microwave network. Roshan is Afghanistan's leading cellular telephone service provider with a countrywide network of more than 160 cities and towns and about 1.2 million subscribers. They directly employ more than 800 people and provide indirect employment to more than 15,000. Roshan has invested over \$240 million in Afghanistan and is the country's single largest investor and taxpayer, contributing approximately 6 percent of the Afghan Government's overall revenue. Areeba has coverage in Kabul, Mazar-e-Sharif, Kunduz, Jalalabad, Herat, Kandahar, and Zabul and is expanding fast to other cities. Etisalat plans to have its commercial launch in 6 cities in June 2007. The GSM networks have their own international gateways and employ a mix of satellite and

Figure 2. "Default" Afghanistan ICT Architecture

## "Default" Afghanistan ICT Architecture

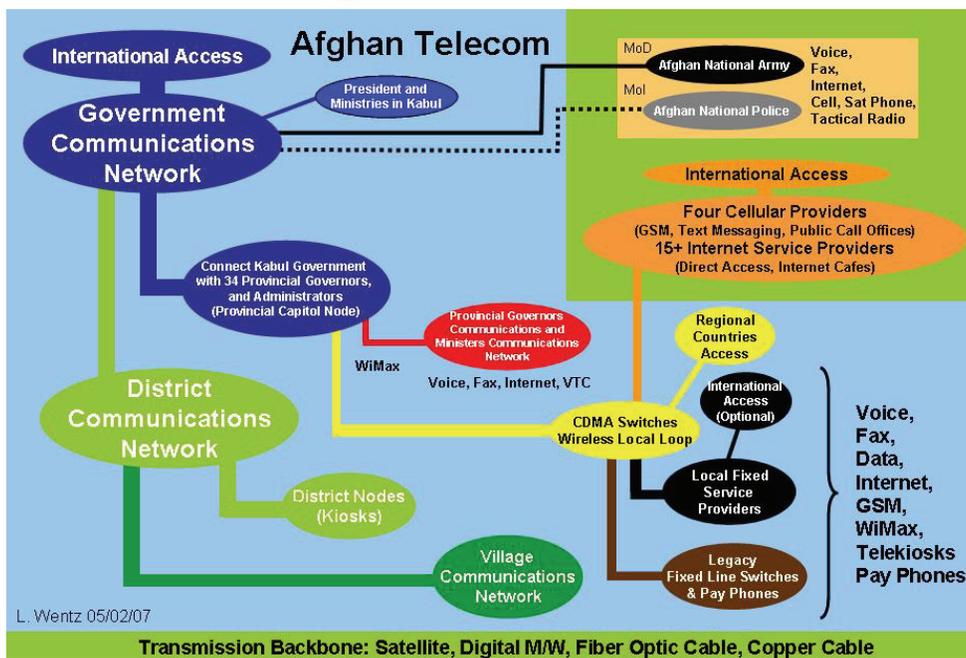
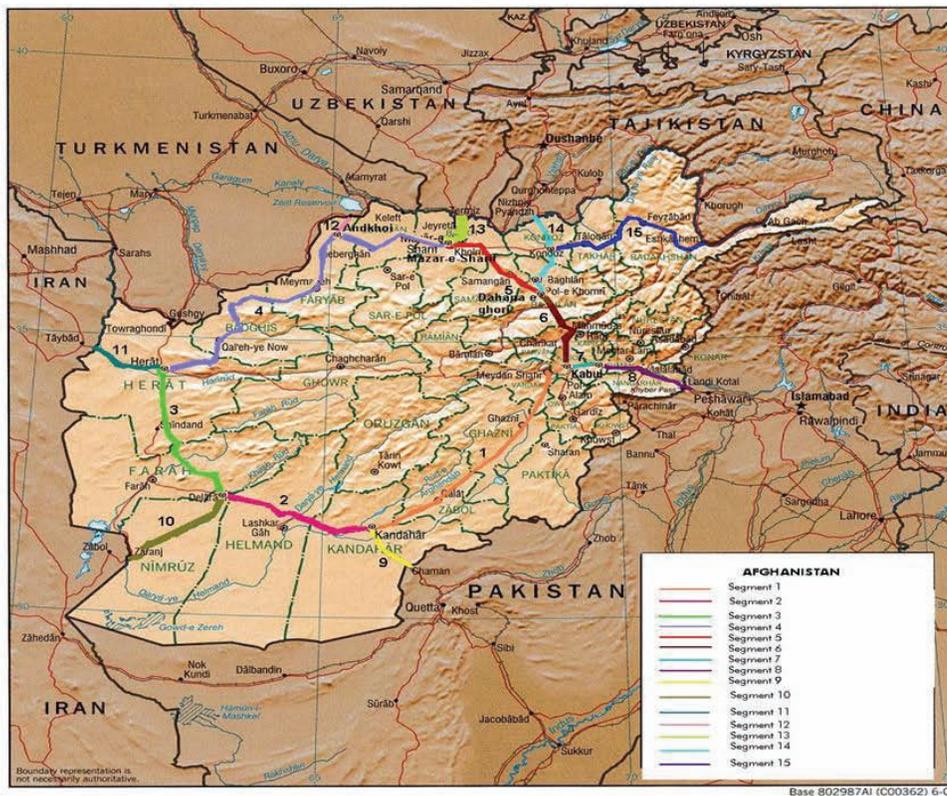


Figure 3. National Fiber-Optic Network



digital microwave transmission for network connectivity, and the networks are interconnected. Prices for calls between networks differ but will converge with competition. Some cell phone users have separate phones for accessing the different cellular networks. AWCC and Roshan each have active roaming agreements with other network operators.

In the 2002 timeframe, phones cost more than \$400 and airtime averaged \$3 a minute. The prices for mobile service dropped about 70 percent between September 2003 and March 2005. In the 2006 timeframe, the cost of phones was around \$35 and airtime charges were roughly 10–15 cents per minute, dropping to 5 cents per minute in off-peak periods. Today, the cost of calls to other networks has come down from 30 cents per minute to 9 cents and Subscriber Identity Module (SIM) card prices have come down from \$30 to \$5.

The GSM providers offer short message service (SMS), and Roshan offers web-based management of SMS text distribution. Roshan is deeply committed to Afghanistan's reconstruction and socio-economic development and has tested and plans to offer General Radio Packet System (GRPS) service that enables customers to plug their laptop into the cell phone and browse the internet, check email, and send data. They offer low-margin public call office (PCO) service to benefit more remote and less affluent sections of society. In some places women's groups and former soldiers have been able to establish PCOs to provide phone services for people without telephones. Someone who runs a PCO can make up to \$120 a month. Additionally, Roshan has tested the mobile commerce service offered by Vodafone's M-PESA mobile remittance transfer service, which enables mobile phone subscribers to transfer money to other mobile users via SMS text messaging. They also are exploring with ATRA and the Da Afghanistan (Central) Bank (DAB) licensing cell phones for electronic cash transfers. Other cell phone techniques are being developed that use SIM cards and text messaging to swap airtime for goods and services.

### **Private Internet Cafes and ISPs**

In mid 2001, the Taliban banned the use of the Internet to stop access to vulgar, immoral, and anti-Islamic material. With the fall of the Taliban, ad hoc Internet cafes emerged as early as 2002 in Kabul. AWCC opened the first Internet Café in the Kabul Intercontinental Hotel in July 2002. Since then, hundreds of privately run Internet cafes have opened around the country—mostly in urban areas such as Kabul, Herat, Mazar-e-Sharif, Khost, Jalalabad, and Kandahar. In an Internet Café visited in Khost, it cost about 40 rupees (67 cents) per hour to use the Internet and approximately 60–70 customers visited per day—mainly youth checking emails and chatting on either Yahoo or MSN messenger. Although the Internet has become one of the most efficient ways for Western firms to communicate and conduct business with distant clients, Afghan business use of the Internet has been slow to catch on and nearly nonexistent outside the largest cities. A December 2005 World Bank report suggested that businesses in cities such as Kabul, Herat, and Mazar-e-Sharif were using the Internet, but in Jalalabad and Kandahar only a few firms reported using websites and email to interact with clients and suppliers.

The first ISP was licensed in 2004. Since then, ATRA has licensed more than 15 ISPs that provide Internet service to over 500,000 users. Although most of the ISPs can provide a satellite connection anywhere in Afghanistan to facilitate access to the Internet and many use WiMax in major urban areas to accommodate local direct access arrangements, there is no nation-wide ISP equivalent to Verizon, Cox, or NETZERO. ISPs typically offer VSAT arrangements, wireless broadband up to 20 Mbps, and dial-up access up to 56 Kbps. Some of the major Afghan ISPs are Ariana Telecom, CeReTechs, Neda, Insta Telecom, New Dunia Telecom, KBI AF (VARIA), and LiwalNet. The cost of Internet access from an ISP has dropped over the last several years; the Afghan ISP Association cited a reduction from \$1,500 for a “shared 64 Kb/s” connection to about \$200.

### **Public Fixed Line and Wireless Local Loop Services**

A few, legacy, fixed line switches provide local voice services and support some 300 pay phones in Kabul. A few other fixed line switches and pay phones are found in a couple of the other larger cities, such as Herat, Mazar e Sharif, and Kandahar. These switches are interconnected with the local CDMA wireless local loop switches.

In 2003, the GOA contracted with Huawei and ZTE of China and TCIL of India to implement a Code Division Multiple Access (CDMA)<sup>5</sup> network to provide wireless local loop service in urban areas. Plans are also in place to expand this service to rural areas. There are now 31 CDMA switches and 85 Base Transceiver Stations (BTSs) deployed throughout Afghanistan, providing wireless local loop service. Nine provinces have Hauawei-China switches, 10 have ZTE-China switches, 11 have TCIL-India switches, and one has a Siemens EWSD digital switch. The existing CDMA network, along with the fixed line network, provides access to over 165,000 digital lines and has the capacity to build out to 225,000 CDMA lines and 101,400 fixed lines. The network connectivity is a mix of satellite and digital microwave; 27 provinces are connected by satellite and seven by digital microwave. CDMA subscribers have both desktop and handheld versions of CDMA phones. There is, however, limited mobility (restricted to geographic coverage area of the BTS providing service), since the network does not have national or global roaming capability. Interconnections exist between the CDMA and GSM networks enabling calling between networks. The CDMA network is managed by Afghan Telecom and uses post-paid call billing. Afghan Telecom has been considering adding a pre-paid billing capability and Mobile Switching Centers (MSCs) to accommodate roaming services. This would create a public CDMA-based cellular network that would compete nationwide with the four private GSM networks. A Packet Data Switching Node (PDSN) is being used to pilot mobile data service in the Kabul area, and there are plans to extend this service throughout Afghanistan.

In early 2007 actions were taken to issue a request for proposal (RFP) to broaden the coverage of the CDMA network and add functionality. ATRA issued a tender for a CDMA-based mobile network and a landline operator, both supporting the MCIT plans. Afghan Telecom plans to re-configure and re-orient the existing CDMA and Fixed Line networks and implement the first CDMA-based, fully mobile, pre-paid voice and data

---

<sup>5</sup> A digital cellular technology that uses spread-spectrum techniques.

network, covering all 34 provinces in Afghanistan. The CDMA network will offer pre-paid services using the Wireless Intelligent Network platform and the data services will be provided by PDSNs. The Fixed Line network will offer pre-paid service using Fixed Intelligent Network platforms and DSLs and ADSLs data services will be offered using data cards in the Fixed Line Switches and DSL and ADSL equipment at the customer premise. During an April 2007 MCIT presentation on the status of ICT, it was noted that contracts have been signed for 150,000 digital lines in the major cities of Kabul, Kandahar, Mazar, Jalalabad, and Kunduz at a cost of \$40 million and a 50,000 digital line expansion in Herat at a cost of \$15 million. Completion is expected the first quarter of 2008.

### **Afghan Telecom Network and Services**

To enable public ICT reconstruction and development, the World Bank and USAID provided the MCIT funding to help create a government and public communications network, which is now maintained and operated by Afghan Telecom. When fully implemented, this network will provide voice, fax, and Internet services, national and International calling access to provinces and districts, and video teleconferencing (VTC) services to provincial governors. Funding included an international satellite gateway in Kabul to access global voice, data, and Internet services. The World Bank invested \$16.8 million to develop the government communications network (GCN) and another \$3.7 million to rehabilitate the International Satellite Gateway in Kabul. The GCN provides International voice and Internet access and communications services to support governance to the provincial capital level—governor and key administration elements, including in some cases police chiefs. USAID invested \$14.2 million to develop the district communications network (DCN) to extend voice and Internet access to the district level for use by local government officials and the local population. GCN and DCN serve to enable good governance at the provincial and district levels by helping remote communities and government offices throughout Afghanistan communicate effectively with each other and the world.

In 2004, the MCIT contracted with the American firm Globecom Systems, Inc. (GSI) to engineer and implement the GCN and DCN and rehabilitate the International Satellite Gateway. The 34-node GCN network was commissioned in 2005, and the rehabilitated International Satellite Gateway in Kabul was commissioned in July 2006. The GCN network connects 42 ministries and other major offices in Kabul to each other and links the central government in Kabul to the governors of the 34 provinces. A meshed satellite network supported by some digital microwave links provides the network connectivity for GCN and the Kabul-based GCN satellite gateway provides access to the Hong Kong International gateway for worldwide calling and global Internet access. The rehabilitated earth station provides alternative routes for both national and international calls and also has been connected to the Afghanistan Radio and Television facility in Kabul to support TV Broadcasts. The GCN satellite links provide T1 connectivity (but can be engineered for higher data rates) between the network nodes. The network supports voice, fax, Internet, and VTC services to the provincial capitals and key Kabul-based government elements. In regard to the latter, a Taliban-era fiber optic ring, supported by digital microwave links, provides connectivity in the Kabul area for interconnecting the ICT

capabilities of the offices of the President, Ministries, and Kabul city offices with the GCN.

Because of funding limitations, GCN service was only extended to the MCIT buildings in the provincial capitals, not to the governor and other key offices as originally intended. A program, referred to as the Provincial Governors Communications Network (PGCN), was developed to acquire and implement ICT capability packages to extend services from the MCIT building to the governor and other key administrative offices. In 2006, the coalition military [Combined Forces Command-Afghanistan (CFC-A)] used the Commander's Emergency Response Program (CERP) funds to purchase and implement a PGCN solution package that provides WiMax terminals at the MCIT facility and related end user equipment to extend GCN voice and Internet services to the governor and related administrative facilities—five telephones and five computers. The initial CERP funding covered 12 provinces and these sites are now operational. Sources of funding are being explored to equip the governor and related administrative facilities in the remaining 22 provinces. One option under consideration is a two-phase effort where CERP funding would be used for part of the project and MCIT would fund the remainder. If this occurs, it will illustrate the successful use of U.S. government funds to jump-start a reconstruction program that is then transitioned to the local government for completion.

The initial PGCN extended only voice and Internet services to the governor's facilities; the governors had to go to the MCIT building to use the VTC service. Since the VTC capability is used frequently by President Karzai to conference with provincial governors, and since it is becoming increasingly dangerous for the governors to travel in certain areas, actions have been taken to extend the VTC to the governors' facilities. Several of the 12 PGCNs implemented have been adjusted to accommodate VTC, and the remaining installations are being engineered to do this. Implementation of the remaining 22 PGCNs will include extension of voice, Internet, and VTC.

Only 337 of Afghanistan's 365 districts have been funded to receive DCN nodes. By early 2007, only a few more than 200 of the 337 funded district sites had been commissioned and were connected by a VSAT star network configuration. The network offers district-level access to phone, fax, and Internet services. At each DCN node, a telekiosk arrangement provides access to five phones, five workstations with Internet access, and a fax machine. The DCN links operate at roughly 256 kbs but could be engineered for higher data rates. Since there is no national power grid, diesel generators and batteries power the DCN nodes and related ICT equipment. The DCN sites are located near district centers to enable the local population to make voice calls within Afghanistan or internationally and access the Internet. A small fee is charged for these services, typically 1 Afghani per minute for calls within the district, 5 Afghanis per minute between districts, and 25 Afghanis per minute for international calls; Internet access is 20-30 Afghanis per hour. The exchange rate is about 50 Afghani to one U.S. dollar.

It was recognized during the initial phases of the DCN network implementation that most nodes likely would not be able to generate enough revenue to be self-sustaining, but there

was also a desire to not operate at a major loss. Overall, it has been reported that Afghan Telecom is currently losing several million dollars per year. As noted earlier, the intent was to rapidly expand coverage to districts and start marketing DCN services so that the demand for services would be sufficient to generate the needed revenue to allow the nodes, and the network in general, to become a viable operation. The operational growth in network traffic to date provides evidence that the demand for DCN services is there, but the network statistics also suggest that usage is not consistent across all nodes. It is not clear why some nodes are more successful than others. A large number of the DCN nodes commissioned have been unable to generate enough revenue to sustain their operations cost effectively. This has been attributed to a lack of customers, largely driven by the inability to market the availability of DCN services at the district level. Until recently, there were no marketing plans, no signs on DCN buildings or in the towns to advertise voice and Internet services, and no local radio advertisements. Many locals do not know that DCN service exists in their area. Additionally, some of the nodes are located outside population centers in protected enclaves that do not make it conducive to walk in off the street. Provincial Reconstruction Team (PRT) personnel are now actively involved with the MCIT in several provinces to explore ways to help increase local use of the DCN services.

As a result of the low demand, some DCN sites are only open 2 hours a day, if at all. Some only power up if a customer arrives. The MCIT is monitoring the revenue produced by DCN nodes to identify poorly located and managed DCN sites. Plans will be developed to relocate the equipment and services from these sites to more appropriate locations. There have been MCIT/ATRA discussions about franchising DCN nodes as a way to develop a more profitable customer base and make DCN a financially viable and sustainable service. It has been estimated that monthly revenues of about \$3,000 would be required just to cover operating expenses and break even. Cost of fuel alone for the diesel generators is about \$800 per month and a key factor in the cost of doing business.

Availability of district communications buildings (usually two buildings, one for the ICT equipment and one for the generator) and physical security concerns due to increased insurgent threats have slowed the implementation of DCN nodes, but MCIT/Afghan Telecom are optimistic the remaining nodes will be completed by the end of 2007. However, of the 337 sites programmed for DCN equipment, and for which the equipment has already been purchased and stored in a warehouse in Kabul, only 275 have funding for building construction. The funding comes from a variety of sources, including USAID, PRT CERP money, United Nations Development Programme (UNDP), and Afghanistan Stabilization Program (ASP). Funding for the remaining 62 buildings has not yet been obtained. Delays in funding could impact the ability to complete implementation of the 337 DCN node network by the end of the year. Additionally, funding for DCN equipment and buildings for the remaining 28 unfunded district nodes is yet to be determined. Some of the remaining 28 nodes will be candidates to use equipment relocated from the poorer performing DCN nodes.

The GCN/DCN implementation challenges for GSI were related to both environment and system integration. Outside Kabul, there was little or no infrastructure, roads, or

electricity. Security was a continuing concern. According to GSI reports, in some areas implementation teams had to unload trucks in the middle of nowhere, hand-carry the electronics across a stream, get the truck across the stream, then reload it. Security protection had to be provided by GSI. Unexpected systems integration challenges also caused problems. For example, the MCIT purchased CDMA switches that when implemented formed islands of wireless communications with no outside connections that then needed to be interconnected to form a network. The GSI team was called upon to engineer the interconnection of the CDMA switches with the GCN and its long distance network.

GSI installed a soft switch at the GCN hub in Kabul to handle the GCN/DCN routing, call setup, and tear down, as well as support the CDMA network and the associated fixed line switches connected to it. The CDMA network uses the GCN satellite gateway for international calling; access links connect the CDMA switch in Kabul to Pakistan (digital microwave) and the Siemens EWSD switch in Herat to Iran (fiber optic cable). Similar links to other neighboring countries are planned in the future. The CDMA switches also have interfaces with private cellular networks, and this arrangement provides the means for calling between the public and private networks within Afghanistan. The interconnection of the various networks has served to establish the foundation for evolving to a nationwide network. In fact, what originally had been planned to be a purpose-built network serving government needs and strategic objectives rapidly became a public network, which in a sense serves as the default nationwide backbone network with international and regional access.

In 2005, the GOA approved a decree to transfer the MCIT's public ICT network and operations to an incorporated public company, Afghan Telecom, which is now responsible for providing government and basic public telecommunications services nationwide. The MCIT holds 100 percent of Afghan Telecom; opportunities are being sought to sell this interest to private companies. Plans are also in place to privatize Afghan Telecom. The timeframe for this action is under consideration by MCIT/ATRA.

As part of the MCIT/ATRA and Afghan Telecom objective to extend ICT services to the broader public and, in turn, create investment and job opportunities consistent with approved Telecom Policy, licenses are being issued to allow the private sector to establish essentially independent telephone companies that will eventually become part of Afghan Telecom. This initiative is referred to as the local fixed service provider (LFSP) program. Its main objectives are to facilitate faster roll out of services to small towns and rural areas and to provide investment opportunities for small-to-medium local investors across the country. It is hoped that the LFSP initiative will result in more than \$100 million in investments, the creation of thousands of new jobs, and rural areas receiving ICT services sooner.

In May 2006, the first LFSP license was granted to Wasel Telecom to implement wireless services in small towns and rural areas in the provinces of Kunduz, Jawzjan, and Balkh; the first facility was commissioned in Mazar in April 2007. In February 2007, three additional licenses were issued: one to Shaheen to cover 20 districts in the Logar, Paktya,

and Khost provinces, and one each to Ertibat and Watan to provide services in five districts of the Herat province. The LFSP providers can offer wireless voice and data services. The LFSP facilities interconnect directly with the Afghan Telecom CDMA switches and also may interconnect with the private cellular networks. Additionally, while the LFSP license offers the opportunity to use their own international gateways, MCIT/ATRA has directed that they use the GCN International gateway as part of the Afghan Telecom suite of nationwide capabilities.

Rural area ICT coverage is essentially non-existent today. The MCIT and Afghan Telecom have proposed exploring low-cost and low-power solutions for the rural area, referred to as the Village Communications Network (VCN). It is envisioned that the VCN would be an extension of access to DCN voice and Internet services for the rural areas and that low-cost ICT capability packages would be employed to interconnect with the DCN network.

A number of vendors already have suggested the use of low-cost ICT packages in rural areas, consisting of a solar-powered wireless data communications capability that provides customers wireless service to access the Internet and use VoIP for voice service. These ICT packages would be connected to a DCN node. Afghan Telecom plans to launch a pilot program and estimates equipment to get started would cost approximately \$10,000 for an ICT package with Internet connectivity or \$4,000 for basic telephone service. Additional costs would include transport to the site; site preparation; training; maintenance; operational and/or security staff; and telecom usage charges. This could be an ideal solution for an entrepreneur or perhaps run by the village elder. Funding for part of the extension of services to rural areas likely will be supported by the TDF. The fund had about \$9 million in 2006 and the MCIT expects an additional \$10 million in 2007.

Through a U.S. Trade and Development Agency (USTDA) grant, ATRA has hired a consultant to recommend how to manage the TDF and make the best use of the funds to provide rural communications.

### **Public and Private-Sector Transmission Networks**

At the end of 2006, ZTE Corp was awarded a contract for a national fiber optic network along the national ring road that connects the major population centers (Kabul-Ghazni-Kandahar-Heart-Mazar-Samangan-Baghlan-Kabul) around Afghanistan. Figure 3 illustrates the route and shows the 72 access nodes planned along the ring to provide connection points for additional microwave, satellite, and cable links to connect all district centers and key cities. The fiber ring will be about 3,200 km in length, have a total of 1,008 E1 (2 Mb/s) links, and be carried in a three-tube layout with 12 optic fibers per route for a total of 36 fibers. There will be links to all neighboring countries [two into Pakistan and single links into Tajikistan, Uzbekistan, Turkmenistan, and Iran (existing)] and to the world. The fiber ring will greatly reduce the cost of voice and data traffic, pave the way for more affordable services, and position Afghanistan to become a leading international traffic carrier between the Gulf/India and Central Asia/Newly Independent States. The project cost is \$65 million. Implementation started in April 2007 and is hoped to be completed in 24 months.

In addition to the planned fiber ring, private cellular phone providers already are implementing digital microwave links along the same ring road to urban and other areas. New companies, such as the Asia Consultancy Group (ACG), are starting to build digital microwave links to support public and private provisioning needs. ACG is currently constructing a digital microwave link for Areeba that connects Kabul and Jalalabad and extends connectivity into Pakistan.

The fiber optic network and digital microwave links could be used to provide alternative means for provisioning GCN/DCN, CDMA network, GSM, and other connectivity, thus allowing an eventual migration of the satellite-based connectivity from largely VSATs to a mix of satellite and terrestrial connectivity. Contracts also have been let with ASTER of India and Sher-Gandhi of Iran/Kabul for fixed line outside plant copper cabling in the cities of Kabul, Herat, Mazari Sharif, Kandahar, Jalalabad, and Kunduz.

The mix of satellite, fiber, copper cable, and microwave transmission links could be combined to form a national backbone transmission capability that could be used to provide connectivity for public and private networks and also provide a means for rapidly accommodating surge capacity needs during crises as well as restoration and recovery of failed connectivity due to natural or manmade disasters. It also could be used to create a competitive environment for achieving lower-cost network connectivity through more openly competing backbone transmission provisioning.

### **ICT Support to Cross-Sector Reconstruction**

Private VSAT networks are used to support business communications and information exchange needs of the larger contractors who have reconstruction sites and offices throughout the country. As noted earlier, the UN has VSAT nets and NGOs manage more than 100 VSAT-based sites to support their communications and information exchange needs. Additionally, IOs and NGOs are employing innovative uses of telecommunications and IT to enable sector development, such as healthcare and education. For example, in the healthcare area, Partners in Technology International (PACTEC) implemented a VSAT link, associated LAN, and workstations throughout the Cure International Hospital in Kabul to provide doctors, nurses, and other medical staff Internet access for research and reference material, as well as to facilitate lab work such as remote tissue analysis, support reachback to subject matter experts for consultation, and provide other electronic-Healthcare (e-Healthcare) uses. Donated lab equipment allowed electronic images of tissue samples to be digitized in the lab and sent over the Internet as a .pdf file attached to emails to pathologists in the United States and elsewhere who conducted an analysis and sent the results back to the hospital within 24–48 hours. Before implementing this Internet-enabled service, actual samples of tissues had to be sent out of the country to Pakistan and elsewhere, requiring weeks to get results. Personal Digital Assistants (PDAs) with medical diagnostic software tools have been provided as well and are being used by doctors to diagnose patient symptoms and prescribe medications and treatments. Software updates can be downloaded from the Internet. World Wide Lab, another NGO, provided a software package for a patient record system for the hospital. The software package automated the in-processing of patients as well as

the recording of their medical and payment history and also included an inventory control capability for the hospital's pharmacy.

In the education area, NGO supplied workstations, LAN, and VSAT provide Internet access for the Journalism Lab at Khost University. A CISCO Academy is also located on the same campus and has separate VSAT, LAN, and workstations to support IT training. Ironically, the Computer Science Lab next door to the Journalism Lab and across the street from the CISCO academy has not been as fortunate. It has some 20 workstations, but no power to operate them or LAN or Internet access arrangements. Situations like this are ideal opportunities for the military/PRT, aid organizations such as USAID, IOs like the UN, or NGOs to consider funding an arrangement to leverage capabilities on campus and provide Internet access for a broader student population. In Kabul, for example, the NATO "Virtual Silk Highway" project provides affordable high-speed Internet access to staff and students at Kabul University (Kabul campus is wired with fiber optic net and NATO provides satellite access to Internet) and seven other educational institutions in Kabul. There are partnership and e-Alliance programs between Kabul University and universities in the United States and other off-shore institutions that are part of the Afghanistan eLearning and capacity building programs. The San Diego-Jalalabad Sister City program supports efforts to equip Nangarhar University and Medical School and elementary and middle schools in Jalalabad with computer labs and Internet access. However, not all Afghan universities have comparable capabilities. Additionally, universities within Afghanistan are not electronically linked together over the Internet or otherwise. Medical schools are not electronically linked with local hospitals either but could be as well.

ATRA has taken some initiatives to use the public network to promote distance learning. In discussions with two of the LFSP licensees, it was agreed they would provide free Internet connectivity to each of the schools in the districts they are licensed to serve. It is anticipated that these schools could serve as community access points for distance learning. ATRA also has provided money from its TDF to the Ministry of Education for computer equipment (servers) that will allow video on demand retrieval of educational programming already being broadcast nationally by the government-owned TV station. These broadcasts consist primarily of a new weekly half-hour program similar to Sesame Street. ATRA is also exploring the availability of finances or subsidies for the construction of community towers to expedite rural area service availability from mobile service providers. ATRA will launch public consultations to work out the details and develop simple procedures for communities to obtain funding. An approach being considered would be for the community to sign a petition and simple application. On that basis, ATRA would commission a site survey and a "reverse auction" for funding to build the tower (the least subsidy requirement would win the project). Other selection factors might include how fast the site could be made operational. Space on the towers would be leased to private cell phone providers and other telecom and IT providers as appropriate.

The DAB has licensed 12 commercial banks. Out of the 12, seven are full-fledged commercial banks. Most of the 12 commercial banks licensed to operate in Afghanistan

are concentrated in Kabul and provide services primarily to international donors and businesses, foreign NGOs, and foreign government agencies. International funds transfers via SWIFT have been available through the Central Bank since July 2003. Commercial banks are currently offering International Funds Transfers, some using their own facilities and others using the Central Bank's capabilities. Domestic transfers can be arranged throughout 32 provinces in Afghanistan through the Afghan Funds Transfer System (AFTS). Although relatively new, AFTS has been successfully tested and DAB Kabul is now sending and receiving domestic funds transfers on a daily basis. However, because of widespread distrust of the banking system, many local businesses continue to use the *hawala*<sup>6</sup> system for short-term loans to finance working capital needs, or rely on family and friends.

Given the continuing high risk security environment and lack of broader public access to nationwide banking, MCIT/ATRA, the DAB, and the private sector are exploring alternative means for financial transactions, such as the use of cell phones for electronic funds transfer, G-Cash, e-Wallet solutions, and mobile commerce. Such capabilities could revolutionize economic and social development by offering people a means to swap SIM card credit for goods and services or initiate money transfers using SMS text messaging. New capabilities could be used to automatically pay soldiers and police in remote locations without, as is the case today, having to physically deliver cash to them and then have them leave their posts for several days to take the money home. Funds could be electronically transferred to a family electronic account. A 2007 pilot project between Roshan and DAB successfully tested the Vodafone M-PESA mobile commerce capability, and Roshan plans to apply for a permanent license to offer a range of financial services using the personal cell phone.

The judicial system is exploring e-Solutions and databases and the Ministries are exploring the use of e-Government. A National Data Centre (NDC) is being planned to archive national information records to support and be available to government entities. The Afghan Parliament recently urged the government to accelerate the process of creating a National Identity Card and National Passports, with special focus on decentralizing the application and issuing processes. Other examples of interest in government services to be provided include: record keeping and operations for foreign trade; government pension beneficiaries; utility billing; central bank, population, and demographic databases; and national statistical databases.

### **ICT Capacity Building**

USAID, UNDP, World Bank, and other organization have focused on capacity building initiatives that include rehabilitating the MCIT Telecoms Training Center, upgrading it to a modern ICT Institute, and establishing 12 MCIT ICT training centers and six CISCO networking academies around the country to train Afghans in the use of computers and IT. Establishment of the ICT Institute is ongoing with new buildings under construction, laboratory and curriculum being developed, and training of the trainers underway. The

---

<sup>6</sup> Hawala is an informal value transfer system based on performance and honor of a huge network of money brokers which are primarily located in the Middle East, Africa and, Asia.

first batch of students will enter in 2007 and enrollment is set to produce 50 engineers annually. Plans have been made to add three more CISCO academies in 2007.

University programs are being developed and degrees in Computer Sciences are being offered at major institutions, such as Kabul, Jalalabad, and Khost Universities. There are also initiatives to introduce English language training and Business Management programs. New universities such as the American University of Afghanistan (AUAF) in Kabul are opening up as well. AUAF is offering two undergraduate degree courses, one in Business Administration and the other in ICT.

Local businesses are also emerging to teach computer usage skills and English language. No government certification is required for these training programs, rather it is believed that the community will self discipline and weed out those elements not providing adequate training.

### **Cyber Security and Electric Power Challenges**

Cyber security is an essential component of developing information based services, such as those to be incorporated in the Ministries and National Data Center. There are regulatory requirements for digital signature, cyber crimes, and data protection, and these are being addressed in a proposed ICT law. The appropriate regulatory environment is essential for the development of secure e-commerce, e-health, e-education, and e-government-like services.

The creation of a National Cyber Security Strategy and Plan and the establishment of a National Cyber Security management structure has been under consideration by the MCIT for some time, and some starter elements have been put in place. There are plans to create an Afghan Cyber Emergency Response Team capability (AFCERT). Assignment of information security officers in Ministries and other government organizations as well as establishing cyber training and awareness programs are being considered. Much remains to be done to improve the cyber security posture of the government and public and private networks, including public-private cooperative arrangements.

The lack of reliable electric power for ICT continues to be a major issue, especially in rural areas. Generators are currently the primary power source for ICT equipment with battery backup. The private cellular networks operate 24x7 and use a mix of generators, solar power, and battery backup. The GCN is a full period service as well and operates its nodes 24x7 using diesel generators for power and batteries for backup.

On the other hand, the DCN tends to be operated as an on demand service and therefore does not operate 24x7. DCN nodes use generators and battery backup. Because the fuel to run them is expensive by Afghan standards, many only operate a couple of hours a day or when a customer needs to use the system. The rest of the time the nodes are powered down. In an attempt to provide a lower cost power solution for DCN nodes, the U.S. military has used CERP funds to purchase and implement solar power for 35 DCN nodes

(ZTE is the contractor). Positive results from this effort could result in a more general replacement of DCN diesel generators with solar power.

Designers, providers, and users of ICT have not paid sufficient attention to the use of energy efficient ICT equipment, such as laptops versus desktop workstations or power savings procedures to reduce the demands for power.

Since Afghanistan has no national power grid, a need exists to explore the use of a mix of alternative power sources to reduce pollution caused by generators which are costly to operate and maintain. Alternative power sources such as solar, small-wind, and micro-hydro are being explored.

### **A Continuing Success Story**

In spite of overwhelming challenges, Afghan ICT has proven to be a major success growing from essentially nothing to over 2.5 million subscribers in four years. This represents a telephone penetration rate of 8 percent, a milestone that took India and Pakistan over 10 years to achieve. The ICT sector has generated more foreign investment, high-quality jobs, and new tax revenue than any other legitimate sector. Foreign investments in ICT exceed \$700 million. The MCIT estimates the telecommunications sector today directly and indirectly employs some 40,000 people in Afghanistan—over 8,000 jobs are direct employment by telecom companies and the rest, indirect jobs in the form of sales channels, subcontractors, and telecom services companies. Revenues from the telecom sector make up about 12 percent of total government revenues—rising from less than \$20,000 in 2002 to more than \$100 million in 2006 (issuing two GSM licenses brought in over \$80 million alone). By 2010 the government aims to ensure that more than 80 percent of the Afghans have access to telecommunications services—current MCIT estimates suggest that 50–60 percent of Afghans now live within a coverage area of the Afghan ICT network with the ability to have access. It also is estimated that the number of cellular subscribers will grow by about 100,000 per month, increasing from approximately 2 million in 2006 to more than 5 million in 2010, and that the ICT sector will contribute more than \$200 million a year in public revenues.

Figure 4 is a high-level systems architecture representation of the “as is” Afghanistan ICT. The 34-node GCN network is fully operational including the International gateway. Twelve of the 34 PGCN ICT capability packages have been implemented, and it is estimated that it will cost about \$1.5M to implement the remaining 22. More than 200 DCN nodes are operational and estimates to build out the network to 365 nodes are about \$14M. The CDMA network is growing with plans to make it a nationwide mobile voice and data service. The LFSP (one contractor setting up a network and three preparing to do so soon) have now become active elements of the network. These networks are managed by Afghan Telecom from the network operations center located in their headquarters building in Kabul.

The Village Communications Network concept is part of the MCIT five year plan and is now incorporated into the ANDS goals—it has high visibility within Afghanistan and the international community. Initiatives such as LFSP are beginning to reach out to address

Figure 4. Afghan ICT “As Is” Baseline

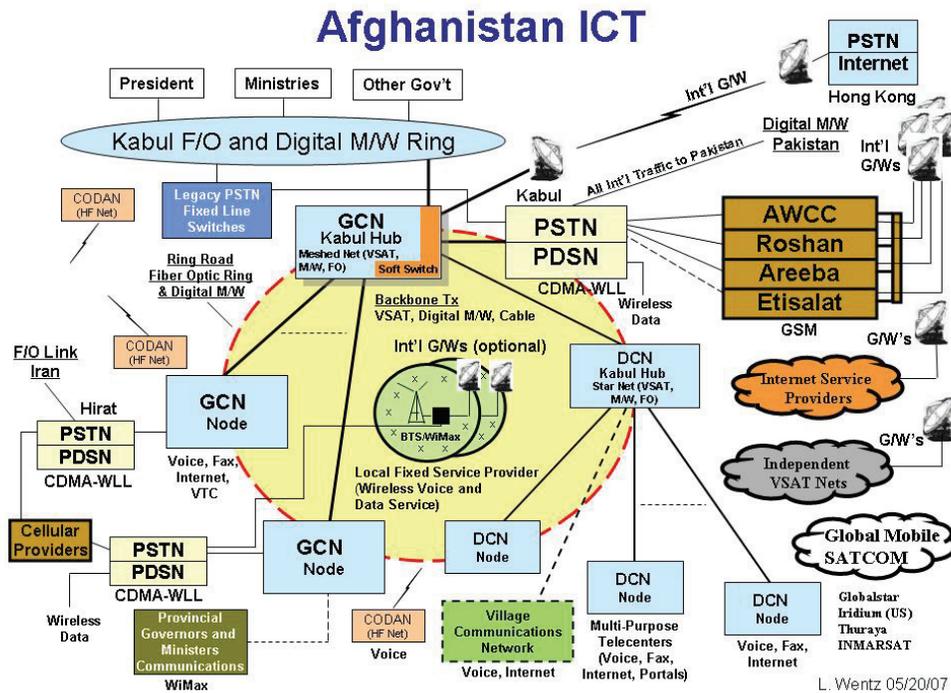
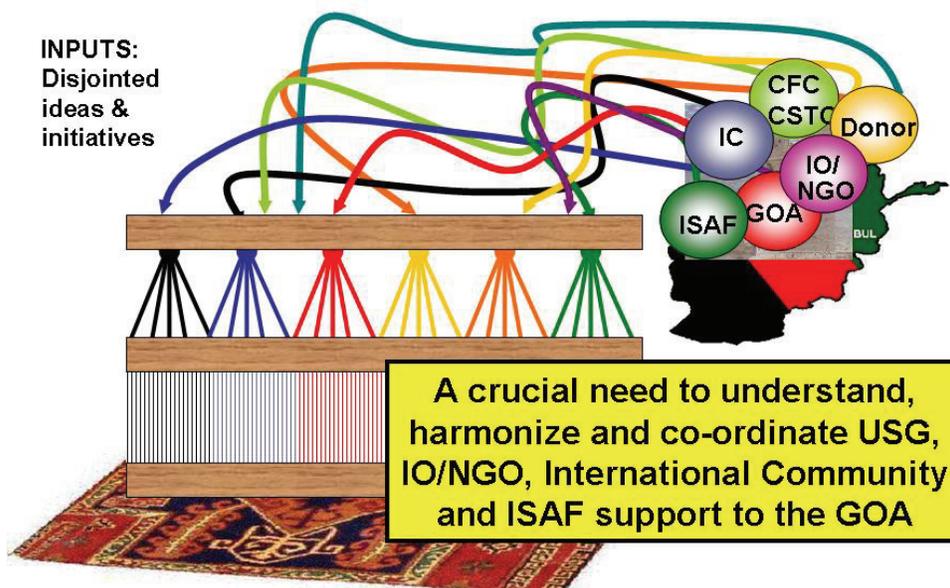


Figure 5. Afghanistan: The Challenge

## Afghanistan: The Challenge



some of the rural area needs. Cellular service is also starting to reach some rural areas with MCIT/ATRA initiatives encouraging further expansion. Several technologies are available to provide tailored ICT services at the village level, but more detailed analysis is needed regarding power requirements, information culture and related village requirements. The cost of providing a family of VCN ICT capability packages to 6,000 villages is estimated to be on the order of \$47M.

Two of the four licensed GSM cell phone providers now offer nationwide urban area coverage and all are planning to expand coverage to rural areas. Additionally, 15 licensed ISPs and hundreds of privately run Internet cafes around the country now operate largely in urban areas with plans to expand to rural areas.

The private cellular companies operate on a pre-paid phone card basis where as Afghan Telecom has been operating on a centralized billing (post-paid) basis. This has proven to be problematic for Afghan Telecom due to an inadequate centralized billing system and a culture that believes government run services should be free. Afghan Telecom has acquired and commissioned a centralized billing system to improve revenue collection. As noted earlier, Afghan Telecom also plans to introduce pre-paid service as part of the CDMA-WLL and fixed line expansion initiative.

A National ICT Council of Afghanistan (NICTCA) has been created to facilitate coordination of ICT actions of all government sectors. With the creation of the NICTCA, the MCIT has taken on the role of the National Chief Information Officer (CIO) and the Ministry reps to the council the roles of Ministry CIOs. An Afghanistan Network Information Center (AFGNIC) was created to coordinate between different private and public organizations concerned with IT/ICT. Spectrum management and usage enforcement is a problem due to a lack of adequate monitoring capabilities—a mobile station for spectrum monitoring has been procured. Pirate cellular and ISP operations exist and the government hopes the new spectrum monitoring equipment will help them better manage spectrum use and eliminate pirate elements. Some illegal operators already have been discovered and their equipment has been confiscated and operations shut down.

Professional ICT societies have been established to improve social networking among the public and private elements. Organizations established include the Afghan Computer Science Association (ACSA), National ISP Association of Afghanistan (NISPA), and the National ICT Association of Afghanistan (NICTAA). A Kabul chapter of the Armed Forces Communications and Electronics Association (AFCEA) was established in June 2007 and will serve to further the improvement of military, public, and private social networking in the ICT area.

### **Community Radio**

Although not discussed in this paper, radio and television are other means to provide information services to the broader population. Initiatives to extend radio and TV throughout Afghanistan are being implemented. Like ICT, initial efforts have been focused on Kabul and other urban areas, and reaching people in remote areas remains a

challenge. For rural areas, where there is no power and the literacy rate is extremely low, radio offers an easy means to communicate useful information about healthcare; local, regional, national, and international news; the weather; educational opportunities; jobs and business opportunities; and government services. Most Afghans have access to radio receivers and are accustomed to using radio as a source of news, information, education, and entertainment.

A possible option to explore for the rural areas is community radio which is a radio station that is community-based, independent, and participatory. The station is based in its community and accountable to it. The legal owner is a local not-for-profit organization, such as an NGO, educational institution, cultural association, municipality, or a partnership of such associations. The station is independent of government, donors, advertisers, or other institutions but operates within the boundaries defined by law and by the constitution/guiding principles of the station. Community participation can be exercised in a wide variety of ways depending on the specific nature of the station, its objectives, and the characteristics of the community. On the whole, community radio is a low-cost and effective way of contributing to medium and long-term efforts for reconstruction, development, and nation-building.

Community radio is already in place in a number of rural Afghanistan areas. For example, in April 2006 one of the authors visited the Tangi Saidan Village Community Center, built by the NGO Morning Star Development, that has a medical clinic serving Afghan families in a rural area 40 miles south of Kabul. Part of this facility is a FM Radio Station that serves the 39 surrounding villages.

Efforts need to be accelerated to provide broader rural area access to radio-based information services, and expanding community radio is an approach to be considered.

### **Coordination and Information Sharing**

Certainly many good people are doing good things in Afghanistan, but the degree to which activities are harmonized, coordinated, and leveraged with information shared about their activities remains problematic. This is not a technology issue. It's a combination of people, policy, culture, and organization issues. Technology is an enabler; the international and USG civil-military crisis response community can (and should) do better.

There was (and still is) no clear mapping of responding stakeholder organizations, such as the U.S. Embassy, USAID, coalition military, International Security Assistance Force (ISAF), coalition civilian partners, IOs, NGOs, and the GOA roles and responsibilities, particularly in the area of ICT reconstruction and development. Figure 5 (see page 29) highlights the current conglomeration. No institutional arrangements or agreed ICT mechanisms and processes (including within USG civil-military elements) are in place for synchronizing and coordinating multinational (and national) actions and information sharing. ICT program development, project coordination, information sharing, and implementation are and continue to be loosely coordinated, ad hoc, and in some cases non-standard, especially across ICT support to Afghan ministries. Harmonization,

coordination, and information sharing is largely personality driven—the right persons at the right place and the right time with the right attitudes. Since the process is not institutionalized, every time there is a change of command, leadership, or personnel, the process starts all over again. This can happen as often as every six months to a year in both the civilian government agencies (U.S. Embassy and USAID) and military elements (PRTs and ISAF). IOs and NGOs also experience turnover challenges. Continuity of support activities and trust relationships built over time are key to success, and the current disruptive approach is not a good way to do business in a complex environment such as Afghanistan.

Given the military is driven by a culture of “plan we must” and the civilian community by one of “plan if we can,” there were (and still are) various versions of draft and approved plans developed by the U.S. Embassy, Combined Joint Task Force-76 (now CJTF-82), Combined Forces Command-Afghanistan (CFC-A, which no longer exists), Combined Security and Transition Command-Afghanistan (CSTC-A, formerly the Office of Military Cooperation-Afghanistan, OMC-A), ISAF, PRTs, USAID, UNDP, World Bank, NGOs, and others. There was (and still is) no agreed coherent, holistic plan and the degree to which the independent plans were (and are) coordinated and synchronized with Shared situation awareness differed among participants and, in general, was problematic (and still is). Coordination and information sharing among responders and with the Afghans remains a challenge. Even among the USG civilian and military participants, where various ad hoc mechanisms were employed to facilitate coordination and integration, there were interagency and personality related challenges, making it difficult to produce a coherent, holistic plan for reconstruction including the ability to share a common picture of civil-military reconstruction and development.

Although limited reconstruction situation awareness information was shared and tracked among participating civil-military elements, ICT was not one of the categories actively tracked or even recognized as important to track. Coalition civil-military emphasis was mainly on roads and to a lesser extent water and power. In contrast, the rural area Afghans’ needs were water then roads and power. This suggests some disconnect in the view of what is needed versus what should be provided by coalition reconstruction efforts. In fact, many locals were of the view that the coalition emphasis on roads was driven more by military operational requirements and logistics than the needs of the local community. The international civil-military community must do a better job of understanding the needs through the eyes of those being helped rather than what the community believes to be in their best interest. Obviously, some balance must be achieved.

The lack of standard formats for data poses significant hurdles to sharing. Free-form text documents make timely roll-up and data-mining efforts nearly impossible. Military data tends to be classified and the declassification process is a challenge. The lack of relational database management systems does not make it any easier—the military process tends to be slow and risk averse. When sharing works it tends to work largely due to the personalities of key personnel on the ground not by institutional policies, procedures, or ICT support capabilities, such as collaborative information environment

(CIEs), shared web portals, common geographic information system (GIS) databases, and shared civil-military SA tools.

Ad hoc approaches continue to be the means to an end to try to improve operations and actions on the ground. Afghanistan was (and to some extent still is) filled with: liaisons; coordination teams; special groups, such as the U.S. Embassy Afghanistan Reconstruction Group (ARG) that consisted of subject matter experts who reported to the State Department but were recruited by DOD from the American private sector; other special purpose USG elements at the U.S. Embassy in Kabul; and national reach back groups in the United States, such as the DOD Afghanistan Reachback Office (ARO) in the Pentagon. Multiple in-country civil and military liaisons took place between and among national and international elements and with Afghan Ministries and UN and USG sponsored subject matter experts who were embedded in the ministries. The MCIT, for example, had U.S. Embassy, USAID, and U.S. military advisors and liaisons as well as embedded subject matter experts, for example, USAID funded BearingPoint support to the MCIT and ATRA. There were multiple efforts to develop GIS based Afghanistan reconstruction SA tools and web portals. For example, the UN, USAID, ISAF, U.S. Army Corps of Engineers, and the office of the U.S. Assistant Secretary of Defense for Networks and Information Integration (ASD NII) were developing tools and/or web portals. Only the ASD NII effort was focused specifically on Afghanistan ICT.

One of the more successful USG in-country efforts to facilitate ICT coordination and information sharing in Afghanistan was the creation and staffing of the office of the Senior Telecom Advisor (STA) in the ARG. The first STA arrived in October 2005 and left in early October 2006. His replacement did not arrive until December 2006, creating a potential several month gap in Kabul office operations. In order to maintain continuity of operations and provide appropriate ICT focus and support to the MCIT and others in country during this time, ASD NII provided a subject matter expert in country to bridge the gap until the new STA arrived. There have been several subsequent extended ASD NII deployments to support the office of the STA over the last year and plans are in place to continue to help as appropriate.

A number of the first STA's initiatives to improve collaboration and information sharing are candidates for best practices for future operations as well as ongoing operations in Afghanistan. He was successful in getting the U.S. Ambassador to designate the STA position as the principal U.S. Embassy spokesperson for ICT matters and as the U.S. liaison responsible for dealing with the Afghanistan Minister of Communications. To create a cooperative environment, he established a U.S. integration team, referred to as the I-Team, which consisted of U.S. ICT representatives from the U.S. Embassy, USAID, and the U.S. military. Over time, the team was expanded to include ISAF, the GCN/DCN contractor GSI, and BearingPoint experts embedded in the MCIT and ATRA. I-Team meetings were held several times a month to share and coordinate ongoing ICT activities and discuss challenges and approaches to leveraging activities. Meetings were action-oriented and used as a means to inform, coordinate, and develop a shared agreement on initiatives to be pursued.

The STA established two U.S.-based reach back capabilities to build social networks to coordinate and share information on important ICT-related issues and actions and to seek advice, assistance, and best practices. One group supported USG-only activities and included the U.S. I-Team members, ASD NII, DOS, USAID, ARO, NDU, Army Corps of Engineers, and other U.S. government elements as appropriate in CONUS. This group held weekly teleconferences. A second group consisted of U.S. industry volunteers with an interest in helping Afghans and Afghan ICT be successful. They were engaged to seek advice and best practices as well as provide mentoring support for Afghans and related ICT initiatives. This group held a teleconference about once a month and the STA participated on an as appropriate basis.

The STA also led an effort to try to get the GOA to set up an I-Team led by the MCIT ICT directorate to bring together ICT reps from the MCIT, Afghan Telecom, MoD, Ministry of Foreign Affairs, and MoI to discuss ICT initiatives, share and coordinate ongoing activities, and discuss public and private sector, ANA, and ANP challenges, including emergency services ICT. It was envisioned that the USG and GOA I-Teams also would meet on some regular basis to coordinate and share information. The MCIT ICT directorate agreed to try to set up a GOA I-Team, but it never really happened.

The STA initiated an effort to establish a coherent USG ICT strategy and plan for supporting the MCIT ICT strategy and plans. Although some early success was achieved in starting to build a strategy and plan, the effort was not approved by the Ambassador as the framework and way ahead for selecting and implementing USG ICT initiatives. As a result, this remains an important gap in the USG strategy and plans supporting Afghan ICT evolution and capacity building—the process is still ad hoc.

The STA, in cooperation with ASD NII and U.S. Navy SPAWAR, set up an Afghanistan-ICT portal as a way to openly share ICT-related information and inform the community on related policy, technical, operational, and implementation activities, issues, and opportunities. It was to be a repository for all relevant ICT documentation and serve as an electronic library with links to other key web sites, such as the Afghan MCIT, ATRA, USAID, UN, and others. Chat room capabilities also were offered to facilitate collaboration and coordination among those in different geographic areas and time zones. Unfortunately, the portal never realized its expectations. Other independent databases, such as the USAID SharePoint reconstruction database, the UN Afghanistan Information Management System (AIMS), and the ISAF Afghanistan Country Stability Picture (ACSP) GIS database were established, but information was not actively shared on a regular basis and the databases were not electronically linked or held to common data standards. In early 2006, the U.S. Army Corp of Engineers was tasked by the U.S. Ambassador and U.S. military commander to develop a GIS-based Afghanistan common operational picture for reconstruction. This effort was subsequently rolled into the ISAF ACSP effort. None of the databases mentioned actively tracked ICT activities.

The current STA continues to try to sustain an effective in country civil-military CIE, but it is a challenge due to the large turnover of civilian and military personnel and the fact that the collaboration processes put in place by the first STA were not institutionalized. In

the absence of an agreed process, collaboration and information sharing becomes a function of having the right people at the right place at the right time and with the right attitude. It's a learning and trust building activity that gets repeated with every change over of civilian and military personnel. The current STA has continued weekly teleconferences with ASD NII and NDU and has initiated actions to strengthen the USG relationships with the MCIT and ATRA and U.S. Embassy relationships with USAID, U.S.-led ISAF, and the new CJTF-82.

The STA has the lead role for the international community support to the MCIT who has the lead responsibility for the ANDS telecommunications working group activities. This working group meets twice per month to review the MCIT ICT goals and results. The MCIT ANDS working group includes key MCIT managers, executives, and representatives of: ATRA, Afghan Ministry of Finance, USG Afghanistan Reconstruction Group (ARG) and U.S. Embassy Economic Section, Bearing Point, USAID, United Nations Assistance Mission in Afghanistan (UNAMA), UNDP, and other invited guests. The output of the working group is a document that outlines the MCIT's ICT Sector Strategy, which is presented to the GOA ANDS General Council for review and incorporation into the national goals and strategies.

The STA also has taken action to build a stronger ICT-oriented relationship with ISAF and the PRTs. In this regard, he meets with PRT reps (typically PRTs do not have an ICT expert, however, some members of the civil-military team have ICT skills) when they are in Kabul to discuss with them ICT-related opportunities in their area of interest. He has created a "Briefing Handbook on Afghan Civil Communications Systems" for their use and he also arranges meetings between the PRT reps when they are in Kabul and the MCIT, ATRA, and Afghan Telecom to discuss ICT opportunities and issues, such as the construction status of DCN buildings in their areas of interest.

The NATO-led ISAF IX implemented several initiatives to improve the civil-military response to reconstruction and to improve coordination and information sharing. Two Development Advisor positions (one from the UK (DfiD liaison) and one from the United States (USAID liaison)) were created to advise ISAF on reconstruction matters and they report to the Commander. As noted earlier, the ACSP was created and maintained by ISAF to share reconstruction SA status information with the civil-military community. ISAF scheduled a series of PRT conferences in Kabul to build a more informed and shared understanding of ongoing PRT reconstruction-related activities, needs, support opportunities, and activities among ISAF, the PRTs, other coalition military, national government elements, IOs, and NGOs. A PRT Handbook was created by ISAF and its development involved military as well as civilian elements. A PRT Executive Steering Committee was established to provide PRT policy guidance; pre-deployment PRT training courses were established; improved arrival orientation training was provided; and an ISAF PRT help desk and portal were created to facilitate ISAF response to PRT questions and needs. These are representative of many of the ISAF actions taken to improve PRT coherence.

PRTs also took actions to improve their ability to conduct reconstruction operations. For example, the Nangarhar PRT<sup>7</sup> developed a method of programming development funds at a sub-national level to positively affect a counterinsurgency in Eastern Afghanistan. A strategy for affecting stability through maximizing resources each agency brought to the table to create a “unity of effort” was developed along with an eight-step process of project development that culminated in the execution of a series of projects. The steps proposed included: Understanding the Strategic Framework; Operationalizing the Strategy; Determining Geographic Focus through Tribal Analysis; Defining Project Parameters; Conducting the Project Identification Process; Gaining Government Approval; Holding the PRT Project Nomination Board; and Implementation. The eight steps were developed by the command group (CG) of the PRT, which consisted of a representative from USAID, DOS, U.S. Department of Agriculture and the U.S. Army Civil Affairs.

### **Other Reconstruction Challenges**

Trust is an important element of the Afghan culture. Trust is earned over time but can be easily broken and much harder to re-earn. In Afghanistan, trust is earned through multiple visits and many long conversations with Afghan leaders that include discussions about beliefs, values, and family. All of this must be undertaken before entering into discussions about things that need to be done to help the local Afghans. Additionally, it is important to have a working understanding of the culture and it helps to be able to speak a little of the local language. One needs to be understood and accepted by the Afghans in order to do business. It’s sometimes referred to as the “three Chai tea” rule. You need to have at least three teas before starting to discuss business. Perception of power counts as well, and one needs to keep their word. The poor literacy rate in rural areas also can create special challenges for military and civilian reconstruction teams dealing with local leaders, warlords, and tribal leaders who may not be able to read or write but are shrewd operators. It is important to manage expectations: do not over expect Afghans’ ability to perform and likewise, don’t raise expectations of the Afghans if one is not sure of their ability to deliver.

A number of other factors create challenges for conducting civilian and military ICT-related reconstruction activities, particularly in high-threat areas. For example, military and civilian government personnel security protection rules add complications to conducting ICT reconstruction and development activities. The rules of engagement tend to be risk averse, leading to protecting the forces having a significantly higher priority than conducting reconstruction activities. The imbalance in the application of priorities can (and does at times) impact the ability to effectively execute reconstruction activities, especially in high-threat environments. Operational risks must be better managed. One consideration would be to give higher operational priority to conducting the reconstruction mission so that the military and civilian protection forces can more effectively balance force protection with reconstruction mission needs.

---

<sup>7</sup> Michelle Parker, “Programming Development Funds to Support a Counterinsurgency: A Case Study of Nangarhar, Afghanistan in 2006,” *Case Studies in National Security Transformation*, Number 10, Center for Technology and National Security Policy, available at <<http://www.ndu.edu/ctnsp/pubs/Case%2010%20-%20PRTs.pdf>>.

In the higher threat areas, PRTs were formed to create a safe and secure environment for conducting reconstruction operations. The teams combine military personnel and civilian staff from the diplomatic corps and developmental agencies and their mission is to extend the authority of the Afghan central government, promote and enhance security, and facilitate humanitarian relief and reconstruction operations. PRTs are provided by the United States as well as other nations under ISAF command, and the size, scope, and mission focus differ among national elements. Additionally, each PRT's composition and mission is tailored to meet its national rules of engagement and the requirements for security, political, and socio-economic dynamics in their area of responsibility. For example:

- A U.S. PRT consists of both military Civil Affairs and force protection personnel, civilians from USAID and/or DOS, and sometimes reps from U.S. Department of Agriculture and other USG elements as needed. The civil-military teams are based in heavily protected military compounds and they frequently travel by military convoy into their area of responsibility. The travel in the local area typically requires three up-armored High Mobility Multipurpose Wheeled Vehicles (Humvees) with military in full battle gear and weapons loaded. Civilians are required to wear body armor and helmets while in the Humvees. There are also locally hired armed protection teams that perform the roles of cultural specialist, interpreter, navigator, and hired gun. They travel in Toyota trucks and provide front and rear security protection for the military convoy. Dismounted operations include armed force protection teams.
- The German-led PRTs are precluded by the German Federal Parliament directives from taking on combat roles, and this has had an impact on their willingness and ability to escort aid and reconstruction workers in high-threat areas, thus affecting the capacity to conduct these activities. Additionally, the German-led PRTs maintain a strict division of responsibility between the military and civilian components. They function more as a “secure guest house” for the civilian specialists.

In high-threat environments, contact with the local population is often of short duration and limited in many cases to key local leaders. The short visits with local leaders can make it hard to build trust relationships and conduct business. Hence, assessing shortfalls and needs, conducting reconstruction activities, and building trust relationships with the local Afghan people and leaders is a constant struggle under such conditions, especially for the civilian elements.

Even in a lower threat environment (but still a wartime environment), such as Kabul and its surrounding area, conducting civilian reconstruction related activities is a challenge. U.S. military and civilians are restricted to living and working on protected compounds within a security zone. Civilian travel outside of the compound and within the city limits must be scheduled and is by armored vehicles with an unarmed local hire Afghan driver and no force protection personnel. Travel is only allowed to and from destination meeting

points within the city limits, and unescorted walking around the city is not permitted. Travel outside of the Kabul city limits must be approved by the U.S. Embassy Regional Security Officer (RSO), and armed security details are provided by Diplomatic Security personnel, private security contractors, or the military. Civilians must wear body armor and helmets while traveling in vehicles outside of Kabul city limits. During trips outside of the city, walking around a town or village with the personal security detail is permitted, including spending time talking with local leaders, shop owners, and the local population.

In response to an incident, such as the detonation of a bomb or a rocket attack, or increased threat warning levels, the protected compounds (both in Kabul and at PRT locations) often go into “lock down” for hours. Depending on the seriousness of the situation, travel outside of the compound can be restricted for days to essential mission need personnel only—this was experienced by one of the authors during his visit to Afghanistan. Following a riot in Kabul at the end of May 2006, the U.S. Embassy and ISAF compounds were in lock down for several hours. Additionally, for several days after the incident, only essential personnel were allowed off the U.S. Embassy/USAID compound. These actions not only impact the ability to conduct business with the Afghans but also can impact the morale of the personnel, especially the civilians.

The continuing threat conditions also can create morale problems and reluctance on the part of some civilian elements—largely driven by personal security concerns—to travel outside of the protected compounds. Trips are often limited to within the city limits and few trips are taken to the local countryside or to the PRTs. In fact, some civilians have been known to spend their full tour of duty on the U.S. Embassy/USAID compound in Kabul, only leaving this area to go to the U.S. military base, Camp Eggers, which is also located within the security zone of U.S. elements in Kabul, for the local Afghan crafts bazaar held each Friday.

Afghans can be invited to come into the protected compounds to conduct business, but this, too, can be a challenge. In Kabul, Afghans can be invited to visit U.S. Embassy/USAID and military personnel, and many come to the compound for meetings. There are, however, very restrictive search procedures that can be offensive to some Afghans, and hence, a number refuse to come for visits or meetings. In the higher threat areas, local leaders can access the military compounds to visit PRTs but such visits also can be problematic. Restrictive search procedures that include the disarming of bodyguards are offensive to some Afghan leaders and they refuse to come for visits. For others, this is not a problem. For example, during one of the authors visit to the Khost PRT, the provincial governor visited the PRT commander at his office on the military compound once a week, and other key personnel, such as the Director of Education also made frequent visits. Yet other local leaders would not come on the compound. As a result, it can be a challenge to effectively conduct meetings and build trust relationships with key officials and business leaders both in Kabul and in the high-threat areas.

## **ICT-Related Lessons from Afghanistan**

---

Significant progress has been made in the Telecommunications and IT sector in Afghanistan, and it has truly been the “success story” emerging out of the recovery of a country left dysfunctional from 23 years of war. Progress towards bridging the digital divide and moving Afghanistan into the 21<sup>st</sup> century information age has not been accidental but is largely due to having the right people at the right place with the right vision, energy, and expertise to make reasonable decisions and take actions to make things happen.

Afghanistan ICT success was and continues to be enabled by a number of factors:

- A GOA understanding of the importance of ICT as an engine of economic development and its role as an enabler of cross-sector reconstruction
- Early GOA establishment of ICT policies, regulations, laws, and a regulatory authority
- Knowledgeable and experienced Minister of Communication (now Communications and Information Technology)
- MCIT vision, strategy, and plan for moving Afghanistan ICT into the 21<sup>st</sup> century information age supported at the highest level of government, President Hamid Karzai
- Establishment of a good public-private partnership that enabled private ICT investments and rapid growth of their networks
- International and USG community support
  - Placed early emphasis on ICT capacity building, including the establishment of related educational institutions, training facilities, and capabilities
  - Willingness to invest in and support Afghan MCIT creation of a national telecommunications and IT network

The U.S. Army Center for Lessons Learned some years ago made the observation that lessons are learned when behavior changes. Opportunities to change the international and USG intervener community behavior and approaches to ICT reconstruction and development remain. Some key areas where changes need to be made are as follows:

- Policy actions
  - Recognize ICT as an engine of economic development
  - Agree on importance of telecoms and IT as an enabler of cross sector reconstruction and development
  - Elevate ICT investment priorities to be equivalent to roads, power, and water
  - Ensure “political will” to coordinate and share ICT-related reconstruction and development information
- Strategies and plans
  - Improve understanding of affected-nation information and related ICT business cultures
  - Develop agreed coherent community strategies and plans for supporting and enabling affected-nation ICT reconstruction and development strategy and plans
  - Improve management of the risks of protecting civilian and military elements and implementing reconstruction initiatives.
- Collaboration and information sharing
  - Agree on mechanisms and processes to facilitate coordination and information sharing, including a shared SA of reconstruction and development activities, especially for ICT
  - Institutionalize agreed process
  - Agree to implement shared ICT capability packages that enable and facilitate collaboration and information sharing

## The Way Ahead

---

Much remains to be done to make Afghanistan ICT a viable and robust network to effectively support civil security, governance, economic growth, healthcare, and education. A discussion of gaps and shortfalls and some thoughts on actions that could be taken to overcome them and help realize the network's full potential follows.

The Afghan ICT network is fragile but growing and becoming more robust. ICT capacity building has started but much remains to be done. International and USG ICT-related support activities are fragmented and not well coordinated. For example:

- The telecom network has limitations in effectively supporting emergency response services. During riots in Kabul at the end of May 2006, the cellular network was overloaded, which impacted the ability of first responders and others to make calls during the crisis.
- ICT infrastructure and processes are not adequately protected against cyber and physical threats.
- Nationwide coverage, service quality, and capacity has been marginal but improving with increased competition. Cost of services was high to start with but has been coming down. The growth of DCN for public access and extension of GCN for governance has been slow.
- Data services and access are inadequate to support e-Solutions. There is a shortfall in broader community access to the Internet. MCIT and ATRA have plans to offer expanded, nationwide, fixed and wireless data services as well as expanded community access to the Internet including rural areas.
- Rural area information and ICT service needs remain unmet by public and private ICT investments.
- Cyber security is a major problem: the GOA lacks adequate virus and spyware protection, intrusion detection-protection, and firewalls. The government is unable to effectively control use of pirated software and hardware. Within government ministries, inappropriate surfing of the Internet introduces viruses and spyware that corrupt network operations. There are no cyber laws or enforcement mechanisms. A Computer Emergency Response Team (CERT) is planned but not implemented.
- Most Afghan ministries have minimal IT organizations and implementation of internal IT capabilities and services are uncoordinated and non-standard. There is a lack of a "CIO Culture" with agreed cross-ministry business processes,

standards, and best practices. There is also a lack of an “Information Security Culture.”

- A thin layer of ICT competence and skills is present in the workforce of the Government elements and related Ministries. The MCIT, with the help of USAID, the UN, and others, is taking action to establish ICT training facilities for its staff.
- Reliable power is lacking for ICT. Current solutions do not employ energy saving ICT options such as the use of low power IT equipment and power saving procedures. A mix of alternative power sources must be encouraged, such as expansion of the national grid, solar, generators, small wind, micro-hydro, and batteries.
- There is no agreed, coherent international (or USG) strategy and approach for supporting Afghan ICT reconstruction, development, and capacity building. There are independent and loosely connected activities, such as U.S. military funding of the PGCN and solar power for DCN nodes and USAID funding of selective DCN initiatives. The USAID Afghans Building Capacity (ABC) program includes initiatives related to ICT capacity building and these are loosely connected with UN and NGO related ICT capacity building initiatives.

The international community, and the USG in particular, needs to take a leadership role to promote support of the Afghan ICT evolution and protect its ability to sustain capabilities already realized. To do this, as a minimum, there is an urgent need to create a coherent USG investment strategy and plan that supports the GOA intention to use ICT to create jobs, enable economic activity in all sectors, and improve governance, civil security, education, healthcare, and social well-being in general. Some specific actions to be considered by the GOA, USG, and international community are as follows:

- Security and governance certainly needs to be high on the priority of ICT opportunities and capability packages to be considered for implementation.
- An ICT support strategy and plan should be developed for emergency response command and control and emergency services ICT support (police, fire, hospital, rescue). Specific plans to be considered are a U.S.-like National Response Plan, a supporting ICT strategy and plan, and Critical ICT infrastructure protection strategy and plan.
- MCIT, MoD, MoFA, and MoI need to create an ICT-based CIE to facilitate coordination and information sharing of their ICT initiatives related to improving ICT support to emergency services and security needs.
- The USG needs to actively pursue enabling (including sources committed to funding) the implementation of the remaining 22 PGCN capability packages to support extension of effective governance to the provincial governor level.

- Actions need to be taken to extend GCN services to key ANA and ANP elements to help improve security and emergency response communications.
- DCN implementation needs to be accelerated and services pushed out to key local district government officials as a means to increase the reach of civil security and governance to the district level and to extend access to ICT services and government services for the broader population.
- To more effectively respond to and support emergency services needs, consideration should be given to:
  - Accommodating embedded emergency services in the cellular network by introducing priority access and call set up for first responders and key decision makers.
  - Investing in crisis response and ICT recovery and restoration needs, such as network operations tools to accommodate surge capacity and recovery management and deployable emergency ICT capability packages to accommodate network access, coverage and recovery management.
- MCIT should develop a strategy, architecture, and enhancement plan for a robust, national, long-distance network and backbone infrastructure to enhance Afghan ICT coverage, access, services, and performance. The following steps would assist:
  - Consider creating a virtual backbone transmission infrastructure and implementation of network operations tools and platforms to facilitate provisioning, managing services, fault recovery and reconstitution, and usage mediation and service billing management.
  - Improve GCN/DCN network robustness, capacity, coverage, services, and marketing (DCN franchises) as a means to make GCN/DCN an effective provider of security, governance, and other network services as well as a sustainable and financially viable business.
  - Develop new initiatives to enable and enhance public and private data service offerings nationwide and to enhance regional and international access and capacity to better position Afghanistan for access to and participation in the global market economic environment.
  - Explore early introduction of e-Commerce solutions and mobile commerce, such as Internet banking, G-Cash/e-Wallet, and M-PESA on cell networks to accommodate remittance transfer service which enables mobile phone subscribers to transfer money to other mobile users via SMS text messaging.

- Results of a Vodafone pilot program are currently being discussed among ATRA, USAID, cellular providers, and Afghan National Bank for possible implementation.
    - Internet Banking services to improve financial transactions are being explored as well.
    - Licensing electronic funds transfer arrangements will revolutionize economic and social recovery, especially in high-threat environments and areas where access to banking services does not exist.
  - Encourage USG, ISAF, and other interveners to selectively invest in Afghan ICT enhancements to provide coverage and capacity in areas to support their operational needs then lease back services rather than build their own systems.
- As part of enhanced capacity building, Afghan ICT needs to be used to:
  - Support literacy and community empowerment. This can be done by providing access to the following:
    - USAID, UN-Habitat and Ministry of Education programs for reading, writing, and interpersonal and other life skills
    - USAID and Ministries of Women’s Affairs, Health, and Education “Learning for Life” program to improve reading, writing, health, and hygiene skills
    - Computers, video, CD players, commercially available DVDs, educational video tapes, CDs, and Interactive electronic books, such as the International Medical Corps “Family Health Notebook.”
    - Telekiosks and community centers with Internet access and related capabilities
    - Distance learning for education and training
      - Computers, English language, business practices, health care, family health, and medical advice
      - Internet portals for education, health care, and medical advice
  - Enable Internet access for schools and universities.

- Support provision of ICT enabling infrastructure to wire up schools and universities and offer access to Internet
- Provide wired and wireless local area networks on campus with access to Internet that uses both public and private ICT for voice, data, and Internet access
- Make available e-Learning and e-Education capabilities and tools
- Offer access to up-to-date teacher training material
- Develop centers for teaching and learning
- Open up opportunities for distance learning, such as English language training, computer skills, use of ICT, and e-Solutions training
  - Use the Internet to link universities within Afghanistan and with universities outside of Afghanistan and provide opportunities for:
    - Partnership programs and alliances
    - e-Learning, e-Education, e-Library
    - Access to Centers of Excellence and subject matter experts
- Enable Internet access for healthcare and hospitals
  - Wire up hospitals and healthcare centers and provide medical software
  - Provide software for medical diagnostics, administration, pharmacy, and patient records systems
  - Provide ICT connectivity and Internet access to
    - Link Medical schools with hospitals and healthcare centers
    - Link hospitals with healthcare centers
    - Link hospitals and health care centers with international centers of excellence and subject matter experts
    - Offer e-Training, e-Learning, e-Diagnostics, e-Healthcare, and e-Reference

- Establish alliances with medical schools, facilities and experts outside of Afghanistan, and
  - Healthcare web portals, on-line Medical diagnostic tools, and medical and related subject matter experts
- Efforts need to be accelerated to provide rural area access to ICT services. In this regard, mobile communications can revolutionize economic and social development in rural areas and Internet can be used to educate and help improve literacy. Making information more widely available also can help eliminate abuse by making government more accountable, improving legitimacy, and reducing corruption. Consideration needs to be given to actions, such as:
  - Funding a pilot program for ICT capability package options for the VCN;
  - Supporting investments in community provisioning of towers to encourage cell phone providers to extend services to rural areas;
  - Developing private-sector incentives for expanded LFSP licenses that target the rural areas;
  - Expanding cell network coverage to rural areas;
  - Implementing a pilot DCN franchise targeting expanded coverage to rural areas; and
  - Provisioning micro-financed loans for VCN-like capabilities.
- The GOA should be encouraged, and the USG prepared to help, to enable an early introduction of a CIO-like culture and e-Government capabilities into the ministries.
- The NICTCA must be leveraged and the MCIT in its role as National CIO needs to enable more effective government use of IT with the following actions:
  - Standardize ICT capabilities across ministries;
  - Coordinate cross-ministries ICT investments;
  - Standardize business processes including application of e-Government-like solutions;
  - Prioritize ICT spending to support anti-corruption goals;

- Oversee and advise on cross-ministries ICT processes that support data sharing and audits of software via development or purchase and use of the National Data Center;
- Enable “CIO” capacity building through cooperative efforts with educational institutions, such as the NDU Information Resource Management College (IRMC) CIO education and training programs and ICT and eServices capacity building through alliances with universities around the world; and,
- Automate government business functions and processes and extend and improve GOA provided services to the population to establish transparency and legitimacy and reduce corruption.
- Develop and implement a National Cyber Security Strategy and Plan that includes actions such as:
  - Creating a cyber information security culture;
  - Assigning Information Security Officers in Ministries and key government agencies;
  - Initiating training and awareness programs;
  - Establishing an Afghan CERT with a national cyber-security management structure;
  - Adopting cyber-security laws, regulations, standards, and policies and implementing enforcement mechanisms;
  - Defining the cyber security organizations;
  - Adopting a prioritized, defense-in-depth strategy; and,
  - Implementing Cyber-Security Plans, to include:
    - Public-private cooperative arrangements, and
    - Key asset protection (infrastructure, people, and electronic)

## Conclusion

---

Study findings suggest that ICT has been an enabler for developing the Afghan government, economy, and social well-being. While there have been successes, challenges remain. Continued smart investments and use of information and ICT will serve to further enhance government capacity, legitimacy, and transparency, help reduce corruption, increase economic growth, and support social stability. Information is power and the generator of stability for countries undergoing stabilization and reconstruction—the theme of the NDU CTNSP I-Power study. It is certainly a key to being successful in Afghanistan.

A word of caution must be issued, however, now that the ICT sector in Afghanistan has been relatively successful and appears to be operating reasonably well on its own initiative, there may be a desire on the part of international elements, coalition military, and the USG to shift support to other sectors that have not been as successful. Such a shift without careful consideration of not only first order but second and third order effects could have significant unintended consequences, especially if the ICT sector is not yet prepared to truly sustain operations on its own without the support and attention of the international community. Consideration of such a shift in international and USG support needs to be carefully assessed, monitored, and managed over time to ensure informed choices and decision are made and that progress continues to bridge the digital divide and move Afghanistan into the information society of the 21<sup>st</sup> century.

## References

---

Afghanistan Country Report: Telecommunications, Afghanistan Ministry of Communications, April 2005.

Afghanistan Five Years Later: What Can the United States Do To Help?, U.S. Institute of Peace, November 2006.

Afghanistan Ministry of Communications Five-Year Development Plan, 25 July 2005.

Afghanistan National Development Strategy (ANDS), 2005.

Afghanistan Telecommunications and Internet Policy, November 2003.

Afghanistan Telecom Brief, Ken Zita, April 2004.

Afghanistan—Telecoms Market Overview and Statistics, Paul Budde Communication Pty Ltd, 2006.

*An ICT Primer, ICT for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction*, Larry Wentz, Defense and Technology Paper 31, Center for Technology and National Security Policy National Defense University, July 2006.

Asia-Pacific Telecommunity Yearbook 2005, Afghanistan country profile.

Assessment of Wireless Telecommunications Trends and Technologies in Kabul, Afghanistan, ANSER, March 2004.

Briefing Handbook Afghan Civil Communications Systems, Afghanistan Reconstruction Group, U.S. Department of State, James Baker, Senior Telecom Advisor U.S. Embassy Kabul, draft May 2007.

Building Peace Through Information and Communications Technologies, U.S. Institute of Peace, June 2007.

Countering Afghanistan's Insurgency: No Quick Fixes, International Crisis Group, Asia Report No. 123, 2 November 2006.

Creating a Development Dynamic, Final Report of the Digital Opportunities Initiative, Accenture, Markle Foundation and UNDP, New York, 2001.

District Communications Network (DCN) Franchisee Business Case Preliminary Recommendation for the MCIT, Alan Chelko, USAID Contractor, September 2006.

Information and Communications Technology Policy for Afghanistan, Final Report, Asia-Pacific Development Information Programme, UN Development Programme, October 2002.

*I-Power: Using the Information Revolution for Success in Stability Operations*, Frank Kramer, Stuart Starr, and Larry Wentz, *Defense Horizons* 55, Center for Technology and National Security Policy National Defense University, January 2007.

Ministry Sector Strategy (MCIT -ANDS WG), February 2007.

Summary of Achievements, Afghanistan Ministry of Communications Pamphlet, 2006.

Supporting Afghanistan Reconstruction Through ICT: Challenges and Opportunities briefing, Frank Kramer and Larry Wentz, Center for Technology and National Security Policy National Defense University, December 2006.

Telecom & Information Technology Briefing – FAQs USAID FPOs at ISAF PRT Conference May 2007, ATRA.

The Afghanistan Compact, February 2006.

Transforming Telecoms in Afghanistan, GRIDLINES, PPIAF/World Bank, April 2006.

World Telecommunications/ICT Development Report 2006, International telecommunications Union, March 2006.