Deployed Communications in an Austere Environment

A Delphi Study

Capt Andrew Soine, USAF
MSgt James Harker, USAF
Dr. Alan R. Heminger
Col Joseph H. Scherrer, USAF

The information and communications technology (ICT) field is undergoing a period of tremendous change. The exponential growth rate of ICT capability in recent decades, which has had an undeniable effect on every aspect of our society, will likely have ramifications for military operations in austere environments.[1] The Air Force's 689th Combat Communications Wing commissioned a study to forecast the future of mobile ICT in such environments. Researchers at the Air Force Institute of Technology chose to employ the Delphi technique as the methodology for executing this task. The following scenario, based on the results of that study, demonstrates how possible changes in ICT might affect military operations. The article then discusses relevant issues that one would need to address before such possibilities become reality.

The Scenario: Sometime during the Next 10 to 20 Years in a Country Wracked by Natural Disaster and Sectarian Strife

The stealthy remotely piloted aircraft (RPA) streaked silently over the valley. If Senior Master Sergeant Riley had blinked, he would have missed it, but he was expecting the aircraft. The sergeant watched in anticipation as the pointed, narrow cylinder dropped from an opening in the bottom of the platform. The attack drone veered and accelerated towards the north, vanishing before its payload hit the ground.

With perfect precision, the cylinder (not standard ordnance but a radio frequency–satellite communications [RF-SATCOM] network link) hit its mark—the top of the tallest mountain overlooking the valley. This new device supplied cell-phone-like connectivity to each Soldier throughout the area of operations, along with back-haul connectivity to the rest of the Department of Defense's worldwide communications network. Riley had used the backup system to enter the request only 20 minutes ago, employing a series of linked drones to send a message to the larger staging area about 400 kilometers due north. His team was responsible for securing this valley and setting up the communications infrastructure in preparation for arrival of the main force, which would conduct humanitarian-relief efforts for the local population. The latter had suffered from disastrous flooding and landslides brought about by a stronger than normal monsoon season.

A light began blinking on the small device strapped to Sergeant Riley's forearm as he walked back into the tent.

"We're back up," said Airman First Class Biggs.

"Good. Where are they?"

"About 15 kilometers to the east. Everyone's vitals are within normal, no injuries. Staff Sergeant Ramirez reports that somebody tried to take a shot but turned tail when they returned the favor. They're resuming their patrol. I'll mark it." Airman Biggs hit a few buttons on his terminal. A moment later, a chorus of beeps arose from inside the tent as everyone's armband announced to its wearer the alert and subsequent map update. Fifteen kilometers way, Ramirez hit a few keystrokes on his armband. A mortar tube automatically pivoted towards the marked sector should its services be needed.

Riley sighed in relief. The scout patrol had recently reported that it had taken some harassing fire, and then as if on cue, the primary network went down. Several warlords in this part of the country weren't thrilled about their presence, so someone had remotely hacked into the network and introduced a virus that attacked friendly tactical systems. The intelligent security systems had detected the intrusion and deployed countermeasures but not before the primary intratheater link went down. Though internationally banned, those types of technologies somehow still showed up in environments such as these. Riley grinned, wondering if his adversary had his device in his pocket when it suddenly overheated and caught fire.

"Sergeant Riley, Ramirez says his helmet cam caught a glimpse of one of the attackers, but I doubt that these guys are in the system at Langley. I saw this improved 'hostile or friendly' app on the net earlier. What we've got is tied only to the known hostiles in the system, but this new one can match the pic from Ramirez with anybody in view. If somebody crosses paths with him again, like in the village market, it'll 'paint' him," offered Biggs.

"Nice. If it's got more than three out of four stars, go ahead and pull it down," replied Riley. The online toolbox was a lifesaver, literally. Troops in the field who needed a new capability for any particular situation—or who already had one but needed an upgrade—could just download it from the secure repository practically anywhere on the planet. They could even rate it as a good app or a dud. Riley looked back at Airman Biggs and tried to remember being so young. Biggs really knew his way around this technology stuff, as was usually the case with the younger troops. Obviously a generational thing, they all grew up just expecting it to be there and ready to use. He probably wouldn't even recognize the Air Force that Riley knew when he was that age: hauling around all that comm equipment that usually did only one thing and oftentimes not all that well; bulky, fuel-hungry generators that advertised your exact location to every jerk with an AK-47 within 100 kilometers; the mountains of batteries that you had to bring in and carry around. . . .

A voice emanating from his armband brought him back to the present. “Sergeant Riley, what’s your status?” It was Major Hanson. Located at the staging area, he was conducting final preparations for deployment of the main force.

“Sir, we’ve had a few hiccups, but nothing serious. We’re on schedule, and the equipment is almost ready,” Riley responded.

“Brilliant. We’re bringing a few extra teams for security. Will that be an issue?”

“Shouldn’t be, but it might be a good idea to throw on a couple of extra gateways to increase our bandwidth, just in case.” You can never have too much bandwidth, even out here. “A few extra teams” had a wide interpretation; too many heads might start dragging down the local network. Having some cushion ready to go would be nice. Maybe he should ask for another solar power supply as well—after all, they don’t take up much room.

While Riley updated the major, the network autonomously uploaded a profile of the attack to the main system at Langley. There, it would analyze the data and push out a patch with updated security algorithms. The entire theater would have immunity within the hour.

Behind the Scenario

This story sounds like something out of science fiction. However, according to the Delphi panel that offered input for this research, the technologies it describes may be in place within the next 10 to 20 years—in some cases, perhaps even sooner. A research methodology, the Delphi technique forecasts future possibilities based on expert knowledge of areas relevant to the study.[2] This method “has become a fundamental tool for those in the area of technological forecasting.”[3] In fact, many researchers advocate it for research involving subjects for which a previous datum is unavailable or nonexistent.[4] R. C. Oliver and his colleagues also confirm that “Delphi is best suited for evaluating the alternatives of some definable although not necessarily narrow issue . . . in which the experience of experts is of particular value."[5] Finally, Somnath Mishra, S. G. Deshmukh, and Prem Vrat's analysis to match forecasting techniques with specific technologies found the Delphi method a particularly good fit for studies related to information technology.[6]

The National Defense University has presented four major categories of the ICT industry: hardware, software, information services, and communications. It further divides these categories into sectors such as cable, telecommunications, manufacturing, cellular phones, software, computer and networking hardware, the Internet, data storage, and associated services and applications.[7] In the context of its report, the university developed these categories to capture the state of the ICT industry as it presently exists. However, research for this article attempted to address the predicted capabilities of ICT in future states. Certain knowledge areas that would prove useful in generating a forecast—such as trends, revolutionary concepts, and both basic and applied inquiry—did not seem well represented in the existing categories as defined. Therefore, researchers at the Air Force Institute of Technology first examined major categories of the ICT field and derived five general knowledge areas more practical for forecasting future capabilities: concept design and demand, research and intellectual aspects, technology development, application, and, ultimately, employment.

No firm agreement exists on the number of panelists necessary for an effective Delphi.[8] On the one hand, Albert P. C. Chan and his colleagues find 10 members an adequate number of panelists to represent a sufficiently wide distribution of opinion.[9] On the other hand, some studies show no consistent relationship between panel size and effectiveness.[10] Regarding the minimum number of panelists, Jacques Etienne Des Marchais indicates a minimum of six.[11] Further, David Boje and J. Keith Murnighan found no effect for group sizes of three, seven, and 11.[12]

Using the Internet, academic journals, and social networking, the research team developed a list of 100 potential panelists across the five knowledge areas from organizations including academe, non–Air Force governmental organizations, and the private sector. These individuals represented a wide spectrum of involvement within the ICT industry, including concept development, research and development, technology development, application, and the employment of technology. After prioritizing the list with the sponsoring agency, the research team contacted the 25 most desirable candidates, securing the participation of eight experts.

Critics of Delphi cite the difficulty of defining those criteria that make someone an expert. For the purposes of this article, we use V. W. Mitchell's definition of an expert as one who has had a significant amount of involvement within the industry, both past and present.[13] Many studies recommend a minimum of five years of specific experience in the particular industry, which we used as the defining factor of expertise within the ICT industry.[14] All participants have between 20 and 40 years of experience in their field.

Participants on the Delphi panel included a board member of the Association of Professional Futurists who has coauthored books on the future of technology; a program manager in the area of defense electronics, communications, and signal processing; an associate professor of systems engineering specializing in information operations, mission assurance, computer and network security, quantum cryptography and information, and mission-impact assessment; a director of business development and sales for a major satellite communications group, specializing in deployable communications; a practice leader specializing in telecommunications, innovation science, and operations management who has worked at major research facilities; a chief software architect and development lead at a technology consulting group; a disaster-communications engineer at a major networking corporation; and a federal government professional in emergency response to information-technology disasters.

Although the scenario is based on the forecast developed by the Delphi panel, the latter did not create it. Rather, the authors developed the scenario to illustrate how the ideas presented in the forecast could affect the use of deployed communications in the near future. The following discussion explores issues included in the scenario that highlight changes we may expect to see in such communications during the coming years.

Bandwidth

The RF-SATCOM network link dropped from the RPA signifies one of the trends among the panelists' forecasts. As ICT evolves, despite evolutions in protocols and data-compression techniques, bandwidth requirements will continue to grow—possibly at an exponential rate. The panelists suggested that the increase in bandwidth needs stems from expanded data exchange among robots, sensors, RPAs, and personal ICT devices such as smartphones and tablets. Therefore, as we move into future engagements, the availability of usable bandwidth providing gateways to access the Global Information Grid (GIG) will escalate dramatically. The ability simply to "deploy" a unit similar to the RF-SATCOM network link in an unforgiving environment as a means of facilitating near-instant accessibility to data exchange will likely increase virtually all aspects of the campaign it supports, whether a humanitarian-relief effort in Haiti or terrorist suppression in Africa.

Satellites versus Alternatives

The experts had divergent views on how deployed communications systems would link back to the GIG. The scenario uses both projected technologies. First, the self-configuring RF-SATCOM network link acts as a gateway to the GIG, providing wireless RF connectivity to authorized devices within the area of operations. As described by the panelists, some austere locations create great difficulties for a direct satellite link. For instance, locations under high foliage, such as a jungle environment, as well as those inside hardened shelters and under water render satellites less effective. Other panelists envisioned highly mobile data links in the form of RPA relay systems. In the scenario, Sergeant Riley uses this as a temporary communications medium to request the more robust satellite-link back-haul system.

Personal Information and Communications Technology

As devices and applications converge into smaller, faster, and cheaper individual computing devices, their interfaces will evolve. The interaction will become more fluid as the interfacing experience begins to transform to sensory inputs, biological queues, and eventually human-enhancement implants. Sergeant Ramirez communicates with Airman Biggs with a device similar to current smartphones, but it also monitors his vitals via a few nonintrusive biological sensors capable of immediately alerting both the wearer and nearby allied forces if any readings fall outside a predetermined threshold. Additionally, thanks to the fact that the RF-SATCOM network link offers local device-to-device communications, the dissemination of mission-critical information and supporting data now takes place in real time—as occurred when Airman Biggs sent an alert and map update throughout the unit. This update warns friendly forces about hostiles nearby and allows Sergeant Ramirez to coordinate retaliatory fire from isolated locations, enhancing both his unit's safety and combat effectiveness. The sergeant captures and processes photos, using them to query and update the remote database. This ability signifies two possibilities. First, it underscores the necessity of global connectivity to send data to troops in rugged locations. Second, it illustrates possible advantages of an application repository providing real-time access and updates to mission-support software. According to the panelists, multiple commercial entities have already successfully implemented similar corporate repositories.

Power

The panelists also considered the powering of ICT devices, identifying power generation, storage, and distribution as areas of concern. In the scenario, Sergeant Riley reminisces about deployed forces relying exclusively on petroleum-based power generation and replaceable batteries. The panelists forecast that power generation will slowly change from current methods to technologies such as fuel cells and locally developed power that uses renewable methods such as wind, water, and sunlight. Such renewability is beneficial from more than simply an environmental standpoint. Currently, the power needed to run a forward operating base demands many fuel generators, which leave a large footprint. Additionally, the fact that generators require fuel and maintenance adds to the logistics burden. Local renewable energy sources would drastically reduce the number of support personnel and demands for supply. Power storage and distribution converged in this scenario when the sergeant thought to request another solar power supply. Panelists suggested that the incremental battery improvements, combined with personal ICT evolution that lowers power consumption, will extend ICT battery life substantially. Members of the panel suggested wireless power distribution but acknowledged that it might not be feasible in the near-to-moderate future due to radio interference and health-related risks.

Security

The panelists forecast that as our networks become more modular and based on Internet protocol, devices would become more autonomous—witness the part of the scenario when the network pushes the attack profile to Langley for automated analysis and creation of a security patch. However, some panelists cautioned that because these modular network devices may be engineered, manufactured, and programmed for autonomy outside the Department of Defense, one must consider possible security risks akin to "backdoor computing" (bypassing normal authentication and thus securing illegal remote access to a computer). The panelists concurred that data security will be a concern in the distant future. As ICT evolves, so will malicious attackers; furthermore, as personal ICT proliferates, becoming less expensive and more ubiquitous, the pool of potential attackers will grow in step with it.

The Way Ahead

It seems naïve to assume that humankind will continue to conduct traditional warfare even as ICT developments prompt new operational capabilities and demands. Instead, we should attempt to envision how the latter will improve operations. Commentary from the eight experienced ICT industry experts yielded the common trends identified and discussed above. Bandwidth requirements will increase rapidly, and back-haul systems linking forward operating locations to the GIG will develop. Satellite capabilities will multiply, just as alternatives and RPA-relayed mediums will emerge. Personal ICT devices will progress and proliferate. The convergence of applications and data services on these devices will decrease the number of tasks that they cannot perform. As power techniques develop, a "charged" device will operate substantially longer before depleting its power source. In terms of security, human nature creates a continuous, reciprocal battle of measure/countermeasure/countercountermeasure, and so forth. An interesting perspective to consider is that the forecasts we used to produce this scenario did not specify particular developments or actual capabilities; rather, they identified distinct trends and likely paths of ICT evolution. Through this perspective we can apply these trends not as a specified plan of action but as a planning tool designed to gain and maintain adversarial advantages. As President Dwight D. Eisenhower declared, "Plans are nothing; planning is everything." ✪

Notes

[1] Richard E. Albright, "What Can Past Technology Forecasts Tell Us About the Future?," *Technological Forecasting and Social Change* 69, no. 5 (June 2002): 455; Heebyung Koh and Christopher L. Magee, "A Functional Approach for Studying Technological Progress: Application to Information Technology," *Technological Forecasting and Social Change* 73, no. 9 (November 2006): 1071; Christopher L. Magee and Tessaleno C. Devezas, "How Many Singularities Are Near and How Will They Disrupt Human History?," *Technological Forecasting and Social Change* 78, no. 8 (October 2011): 1368; Luiz C. M. Miranda and Carlos A. S. Lima, "Trends and Cycles of the Internet Evolution and Worldwide Impacts," *Technological Forecast-*

ing and Social Change 79, no. 4 (May 2012): 744–65; and Béla Nagy et al., "Superexponential Long-Term Trends in Information Technology," *Technological Forecasting and Social Change* 78, no. 8 (October 2011): 1356–64.

2. Norman Dalkey and Olaf Helmer, *An Experimental Application of the Delphi Method to the Use of Experts*, Memorandum RM-727/1-Abridged (Santa Monica, CA: RAND Corporation, July 1962), http://www.rand.org/content/dam/rand/pubs/research_memoranda/2009/RM727.1.pdf; and Norman C. Dalkey, *The Delphi Method: An Experimental Study of Group Opinion*, RM-5888-PR (Santa Monica, CA: RAND Corporation, June 1969), http://www.rand.org/content/dam/rand/pubs/research_memoranda/2005/RM5888.pdf.

3. Harold A. Linstone and Murray Turoff, "Introduction," in *The Delphi Method: Techniques and Applications*, ed. Harold A. Linstone and Murray Turoff (Reading, MA: Addison-Wesley Publishing, Advanced Book Program, 1975), 11, http://is.njit.edu/pubs/delphibook/delphibook.pdf.

4. Gene Rowe and George Wright, "The Delphi Technique as a Forecasting Tool: Issues and Analysis," *International Journal of Forecasting* 15, no. 4 (October 1999): 353–75, http://www.forecastingprinciples.com/files/delphi%20technique%20Rowe%20Wright.pdf.

5. R. C. Oliver et al., *Survey of Long-Term Technology Forecasting Methodologies* (Alexandria, VA: Institute for Defense Analyses, November 2002), ES-2, http://www.dtic.mil/dtic/tr/fulltext/u2/a410179.pdf.

6. Somnath Mishra, S. G. Deshmukh, and Prem Vrat, "Matching of Technological Forecasting Technique to a Technology," *Technological Forecasting and Social Change* 69, no. 1 (January 2002): 20.

7. Industrial College of the Armed Forces, *Final Report: Information and Communications Technology Industry* (Washington, DC: Industrial College of the Armed Forces, National Defense University, Spring 2007), 4, http://www.nationaldefensemagazine.org/archive/2008/August/Documents/ICAFAug.pdf.

8. Patricia L. Williams and Christine Webb, "The Delphi Technique: A Methodological Discussion," *Journal of Advanced Nursing* 19, no. 1 (January 1994): 180–86.

9. Albert P. C. Chan et al., "Application of Delphi Method in Selection of Procurement Systems for Construction Projects," *Construction Management and Economics* 19, no. 7 (January 2001): 699–718.

10. Fergus Bolger and George Wright, "Assessing the Quality of Expert Judgment: Issues and Analysis," *Decision Support Systems* 11, no. 1 (January 1994): 1–24; and Klaus Brockhoff, "The Performance of Forecasting Groups in Computer Dialogue and Face-to-Face Discussion," in Linstone and Turoff, *Delphi Method*, 285–311.

11. Jacques Etienne Des Marchais, "A Delphi Technique to Identify and Evaluate Criteria for Construction of PBL Problems," *Medical Education* 33, no. 7 (July 1999): 505.

12. David M. Boje and J. Keith Murnighan, "Group Confidence Pressures in Iterative Decisions," *Management Science* 28, no. 10 (October 1982): 1195.

13. V. W. Mitchell, "The Delphi Technique: An Exposition and Application," *Technology Analysis and Strategic Management* 3, no. 4 (1991): 340.

14. Ibid., 356; and Rowe and Wright, "Delphi Technique as a Forecasting Tool," 371.

Capt Andrew Soine, USAF

Captain Soine (BS, Louisiana Tech University; MS, Air Force Institute of Technology) is a program manager with the Manufacturing and Industrial Technologies Division, Materials and Manufacturing Directorate, Air Force Research Laboratory, Wright-Patterson AFB, Ohio. He is responsible for planning, managing, and executing programs that provide advanced manufacturing processes, techniques, and technologies for timely, high-quality, and economical production and sustainment to strengthen the defense industrial base under the Title III program of the Office of the Secretary of Defense's Defense Production Act. He also addresses Air Force systems through the service's ManTech program. Captain Soine previously served in the Space Development and Test Directorate, Kirtland AFB, New Mexico; the 580th Aircraft Sustainment Group, Warner-Robins Air Logistics Center, Georgia; and as air and ground movement officer in charge with the US Army Corps of Engineers, Afghanistan Engineer District, Kabul, Afghanistan.

MSgt James Harker, USAF

Master Sergeant Harker (BS, New York Institute of Technology; MS, Air Force Institute of Technology) is the wing deployment manager for the 689th Combat Communications Wing, Robins AFB, Georgia. He is responsible for ensuring the combat readiness of equipment valued at $460 million and 1,500 Airmen from 10 squadrons composing two groups. Master Sergeant Harker has managed several work centers charged with various functions, including the maintenance of security systems that guard nuclear assets and the dissemination of Armed Forces Network radio and television broadcasts to their intended audiences. He also completed a special-duty assignment as an academy military trainer at the United States Air Force Academy, where he introduced cadets to the enlisted perspective and facilitated their development as future leaders.

Dr. Alan R. Heminger

Dr. Heminger (BA, University of Michigan; MS, California State University–East Bay; PhD, University of Arizona) is an associate professor of management information systems at the Air Force Institute of Technology, Department of Systems Engineering and Management. He has a background in networked collaborative work systems, strategic information management, and business process improvement. Dr. Heminger has undertaken research and consulting for Air Force and Department of Defense agencies, including Air Force Materiel Command, the Air Force Research Laboratory, the Air Force Center for Systems Engineering, Air Force Special Operations Command, the Air Force Office of the Chief Information Officer, the Air Force Communications and Information Center, the Defense Threat Reduction Agency, the 689th Combat Communications Wing, and the Defense Ammunition Center.

Col Joseph H. Scherrer, USAF

Colonel Scherrer (BSEE, Washington University in Saint Louis; MBA, Boston University; MS, Air Force Institute of Technology; MA, Naval War College; MA, Air War College) is commander of the 689th Combat Communications Wing, Robins AFB, Georgia. He leads 1,500 duty Airmen in an expeditionary cyber operations mission that deploys combat communications and air traffic control as well as landing-systems capabilities in permissive and nonpermissive contingency environments. A distinguished graduate of the Air Force Reserve Officer Training Corps program, Air Force Institute of Technology, Advanced Communications Officer Training School, Naval War College, and Air War College, Colonel Scherrer is the coauthor (with Lt Col William C. Grund) of *A Cyberspace Command and Control Model* (Maxwell Paper no. 47, 2009). He has participated in several theater operations, including Deny Flight, Provide Promise, Joint Forge, Deliberate Force, Southern Watch, and Enduring Freedom. He has commanded a cyber wing, a mission support group, and three communications squadrons. Colonel Scherrer has served in a variety of engineering, fixed communications, tactical communications, and staff assignments, including the Joint Staff, where he authored the Department of Defense's first national military strategy for cyberspace operations.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil