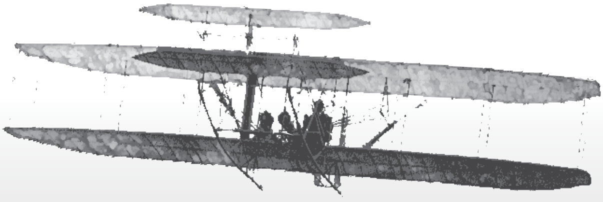
THE WRIGHT FLYER PAPERS

Virtual Wingman

Harnessing the Future Unstructured Information Environment to Achieve Mission Success

Galen K. Ojala
Major, USAF

Air Command and Staff College
Wright Flyer Paper No. 48



Air University
Lt Gen Allen G. Peck, Commander

Air Command and Staff College
Brig Gen Anthony J. Rock, Commandant
Col Robert J. Smith, PhD, Dean
Lt Col Kyle Gresham, PhD, Director of Research
Col Brett E. Morris, PhD,
and Maj John L. Mansuy, Series Editors
Kevin C. Holzimmer, PhD, Essay Advisor

Air University Press
Gen John A. Shaud, USAF, Retired, PhD
Director, Air Force Research Institute

Belinda L. Bazinet, Project Editor
Tammi K. Long, Copy Editor
Nedra Looney, Prepress Production
Daniel Armstrong, Cover Design

Please send inquiries or comments to
Editor
The Wright Flyer Papers
Air Command and Staff College (ACSC/DEI)
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426
Tel: (334) 953-6810
Fax: (334) 953-2269
E-mail: ACSC@maxwell.af.mil

AIR UNIVERSITY
AIR COMMAND AND STAFF COLLEGE

Virtual Wingman

Harnessing the Future Unstructured Information Environment to Achieve Mission Success

GALEN K. OJALA
Major, USAF

Air Command and Staff College
Wright Flyer Paper No. 48

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

December 2010

This Wright Flyer Paper and others in the series are available electronically at the Air University Research Information Management System website at http://research.maxwell.af.mil and the AU Press website at http://aupress.au.af.mil.

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Foreword

It is with great pride that Air Command and Staff College presents another in a series of award-winning student research projects from our academic programs that reach nearly 11,000 students each year. As our series title indicates, we seek to promote the sort of imaginative, forward-looking thinking that inspired the earliest aviation pioneers, and we aim for publication projects which combine these characteristics with the sort of clear presentation that permits even the most technical topics to be readily understood. We sincerely hope what follows will stimulate thinking, invite debate, and further encourage today's air war fighters in their continuing search for new and better ways to perform their missions—now and in the future.

ANTHONY J. ROCK
Brigadier General, USAF
Commandant

Acknowledgements

Information technology (IT) and its gadgets provide no allure. They are neither a marvel nor a toy but exist solely to help get something done. This impassive attitude allows me to avoid capability hype with what IT can do and ask "So, what does IT really do for me?" This attitude is partly due to my mechanical engineering background and to the practical systems engineering philosophies instilled in me by my father. I have successfully exploited IT capabilities to perform engine cold-start analyses, design coal crushers, train missile crews, simulate radar satellite constellations, track satellite parts and construction practices, and create intelligence fusion software. But with each success made possible through IT came scores of frustrations that sprang from IT solutions. While writing this paper I came to realize that this frustration comes from man having to manipulate IT rather than applying it as an extension of oneself. This fundamental disconnect between capability and utility comes from disconnects between developers and users, institutional restrictions on individual innovation, and general ignorance of available tools, practices, technologies, and the art of "market" timing.

If frustration is the fertile ground that bears innovation, then I hope to plant the seeds of ideas collected and cultivated through years of collaboration with astute, competent, business-savvy risk takers and visionaries. My thanks to the Defense Advanced Research Projects Agency and the Air Force Research Laboratory program managers who wrote their own scripts to examine contractors' claims, the geologist-turned-programmer who set the geospatial intelligence standard for software ease of use, the political scientist who instigated asymmetric intelligence collection and exploitation schemas, and to many others no less significant. In particular, my thanks goes to Bryan Talbot for his ideas on tailored applications; Bob Stanton for allowing me to join his innovative discovery and application crusade; and my father, William Keith Ojala, for his lessons on practical and viable engineering and system architecting.

Setting the Stage

The Department of Defense (DOD) is quickly reaching an information technology (IT) crossroad; its choices will determine whether it achieves decisional superiority or becomes paralyzed and drowns in its own data. Information management technologies and practices currently used to exploit the exponentially growing volumes of data are rapidly becoming inadequate.

For instance, a battalion intelligence analyst requires time-critical information spread across 200 different networks in 20 different languages.[1] Upon uncovering a bad lot of batteries, a satellite program manager must survey 15 different contracts' as-designed and as-built lists to ensure none of the faulty batteries are used. A deployed commander cannot write his or her subordinates' promotion recommendation forms because the local area network does not host the requisite form's viewer software. A Marine platoon commander's intelligence requirements change as he moves from stateside training, to forward base operations, to patrol. These users must access and manipulate unstructured data, obtain and share contextually relevant information, and operate from and across dissimilar IT systems.

Unstructured Data—Data that does not fit the expected format of the reader is considered unstructured.

Differences in the hardware, operating systems, application software, and recording media used, all prone to obsolescence and version variety, compound the problem by introducing format differences.

The variety of ways data is recorded and information is conveyed provides additional complexities: text documents, e-mails, maps, images, text messages, spreadsheets, sounds, drawings, and dynamic web pages (web pages generated on the fly from databases and existing only during the viewing session).[2]

Effective information management capabilities are a critical requirement, not a luxury. In their testimony to the Senate Committee on Homeland Security and Governmental Affairs, representatives of the Government Accountability Office (GAO) stated that "the ability to find, organize, use, share, appropriately dispose of, and save records—the essence of records management—is vital for the effective functioning of the federal government."[3] Beyond meeting basic information management capabilities, the DOD requires the ability to simultaneously and remotely share maps, imagery, and video among commanders at all echelons across mounted or dismounted ground terminals and airborne and seaborne assets to support decision making.[4] The DOD's underlying problem is the inability to collect, gather, organize, exploit, share, and store data that comes from multiple dissimilar systems, venues, and media. Dissimilarity transforms carefully structured data into unintelligible unstructured data.

Structured data is organized into a format that an individual user's software can read. If that format is then unrecognizable to a different individual's software, the data, no matter how innately valuable, becomes unstructured and is rendered worthless. This is a problem when considering the approximately 281 billion exabytes of data in cyberspace as of 2006. By 2011 this number is expected to increase by a factor of 10.[5] With a wealth of data tied to incompatible formats and buried within a multitude of evolving networks, the unifying problem becomes how the DOD can best posture itself technologically and doctrinally to harness the rapid growth of unstructured data and infrastructure to achieve mission success. Though many organizations share this problem, military requirements tend to be more challenging than commercial and civilian requirements. The combination of mission diversity, changing operational environments, and the variety of joint and coalition electronic formats and architectures available pose IT challenges more complex than those faced by shipping, health care services, manufacturing companies, and other civilian business sectors or private use.

Exabyte—a million times a million megabytes. (A gigabyte, a common memory size, is only 1,000 megabytes).

This paper goes beyond identifying singular technologies and implementation strategies to propose a comprehensive solution construct called the "Virtual Wingman." The Virtual Wingman construct demonstrates how current and nascent technologies and practices can be integrated and tailored to contextually provide the right information at the right time and in the right form. The Virtual Wingman is not a point solution. Rather, it embodies capabilities the DOD must develop and embrace to avoid decisional and operational paralysis when faced with mounting volumes of unstructured information and increasingly complex systems of systems.

Defining the Current Problem

The DOD's first major challenge is to define the variety of existing hardware, applications, operating systems, and networks and to determine how their lack of interoperability contributes to the current systems of systems' overwhelming complexity. US Army colonel William Davis, deputy director for the Pentagon's intelligence, surveillance, and reconnaissance (ISR) task force, offers the situation in Kandahar, Afghanistan, as an emblematic example: "Right now there are over 200 [coalition] systems at Bagram Air Base, Kandahar, and other places that don't talk to each other; even if they did, the information is scattered across 20 different languages."[6]

Though each system holds a piece of the puzzle for intelligence analysts, insufficient means exist to access, filter, and combine the scattered pieces into a coherent information picture. Additionally, network security complexity creates an environment as difficult to share as it is to steal. With increasing operations tempos, Colonel Davis worries that the entire coalition intelligence effort "will collapse under the weight of systems that do not communicate."[7]

Data format standards are an oft-tried interoperability approach to homogenize interfaces between functional, physical, electrical, or informational entities. This sometimes useful approach does not guarantee success; the inherently positive aspect of agreed-upon formats makes interfaces inflexible. This is especially a problem when current systems are too highly centralized and tightly coupled to respond to man-made and natural variance discontinuities within complex systems of systems.[8] The US Navy's experience in adapting Link 16 for data sharing between its ships and F-18 fighter jets showed that even with strict standards, subtle internal system differences in the sender's and receiver's computer operating speeds and internal logic processes still created disconnects.[9]

In addition, current systems of systems are complex; a single organization rarely owns the entire system. Such distributed ownership and operation can hamper timely propagation of updates and changes across the entire distributed architecture and user base to ensure interoperability. This problem forced the DOD to halt the Defense Integrated Military Human Resources System (DIMHRS), a 12-year attempt at integrating 90 different automated military pay and records systems costing $1 billion.[10] The problem stemmed from a software design philosophy based on creating rigid input/output interfaces to work with 90 different and independently controlled, designed, and sustained sources. Each interface could not be standardized because new incentive plans would come and go, veterans' benefits would change, and so forth, or the services adopted new network and software standards independent of DIMHRS requirements. Such version disparity creates systems that are susceptible to massive and coordinated failures, either by cyber attack or by sheer system complexity.[11]

Rather than creating a system focused on understanding and managing unstructured data, rigid data translator middleware. Middleware is a costly solution. Its code must be altered whenever the connected software changes, which is often unannounced.[12] The end result of the DIMHRS's rigid centralized approach is a defunct personnel system.[13] Overall, standards alone do not ensure interoperability.[14]

Middleware—software that is applied to reconcile dissimilar software formats by translating one format into another and back again.[15]

Computer-to-computer interface is not the only source of trouble. A Slovenian computer interface study cited human-to-computer interface as a growing source of information and capability disconnect. As the number of computer users and systems grow, users are becoming less experienced in the systems they use.[16] People do not have the time to master the variety and versions of operating systems or software applications and still accomplish their primary jobs. Consider the frustration individuals feel when relearning how to format page numbers after each Microsoft Word version change. Though each new version is typically more intuitive, the new interface requires time to learn, while work deadlines loom closer. Multiply this example across an entire range of evolving mission-related software. The result is extracting less utility out of technology despite its increasing inherent capabilities.

Maj Gen John Custer III, commander of the US Army Intelligence Center, sums up the second major unstructured data issue when describing the challenge of finding insurgents among the indigenous population as "trying to find a needle in a stack of needles."[17] Herein lie two challenges: targets are difficult to discern from the background and needed information is buried within a growing mountain of unstructured data. Finding insurgents requires collecting, filtering, sorting, and making sense of numerous loosely associated information snippets that only provide a useful picture when compiled in context.

To quickly find and extract subtle clues from vast stores of data poses a substantial problem. Full motion video (FMV) data from remotely piloted aircraft (RPA) exponentially expands the volume of available data. FMV is popular because it allows commanders, deployed forces, and analysts not only to monitor areas or individuals in real time but also to perform trend analysis using historical video comparisons. The downside is that FMV produces gigabytes of data a day. This creates an information pool too large for human and computer resources to filter and exploit. To make it worse, the US Army is looking to field 32 Class IV RPAs, all with electro-optical/infrared (EO/IR) cameras and nine with radar imagery capabilities. The imagery data collected will be so voluminous that it will require four analysts to exploit imagery from just one RPA. With 18 RPAs flying at any given time, analysts will have to examine one petabyte of FMV data every six months.[18]

Improvements in search engines also cause data overload.[19] New search engines perform more penetrating "deep web" searches to find otherwise buried databases.[20] The resulting increase in search returns multiplies the burden of culling additional unstructured, partially or fully duplicative, irrelevant "dirty data" to extract pertinent information.[21]

Petabyte—To provide a reference point for comparison, the ubiquitous one gigabyte of computer memory stores roughly 25 minutes of video (2^{30} bytes). One petabyte stores 53 years worth of video (2^{50} bytes or roughly 1,126,000 times larger).

The third major unstructured data issue concerns conveying information to those who need it. To win quickly evolving fights and counter asymmetric threats, General Custer stresses that "Soldiers must get access to information, not just commanders, and intelligence dissemination architectures must extend to Soldiers, Airmen, Marines, and Seamen."[22] This strategy has two components: access and dissemination of information and the acquisition, training, and fielding of capabilities.[23]

Need to know has always determined access to classified information. Commanders argue that in high operations tempo and counterinsurgency fights, the individual Soldier has the need to know.[24] The platoon leader needs situationally tailored intelligence products—if an ambush is imminent, for instance—and not the collection sources used to create the warning. Unfortunately, the intelligence community (IC) has yet to widely decouple highly classified collection methods from lower-classified intelligence information to produce useful and easier-to-distribute reduced-classification intelligence products. Though it does not have the human resources to parse large volumes of data, the IC is not ready to trust automated information parsing and classification-downgrading algorithms to quickly deliver down-classified information extractions. The stated risk is that automated systems could allow classified information to be leaked.

Not trusting automated systems creates a missed opportunity, as decoupling intelligence products from their sources often results in smaller file sizes. A one-gigabyte, top-secret imagery and signals intelligence file transmittable only across high-bandwidth, secure communications systems could have been disseminated as a 50-byte unclassified text message alert over a local communications infrastructure. Successful dissemination delivers requested information in a format that fits the users' local dissemination architecture and satisfies the intended need.

Another component focuses on the inability of traditional acquisition processes to acquire, train, and field capabilities to meet frontline units' rapidly changing battlefield needs, with their unique IT limitations and resources. Due to traditional acquisition's failings, combat-intelligence Soldiers are increasingly writing their own code to gather information.[25] These from-the-field products draw upon the latest open-source techniques, scripts, and software to create fast, efficient, and functional, yet Frankenstein-like, patchwork solutions. While theater commanders endorse such efficacy, continental US installation commanders tend to shun untested and unofficial software solutions that are not supported by either program offices or commercial vendors.

Commercial-off-the-shelf (COTS) software provides what seems to be a cornucopia of information management solutions. Tapping uReach Technologies Inc., Verizon Communications enables business professionals to remotely work and stay connected with customers from any network interface, such as a desktop, laptop, cell phone, or iPhone.[26] Initiate Systems is helping health care provider Sutter Health extract and create virtual consolidated individual records from distributed records spread across 30 hospitals and 100 databases.[27] The DOD can also use these capabilities.

These COTS solutions are alluring because vendors provide plug-and-play capabilities supported by established customer service, training, and maintenance plans, and the DOD does not have to pay for their development or infrastructure. The catch is that the vendor determines the customers' visibility into how the products and services work and also how, where, and for how long they are supported.

COTS, moreover, is only COTS if it is unaltered from commercially offered versions; it cannot be modified. DOD-directed changes require vendor development, testing and recertification, and manufacturing expenses, which are paid for by the DOD. As alluring as COTS solutions are, they rarely meet stringent war-fighter requirements because military needs are constantly changing.

Enemy tactics, available local infrastructures, and other battlespace variables change quickly. The Verizon suite works because it is tailored to US communications infrastructure. Initiate Systems' software works because Sutter Health eliminated access issues and implemented version control by controlling the hospitals' databases. The DOD's variety of networks, security protocols, infrastructure, and missions, along with changing requirements, creates a complex need that is difficult and costly for COTS vendors and traditional acquisition cycles to support.[28]

From-the-field software may be patchwork, but its utility, tailorability, and intuitive interfaces signal a shift in IT trends. In a *Military Review* article, "Reach: Leveraging Time and Distance," General Custer posits a "seamless worldwide connectivity at multiple levels of security with facilitating protocols and permissions to access and interact with hundreds of databases that National Agencies, the Department of Defense, Joint Commands, and coalition partners maintain."[29] This can be accomplished by drawing upon commercial and academic open-source standards and techniques to create interoperable solutions whereby petabytes of data can be searched, filtered, and recombined to create situation-appropriate presentations. A common enabling future element will be computational intelligence (CI)–aided software code adaptation. In Clausewitzian terms, patchwork capabilities will be brought together to reduce rather than increase what Daniel J. Boorstin, the librarian of Congress who ushered the computer age into the Library of Congress, called the "fog of information."[30]

Despite many technological and acquisition challenges, the greatest roadblock to harnessing unstructured data and systems comes from organizational policies, practices, and culture. Gen Kevin P. Chilton, commander of the US Strategic Command (USSTRATCOM), the parent command to the subunified US Cyber Command, acknowledges the role institutional inertia and fear of the unknown play in thwarting the adoption of new technologies and practices. In his "Cyberspace Leadership" article, General Chilton states, "We need a change in our culture, conduct, and capabilities if we are going to advance the state of the art and provide the protection and freedom of action we need in this [cyber] domain."[31] When armed with evolving technologies and approaches to creating and fielding solutions, the means exist for the DOD to harness the growing sea of unstructured data to deliver war-impacting information.

The Official Need

The trend of IT's increasing complexity is a growing concern. From national policy to service doctrine, US leaders recognize the importance of harnessing multiple information sources and systems to make and communicate timely decisions across the entire US government structure. The 2004 *National Military Strategy* states that "joint forces will require new levels of interoperability."[32] It also declares that the joint force will use superior intelligence and the power of information technologies to increase decision superiority, precision, and lethality of force. A networked force capable of decision superiority can collect, analyze, and rapidly disseminate intelligence and other relevant information from the national to tactical levels and then use that information to decide and act quicker than opponents.[33]

To achieve success requires the innovative employment of adaptable and decentralized decision authority.[34] This includes "seamless multilevel security access [that] will empower distributed command and control and provide increased transparency in multinational operations."[35]

Logisticians share the intelligence coordination problems described earlier by Colonel Davis. Joint Publication 4-0, *Joint Logistics*, declares that "logisticians face their greatest challenge at the operational level because of the difficulty of coordinating and integrating capabilities from many providers to sustain logistically ready forces for the Joint Forces commander."[36] Many providers include other services, government agencies, commercial vendors, and multinational sources, each using their own data formats and information systems. Melding unique logistics operations into a unified effort produces an unstructured data morass that planners must untangle, usually under crisis timelines. The US Transportation and Joint Forces commands are developing standard data formats and systems. However, rigid standards and inflexible bridging software do not create a flexible architecture to fuse ad hoc sources and processes during the short-notice crises that constitute 75 percent of the DOD responses.[37]

Even without multinational involvement, the United States is swamped by much data which cannot be filtered through and fused on demand. In the US government alone, there are over four trillion paper documents—a stack that is growing at a rate of 22 percent each year.[38] The National Archives and Records Administration required about 400 days just to process 2 terabytes of data (1 terabyte is about 1,000 gigabytes) created by Pres. Bill Clinton's administration.[39] This situation reveals but a tip of the data iceberg.

The Future Information Environment

The future information environment will consist of data, users, tools, and practices, much as it does today. How these elements come together determines how the fog of information will be navigated and exploited.[40]

The Fog of Information

Boorstin's fog of information aptly applies to what may be referred to as the infosphere. The world's infosphere has already reached an incomprehensible dimension. Composed of e-mails, books, databases, broadcast television, websites, and so forth, the 2002 worldwide infosphere was calculated to be roughly 18 exabytes in information volume and grew to 281 exabytes by 2006.[41] Rather than trying to project its future size, future data sources and output rates must be understood.

Though individuals, companies, and governments will continue to grow the information domain by increasingly digitizing their practices, exponential growth in sensor use and the amount of data collected per sensor will account for the greatest raw data increases. Next-generation imagery systems' pixel-resolution increases will produce an eightfold data increase per image frame, not including the trend toward employing multi- and hyperspectral collections.[42] Sensor networks will become pervasive throughout homes and businesses to measure productivity, safety, and energy efficiency, for example. These ubiquitous networks will also become omnipresent in the battlespace and will produce their own data streams to add to the infosphere morass.

The infosphere's size will escape one nation's ability to encompass it. In reference to information, common war concepts of dominance and superiority will be neither realistic nor useful in any sense of overwhelming the enemy. Instead, "information effectiveness" is an achievable goal and the most useful to obtain.[43]

The Future Information User

In the information age's beginning, organizations, not individuals, possessed the latest technologies. However, many of today's users are technologically savvy, owning and operating more sophisticated and user-friendly hardware and applications than their employers' IT departments.[44] Users are increasingly mobile, regularly exploit shared knowledge, and demand the same capabilities and services at work as they have at home.

This capability divergence feeds workplace frustration expressed as a notional IT "Bill of Rights." Bill Jensen, author of *Work 2.0—Rewriting the Contract*, points to fulfilling the basic modern workers' needs by providing "a workplace where it is easy to get what [they] need to get [their] work done—the right information, the right way, in the right amount."[45] Instead of demanding shorter hours or safer working environments, workers are demanding "user-friendly applications and information/capability sharing policies that enable them to be productive from anywhere without compromising the needs of the enterprise from a security and manageability standpoint."[46]

Personal computers (PC) made computer processing available to the populace but have not made computing personal. The human-computer interface has not changed significantly since the 1984 introduction of the Apple Macintosh mouse-menu interface.[47] Users demand that the PC and its descendants (laptops, smartphones, etc.) be customizable with tailored interactions to serve their needs and predict their desires. They seek technology that supports professional practices without distracting them from getting their work done.[48]

Today's software still requires unnatural interactions to achieve desired tasks. From their multipaper research compendium, Paolo Remagnino, a Kingston University faculty member specializing in computing, information systems, and mathematics, and Daniel Shapiro from Stanford University's Computational Learning Lab concluded that users are looking for their IT departments to "endow an environment with the computational power sufficient to sense its inhabitants and to interpret their actions and interactions in order to anticipate their needs, supply them with necessary information, and/or to act on their behalves."[49] The need goes beyond better search engines. It is the desire for proactive and anticipatory systems that forms the impetus for establishing ambient intelligence (AmI).

Information and Communication Technology

AmI is "an interdisciplinary approach borrowing methods and techniques from the computing fields of ubiquitous computing, context-aware computing, human-computer interaction and artificial intelligence."[50] Technologies such as virtual and cloud computing and cognitive radio will be exploited to provide the mobility, processing, security, and expandability required. The addition of mobility into IT across personal and work life has created the information and communication technology (ICT) descriptor.

AmI—analyzes local sensor data to tailor services. Example: Using a variety of sensors and the minimum of direct user input, a computer analyzes household usage and environmental patterns to provide interactive and personalized management of domestic services such as thermal control, security, health monitoring, and watering.[51]

ICT technologists Vivienne Waller and Robert B. Johnston note that ubiquitous computing is not a specific technology but an implementation theory based on the fact that users "don't want to use a computer, they want to accomplish something."[52] Technology should become a seamless extension of the user, disappearing from the user's awareness.[53] This efficacy occurs by reducing unnecessary data entry by the computer, automatically updating and drawing actionable information from a model of the world created using information obtained from the embedded environment.[54] The computer gains this awareness by comprehending the users' environment, location, computer use, tasks, use history, preferences, workflows, and future events. In military language, the pervasive computer becomes an executive officer. Training, intelligence, and the ability to operate independently of its commander enables a computer to anticipate the commander's needs; to gather, consolidate, manage, prepare, and present information in the commander's preferred format; and to negotiate activity interfaces, freeing the commander to focus on duty-appropriate tasks. This support utility forms the Virtual Wingman's functional foundation.

The term *wingman* denotes the subservient yet independent service provided to defensively protect and offensively enable the lead. *Wingman* also signifies a paired relationship that flows from the battlespace to noncombat life. In technical terms, the virtual wingman is a computational agent.

Agent—a virtual representative of the user. The user grants the agent the authority to act on his/her behalf, and the agent carries the access authorizations granted to the user. "Agents have the capability to make their own decisions about what activities to do, when to do them and what type of information should be communicated and to whom, and how to assimilate the information received."[55]

The first step toward achieving the virtual wingman agent-user relationship is establishing more innate human-computer interfaces. By presenting contextually relevant information and options, the user's attention stays focused on the action and is not diverted to an artificial model of the world.[56] Imagine an engineer taking a car trip to deliver a presentation. In planning the trip, an agent is used to see the route on a map, a current traffic model, and potential en route lunch stops. The resulting travel plan is transferred from the desktop computer to the vehicle. While the engineer is driving in traffic, the visual map is replaced by intuitive and less distracting audio directions.

AmI's situational awareness differs from today's global positioning car systems. An AmI travel system uses time, traffic volume, car speed, fuel status, personal schedules, and preferences to recognize that the car is low on fuel, traffic is bad, and there is insufficient time to stop for a lengthy lunch before the engineer's upcoming appointment. Given that information, the AmI agent calculates and then audibly suggests stopping at the third gas station on the right to fuel up and purchase a fast-food sandwich from the collocated and driver-preferred food chain. A useful aspect is the agent's ability to work with the user at the engineer's desk and then appear elsewhere when needed. The agent appears in the vehicle and then in the smartphone to guide the engineer to the appointment. If granted network access, the engineer's agent can preposition itself in the conference room network station to allow the presentation to be given.

Virtualization and Cloud Computing

Various current communications technologies enable an agent to move with or deploy ahead of the user, but virtualization enables the agent to operate across multiple dissimilar platforms as if it were operating from its original/designed hardware.[57] This is a tremendous liberating capability for the future user.

At present, software operates with specific operating systems, hardware, and networks. To ensure compatibility across a wide combination of operating systems, hardware, and networks, software developers must take on the expensive and cumbersome task of designing and testing software to operate with multiple system configurations or limit the customer to a fixed-system configuration. The first design path results in a complex "fit everything" software code that is a nightmare to maintain because operating systems and hardware change. The second path robs users of flexibility. Virtualization frees developers and users of many restrictions and costs by allowing applications to operate from any local or remote system as if they were operating on a designed-to-hardware-and-software operating system. For instance, the engineer in the scenario can present an engineering simulation on a different host computer without worrying about compatibility issues because the host computer will operate a virtual machine copy of the engineer's desktop. While virtual machines are still not widely used in the DOD, by December 2010 they will account for half of all commercial server-based computing, including that of all Fortune 100 companies.[58]

Virtualization—"A computer uses a software simulation of the hardware, called a hypervisor, to create one or more virtual machines that simulate real computers so faithfully that the hardware simulations can run any software from operating systems to end-user applications. The software 'thinks' it has access to a processor, network, and disk drive, just as if it had a real computer all to itself."[59]

When the hypervisor initiates a session on the host system, it creates a virtual operating environment called a guest.[60]

Only the software or discrete components to be used actively within a guest session are checked out from a software repository.

An important inherent feature of this system is that upon completion of a task, the virtual session guest is wiped from existence, freeing the host computer to run a different guest.[61] Virtualization's customizable nature provides useful security protection options. In his article "5 Laws of Virtualization Security," Pete Lindstrom, senior Burton Group security analyst for Web 2.0/SOA/Web Services, points out that virtualization allows "single set or multiple sets of applications to be run in a virtual machine guest separate from all other applications."[62] Because applications can operate as if they were on separate computers, applications can simultaneously run compartmentalized from each other. This process enables users to work classified, unclassified, proprietary, source selection, and personal work sessions simultaneously using the same human-computer interface without fear of cross-systems data contamination.[63]

Though virtual machines operate an additional software layer to simulate the hardware host, virtualization enables more secure computing. In simple terms, virtualization reduces security risks by decreasing the "surface area" of code exposed to outside interfaces.[64] Virtual machines operate only the software or functions needed at that moment, and code designed to one configuration is easier to secure than if designed to multiple configurations. Altogether, virtual machines provide fewer unguarded and exposed exploitable interfaces. If the guest session is maliciously altered, the user or system administrator can terminate the guest and restart the session from a known safe baseline configuration without affecting the software, the host platform, or other untainted guests.[65]

An operational benefit is that virtualization allows hardware to simultaneously run modern and legacy applications. This is a sustainability boon because users no longer need to purchase and maintain expensive stockpiles of old computers and operating systems to operate useful legacy software and equipment. An intelligence analyst can simultaneously process signals intelligence (SIGINT) from a 1980s-era collection system while exploiting the data in the latest geographic information system (GIS) application and disseminate it across decades-old distribution architecture—all from the same new computer the IT department placed on the desk 20 minutes ago.

An associated technology is cloud computing. In cloud computing, software resides and processing and data storage occur at a remote computer center, often without the user realizing it.[66] Though it is reliant on network connections, tremendous processing and storage performance and efficiencies can be gained by accessing mainframe supercomputers. When combined with virtualization, cloud computing allows multiple guests for many users or different projects, contracts, and so forth to tap excess memory and processing capacities. *Technology Review* reporter Erica Naone interviewed Amazon, Intel, Enomaly, and SUN Microsystems executives concerning cloud computing use. They suggested that this practice "allows cloud providers to reap massive economies of scale and . . . gives cloud users access to as much computer power as they want, whenever they want it."[67]

Cloud bursting offers a hybrid solution that allows users to tap supplementary processing power and memory when resident capacity is surpassed.[68] Cloud bursting allows users to operate through peak loads without losing clients or breaking service. Through virtual cloud computing and cloud bursting, users can muster supercomputing capabilities through the interface of their smartphones.

Cloud Computing—By using a thin-client interface, users tap data processing and storage capabilities of several distributed facilities. These remote facilities typically host super computers that allow clients to access the resources needed.[69]

Cognitive Radio

Though not a critical component of ubiquitous computing, mobile communications technologies provide users and their agents with flexible connectivity. Paradoxically, wireless bandwidth is a scarce commodity, but a great deal of it is unused much of the time.[70] To exploit this paradox, developers are pursuing cognitive radio (CR). *IEE* [Institution of Electrical Engineers] *Review* contributor John Walko states that "the goal of cognitive radio is to sense whether a particular frequency band is being used and, if it isn't, to utilize the spectrum without interfering with the transmission of other authorized users."[71]

CR is built upon software-defined radio (SDR).[72] Currently, US military-developed SDR suffers from reliability, security, and operating problems because the system is trying to do everything on all systems, all the time from a rigid internal architecture. Virtualization will likely be SDR's salvation, as it facilitates streamlined operations and simultaneously simulates multiple current and legacy radio configurations. Despite ongoing DOD debates about SDR's future, in 2003 the Federal Communications Commission

(FCC) informed the commercial sector on how to implement CR yet safeguard existing license holders.[73] Foreseeing the opportunity for tailoring the manufacture of nonoriginal equipment, the FCC proactively issued reasonable security guidelines to ensure transmitter operations under FCC rules yet allow flexible tailoring of capabilities.[74] Seeing the demand, the FCC is positioning the community to build a capability around a security strategy, rather than waiting and trying to force retroactive patches to an already established architecture.

A virtualization shortcoming that could affect SDR/CR is that the extra layer of simulation abstraction decreases performance.[75] Though this makes some applications such as streaming video difficult to replicate, two solutions are possible: (1) institute paravirtualization (hybrid virtual machines) to directly access hardware for some functions to provide processing speed increases; and (2) employ faster processors.[76] Given the trend for processor speed, driven by market demand for increased operating speeds in ever-smaller products, there is little concern that sufficiently fast systems will soon be available to support virtual machine CR. More illuminating is that the FCC recognizes that SDR will follow the ICT community's desire for tailored applications, a feature that virtualization can support.

By 2020 CR should be mature enough to replace the shaky joint tactical radio system (JTRS), a DOD-wide program designed to develop, build, and field interoperable, secure software-defined radios that are audio-, data-, and video-capable for dismounted/mounted, air- and sea-platform use. The JTRS's importance and expense are seen by comparing its $12 billion price tag to the $10.8 billion Virginia-class attack submarine program.[77] As a $220,000 ground vehicle radio (as compared to the $20,000 legacy radio), the JTRS provides a data rate of five megabits per second (Mbps), whereas current smartphone technology provides 100+ Mbps.[78] With gigabits-per-second data rates in the works, the JTRS is an expensive improvement topped out at yesteryear's capabilities.[79]

Future of Software Development and Acquisitions

The *National Defense Strategy* emphasizes timely innovation. Technology and equipment are the tools of the total force, and service members must have the best resources to get the job done. First-class technology means investing in the right kinds of technology at the right time. Just as adversaries adapt and develop new tactics, techniques, and procedures, the United States, too, must be nimble and creative.[80]

While the DOD's intent is sincere and appropriate, the processes for developing and fielding technology are not achieving its aspirations. Analyzing the defense acquisition process for its application across the entire spectrum of technologies and goods is not within this paper's scope. It does propose a shift in how the DOD views the acquisition of ICT. The three required changes are (1) greater acceptance of COTS in an as-is configuration, (2) transition to open-source hardware/software development, and (3) empowerment of users to develop and field their own solutions.

Information and Communication Technology Consumables

Commercially developed and sold multifunction electronics such as smartphones and electronic tablets will continue to outpace DOD-created capabilities. As mentioned earlier, COTS products are typically not made to survive the entire range of military rigors. However, as COTS products surpass military specifications (mil-spec) products in capability, the DOD may need to start accepting "good enough" more often in a compromise between physical robustness and purchasable numbers. The cost of fielding the JTRS forced a 71 percent reduction (328,514 to 95,551 units) in handheld, man-pack, and small form-fit radios.[81] This decrease in available tactical radios comes as the United States increases its fielded forces and has to communicate within fluid joint and coalition operating environments. If a COTS ICT product is not rugged enough, a purpose-built protective case may be a more cost- and mission-effective solution than an entirely mil-spec product. Throwaway COTS products may provide a good business- and mission-sense alternative to the high cost of sustaining the infrastructure of the DOD's government-off-the-shelf (GOTS) products. Though the hardware may be COTS, all the supporting software need not be. Using the Apple iPhone's application toolkit business model, many military-centric applications can be created and tailored by Soldiers, Airmen, Sailors, Marines, or Coast Guardsmen.

Software Development Reinvented—Service-Oriented Architecture's Promise and Pitfalls

The evolving commercial sector is pulling away from the proprietary-centric, closed-architecture DOD business models. Service-oriented architecture (SOA) has been hailed throughout the DOD as ICT's savior. Within an SOA, a software-backbone-capability application is established whereby expanded capability software modules can be plugged using published, configuration-controlled, standardized interfaces. SOA has proven a successful systems engineering construct. Failures do not occur because the SOA concept is flawed but because managers and developers do not account for two critical programmatic pitfalls: (1) open architectures do not guarantee interoperability; and (2) uncertainty exists over who pays for third-party module development, testing, and sustainment.[82] Unless the backbone's developer provides source codes in an open-source format, interoperability problems arise because module developers must guess at the backbone's internal process and operating characteristics that may affect their module. The more complex and timing-dependent the SOA system becomes, the more this pitfall becomes a problem.

The second pitfall pertains to code sustainment. In such highly interconnected systems, generally any major backbone code change requires adaptations to plug-in modules. Part of SOA's allure is that development is decentralized by enabling third-party users to develop their own plug-in modules to satisfy specific needs. This lowers the cost of expansion. However, sustainment problems arise because third parties cannot afford to incur the unwelcomed costs of planned or unplanned backbone code changes. This results in third-party capabilities' temporary or permanent termination and the end of the symbiotic relationship.

Two practices can help avoid these hazards and unlock SOA's promise. The first is virtualization, which simplifies software development, reduces costs, produces more reliable and secure code, and promotes modularization, especially within an SOA context.[83] The second practice is open-source coding.

Open-Source Coding, App Stores, and Repositories

Open-source coding is anathema to traditional software development businesses. Andrew Aitken, open-source business consultant and managing partner, said, "Open-source started as a noncommercial response to inefficient technologies and distribution models" and "the desire to solve problems not being solved."[84]

A Swiss team investigating code reuse concluded that open-source development is based on "informal and virtual communities of practice who share the expectation that open-source software developers are to build on each other's work."[85] The team explained that "open-source licenses convey the basic rights to the developer to retrieve the code, inspect, and modify it, and to freely redistribute modified or unmodified versions of the software to others."[86] This applies to software, hardware, and interface standards. The motivation to use open-source is strong. It can tap the collective knowledge of those who have already overcome challenges and therefore avoid reinventing common functions such as saving files and accessing networks. Thus, developers are freed to focus on the "long poles" of the program.[87] This practice helps to cut the average commercial public release time to 44.5 days.[88] The open-source practice bolsters innovation and "helps young projects to gain the necessary momentum to reach a critical mass."[89] An added benefit of open-source code is its robustness, as other coders can inspect it to highlight problems and to propose improvements or fix it.[90]

Long Poles—a project's or program's most difficult challenges. The term is drawn from the analogy that the most difficult task in setting up a tent is to erect the long poles that support the tent's canopy. Until this most difficult and risky task is completed, little useful work can be accomplished in and around the tent.

The temptation is to accomplish the easy short-pole tasks first to show progress. The inevitable result is uprooting all the short poles when the long poles are erected.[91]

Open-source benefits companies, work groups, and individuals by enabling them to produce capabilities at lower costs than traditional practices allow and to expand more rapidly the use base through utility and a sense of ownership.[92] Embracing open-source use often requires an organizational culture shift but does not mean sacrificing profitability or utility. As Sun Microsystems chief executive officer Jonathan Schwartz states, "The money in open-source is found and sold in peripheral services and courting the developer community to eventually depend on [your] products."[93]

Open-source code can be shared directly between two entities (companies and/or individuals) or by the common practice of maintaining source code repositions for communities of interest. The most popular repository is SourceForge.net, which in February 2009 had over 230,000 projects with more than 2 million registered users downloading more than 2.6 million projects.[94] Projects vary from function scripts to complete applications. The site is organized into project categories such as communications, databases, and desktop environments.[95]

Source Code Repository—a site where software developers can post software codes, in whole or part, along with supporting documentation for other developers to view, comment on, use, and modify. Submissions are commonly called "projects." Projects can be a complete application or a single subroutine.[96]

Open sourcing is not an entirely new practice for the DOD, as communities of practice (CoP) within the IC are creating internal code repositories. However, the efficiencies gained by code repositories come from the free, self-managed community practices and collective motivation of individual developers to post and maintain code both as a matter of professionalism and utility for later self-use. These practices tend to be lost in smaller, forced internal organization repositories and result in additional development costs.[97] The larger the repository's developer population, the more robust and self-maintaining it becomes. Thus, within the IC, repositories should be opened along classification levels (top secret, secret, etc.) rather than functional communities (geospatial intelligence, SIGINT, etc.). The concept of code storehouses can be taken one step further to create repositories of completed applications, or "apps," from which users can draw.

Some hardware and operating system vendors provide open-source software development toolkits encouraging third-party developers to create new applications using the vendor's product. This approach simultaneously provides users with access to more capabilities while creating a robust and profitable third-party developer infrastructure with little risk to the vendor and, at the same time, making the vendor's products more relevant and indispensible. This confluence of practices opens the door to making tailored apps a common ICT element.

> *Apps*—the colloquialism for software applications. Apps are typically associated with third-party or personally created, tailored, specific-function software. Apps are commonly developed using a hardware or operating system vendor's open-source software development toolkit.

Apple was the first company to encourage this movement by releasing a software development kit in March 2008 to help companies and individuals create and modify apps for the iPhone, iPod Touch, and now the iPad.[98] Apple then opened the App Store in July 2008, and by October 2008, 7,000 third-party apps were for sale. This number climbed to 50,000 by August 2009 and to 100,000 by January 2010.[99] By 24 April 2009 users had downloaded over 1 billion apps. The hardware represents mobile information and communication technology with the capacity to record sound and video, locate itself geospatially and in three-axis orientation and acceleration, and act as an interface to cloud computing. The marriage of tailorable software to standardized hardware contributed to the sale of over 36 million smartphones in the first quarter of 2009.[100]

The US government is tentatively getting on the bandwagon. The General Services Agency (GSA) has created Apps.Gov, a virtual store for GSA-approved and cost-negotiated IT products and services.[101] Though a step in the right direction, Apps.Gov strictly markets commercially developed business, productivity, and social media applications and cloud IT services. It does not feature or host GOTS apps. As mentioned, within the ICs are pockets of in-house developers. Unfortunately, sharing is informally accomplished, and attempts at formal sharing are impeded by network security bans on tracking applications. These allow developers to track user employment to justify software sustainment budgets and to notify users of and push updated patches, products, and training. In short, the government as a whole and the DOD in particular must expand the Apps.Gov model to allow military personnel, civil servants, and DOD supporting contractors to freely post and download government-created open-source development tools, scripts, and applications to facilitate their daily work.

Coding's Future—Novice and Computer Self-Generated Code

While open-source practices make it easier to tailor code, developers strive to create systems that free users from having to break focus on work to manipulate technology. The goal is to achieve on-the-fly tailoring where either the user or the user's agent adapts the baseline software as the need arises. In the latter case, to successfully modify software requires a high level of computational capability. A simpler hybrid approach to achieve user-based tailoring is "programming by example," otherwise known as programming by demonstration.[102] In this approach the user demonstrates examples of the desired behaviors or results to the computer, which generates the corresponding software code to achieve the objective.[103] The significance of this practice is that even novice users can be empowered to debug software as problems occur without waiting for a patch. To achieve this future capability, software must be dynamic (the code is easily changeable at any time) and introspective (the user is allowed access and visibility into the inner workings).[104]

When a problem arises, the user should be able to ask the computer what it is doing, why it did that, what it did, and how it can be fixed. The next level of abstraction occurs when an artificial agent recognizes when a problem arises, determines various work-around solutions, selects a solution, and implements it without the user being aware there is a problem. On-the-fly debugging will require the nascent discipline of artificial intelligence (AI).

After 30 years of pursuing AI to no avail, researchers at the Massachusetts Institute of Technology (MIT) have decided to depart from the goal of achieving artificial self-cognizance and concentrate on realizing contextual awareness.[105] The MIT team abandoned the human-mimicking Turing test to pursue the goal of having a computer read a children's book and understand what is happening in the story.[106] According to British Telecom's foresight manager and eminent futurist Robin Manning, this new focus on obtaining contextual awareness will help to put "more intelligence into raw information so that it can be more meaningful to humans and computers."[107] Rather than trying to mimic human responses, this AI research stresses reducing "artificial stupidity" in human-computer interactions.[108]

This research holds tremendous potential for harnessing unstructured data by replacing current "matching" search engine strategies with contextual strategies whereby data's utility is judged.[109] In on-the-fly interoperability problems, AI agents can be used to determine how to repackage and present data to optimize user receipt and synthesis. Creating artificial decision capabilities will increase users' employment of software features while reducing frustration and distraction. This is in keeping with Manning's premise that simplicity in technology's use should be the primary goal.[110] These AI capabilities will draw upon CI techniques such as fuzzy logic, neural networks, and genetic algorithms to enable computational learning of the user's style, interests, and requirements to provide adaptive user support.[111] Computational learning allows software to recognize use patterns and contexts to adapt proactively to changing operational environments, ensuring interoperability and relevance.[112] Though many CI and AI development challenges lie ahead, the greatest challenge is in how users, managers, and leaders embrace these new technologies and practices.

General Chilton believes that "we need a change in our culture, conduct, and capabilities if we are going to advance the state of the art and provide the protection and freedom of action we need in this [cyber] domain."[113] This statement sounds good, but are DOD leaders ready to trust their operators and artificial agents to tailor war-fighting capabilities on the fly? In creating a self-correcting software-coding capability, researchers Matjaz Gams and Borut Hribovšek found that the most problematic aspect associated with employing their intelligent personal-agent interface was getting users to trust the agent even when it was correct 99 percent of the time.[114] They found that "since computer systems are not able to display intelligible performance, humans do not trust them."[115]

Virtualization may help assuage the distrust that leaders and administrators harbor against allowing users and artificial agents to alter established software. When a virtual session is initiated, software is "checked out" from a repository on an as-needed basis. If the software is accidentally or maliciously corrupted, the virtual guest can be terminated, and the last configuration-controlled software version can be checked out again.[116] The technique establishes the means to achieve nonuniform operations without devolving established capabilities and architectures.

Security—Moving Past the "Sky Is Falling" Mentality

"To provide greater security" is the traditional argument for centralized ICT services control. The reality is quite the opposite. System administrators and traditional software development along with sloppy user practices have created security vulnerabilities.

In researching web security breaches within the IT community, senior Google developers and security specialists found that "many administrators neglect to update their installations."[117] Thirty-eight percent of Apache installations and 40 percent of PHP installations in compromised sites were unsecure and out of date.[118] Besides sloppy network administration practices, software developers inadvertently discourage good practices because patch installation requires work-disrupting network reboots or system reconfigurations. In other cases, developers took as long as 284 days to create and disseminate major web-browser patches. This resulted in at least 98 days during which criminals could actively exploit these vulnerabilities.[119]

General Chilton pulled no punches when summarizing the source of the DOD's cyber security problems and their impact on obtaining capabilities: "A lack of professionalism in the cyber realm imposes artificial barriers because we do not know what we have, thus we do not know how to protect it."[120] Several ICT security experts also express the need for hiring and retaining professional, vigilant, and competent ICT administrators, eliminating duplicative or overlapping regulations and policies, and conforming to basic best security practices.[121]

Beyond people and policies, the DOD must shift from practicing "design by fear" to "design to requirements," with security as a requirement precondition. Pete Lindstrom, senior Burton Group security analyst, advises that security requirements must be tempered by "a measured approach that carefully considers the impact on the existing IT infrastructure; a factored analysis of threats, vulnerabilities and consequences; and an understanding of the impact on existing security solutions."[122] Senior Google managers have determined that leaders must avoid fear-based decision making and that developers must avoid the failures of earlier web applications and Internet infrastructure designers who did not have a well-thought-out security model as part of the design.[123]

Not every security concern can be addressed, but Lindstrom suggests a few key fundamentals:

1. Reduce, isolate, and eliminate exposed resources to limit vulnerability.[124] System vulnerability is a function of a system's attack surface, and input interfaces represent surface area.[125] This goal is easier to achieve with virtual machines because users can tailor guest sessions despite the addition of the hypervisor software layer.

2. Use cryptographic and access-control protection measures for files and systems.[126]

3. Encrypt network traffic where possible, even internally.[127]

Virtual machines are not without pitfalls. The hypervisor—the layer simulating the hardware—adds surface area exposed to outside exploitation.[128] This can be mitigated by restricting and logging access to hypervisor controls.[129] In all other respects, virtual machines share the same vulnerabilities as nonvirtual machines except that virtualization software exposure can be controlled, whereas conventional systems expose all software contained within the computer.[130]

New Technologies + New Practices = Future Capabilities

If the technologies previously discussed were implemented, the DOD stands to realize greater capabilities and efficiencies through the ability to reduce network load through intelligent agent network use; create robust and fault-tolerant infrastructures where agents help circumvent faults and software can be maintained and improved by users with limited software experience; optimize local effects by implementing forward control of services by users and agents that allow operations to be more closely tied to the local environment; and enable legacy and evolving systems interoperability through asynchronous and autonomous adaptive middleware.[131] Consolidating these capabilities provides the impetus to assemble the Virtual Wingman.

Virtual Wingman Revealed

The Virtual Wingman demonstrates the potential payoffs from fostering enabling technologies and implementation practices, allowing innovation from within and outside the DOD to take root and bear fruit. The goal is to provide a semiautonomous, user-focused, roaming computational/AI agent that proactively and contextually adapts ICT to reduce information management burdens and provide near-seamless ICT interoperability. Assigned to individuals, it assists locally and acts as a portal to tap the expertise of communities of interest and remote cloud computing supercomputer resources. As an extension of the user, the Virtual Wingman applies its user's security authorizations to negotiate security protocols across multiple networks. As the user's mind compartmentalizes information and activities, the Virtual Wingman similarly compartmentalizes itself. It learns the user's habits, routines, and missions to recognize proactive opportunities to find, manage, coordinate, preposition, and present information to assist the user in accomplishing work. The agent interfaces with the user through virtual machine guest sessions on a variety of ICT hardware, including desktops, eNotepads, laptops, wearable computers, smartphones, and helmets.

The User and His Virtual Wingman

In this scenario, Lt Col Max Maxwell is the director of operations (DO) for an Air Force expeditionary intelligence squadron. The squadron integrates and deploys Airmen within other services' and partner nations' combat units to directly provide Air Force intelligence capabilities. This means that Colonel Maxwell's Airmen operate within a variety of dissimilar networks.

Coordination of Life

The DO's daily life is directed by numerous schedules from several organizational- and security-driven communities. Fortunately, Colonel Maxwell's Virtual Wingman can negotiate the various networks and consolidate and deconflict the scheduled demands. The wing commander's executive officer e-mails Colonel Maxwell an "invite" to brief the wing commander about the new training program at 10 a.m. tomorrow. Colonel Maxwell's Virtual Wingman agent coordinates this new event across his personal, squadron, wing, classified, and joint service/agency working group calendars. Although the time block is free, the agent recognizes that the squadron commander's staff meeting is at 11 a.m. on the other side of the base. Having learned from previous sessions, the agent recognizes that (1) the wing commander's meeting takes precedence; (2) the wing commander's meetings usually run long; and (3) it takes at least 20 minutes to get from the wing commander's office to the squadron ready room.

Consequently, the agent notifies Colonel Maxwell of the conflict and automatically presents a solution for approval.

With an "OK," the Virtual Wingman sends a text message to the squadron commander: "Tapped by Wing/CC for training program brief. Captain Smith will fill in." Simultaneously, Captain Smith gets a message that he was tagged to fill in. Major Sharp, the assistant DO, would have been cited, but the Virtual Wingman's scan of her schedule showed that she had a higher-priority engagement.

This opening event seems trivial until viewed in the context of our lives. Currently DOD employees have no way to merge their personal, unclassified, classified, and organizational lives into one unified calendar. The 10 minutes spent manually coordinating this single event could have been spent on value-added activities. During the course of the day, such trivial events rob productivity by taking up time and disrupting focus.

Keeping Life Compartmentalized and Consolidated

To prepare for his next deployment, Colonel Maxwell needs to coordinate collection support from Mr. Smart, an IC civil servant. Mr. Smart's contact information originally came from a classified e-mail. Aspects of Mr. Smart's contact information are classified, but the Virtual Wingman, using Colonel Maxwell's security permissions, extracts, parses, and appropriately populates his various network accounts' address books with Mr. Smart's network-appropriate contact information. Using dirty work searches and security guides, the agent knows not to propagate classified information; yet unclassified and unattributable information is transferred.

The Virtual Wingman performs the same type of tasks for several purposes, from distributing recall rosters and forms to conducting customized intelligence searches and autopopulating briefing charts. The Virtual Wingman enables the old axiom "Train like you fight and fight like you train." When Colonel Maxwell and his Airmen are due to deploy, each Airman's Virtual Wingman copies and transfers user profiles, links, templates, software, and so forth to the destination network. For Colonel Maxwell, his contacts and lessons learned from past deployments and assignments follow him into theater and for the rest of his career. As he makes contacts, his Virtual Wingman maintains his electronic address book. Dynamically updating links are established to track both the contact and its past duty position's contact information. This allows Colonel Maxwell to contact his friend Major Striker and provides him with the ability to contact the person now filling Major Striker's old duty billet as the Fort Huachuca joint service training coordinator.

En Route, but Not Disconnected

While traveling at 40,000 feet en route to theater, Colonel Maxwell's Virtual Wingman is both with and ahead of him at the forward operating base (FOB). There, his agent is creating and downloading middleware and mapping links to establish the same functionality in his new tent office as he had stateside. Meanwhile, he uses his laptop to view the latest intelligence by way of encrypted traffic over open commercial satellite links. Then he settles into his sling seat to work on his three captains' promotion recommendation forms (PRF). Prior to departure, the Virtual Wingman scanned the administrative status of the squadron's personnel. Because these three captains were approaching their promotion boards, the agent preemptively pulled their officer performance records (OPR) and forward-stored the files on Colonel Maxwell's laptop for the deployment. As he selects past OPR performance statements and weaves them into the PRF narrative, the Virtual Wingman automatically maps the words and their sources to the required major command PRF source tracking sheet. In doing so, the Virtual Wingman is able to find, locate, and retrieve specific information from within a variety of current and legacy OPR formats and map it to the PRF source tracking sheet. Though this is an arcane example to outsiders, every Air Force field-grade officer can empathize with the countless frustrating hours spent mapping PRF lines that could have been spent honing testaments to the officers' abilities.

Halfway there, Colonel Maxwell's first sergeant reminds him that the new sensor pallet loaded on board will not fit into the previously assigned Stryker IIs. While still en route, Colonel Maxwell accesses US Transportation Command's portal to the Army FOB motor pool to request a vehicle to accommodate the sensor pallet.

FOB Operations

The Airmen can now get to work when they arrive. Local training is minimized, as the Airmen have been training stateside on real data using theater software tools and the electronic tactics, techniques, and procedures that have been replicated between the sites.

Mounted Patrol Operations

Today, Colonel Maxwell is taking a combined team on patrol. Upon assignment to a next-generation Stryker II combat vehicle, his Virtual Wingman uploads and initiates itself as a virtual guest within the vehicle's network. By the time the mounted patrol leaves the FOB, his agent has not only mapped that day's available mobile command and control feeds and frequencies, blue force tracker, and threat, alert, and ISR feeds but also has downloaded the latest maps and mission orders. As the patrol rolls out, its Hunter II RPA is diverted, and it is reassigned an Army Sky Warrior II RPA. Recognizing that the downlinked feed has changed, the patrol lead's agent uses the Stryker II's CR system to initiate a data pull to download the mySkyWarriorII app software into the vehicle's network server and populate it throughout the convoy.

As the patrols rolls onward, the gunner's Virtual Battle Buddy (the Army's version of the Virtual Wingman) monitors the surrounding roadways using the Sky Warrior II's overhead video feed. The Virtual Battle Buddy applies a cognitive video analytics app that combines video computer vision with machine learning. After several patrols and many days of RPA surveillance of an area, the software can distinguish normal from suspicious activity.[132] With time, the software learns patterns of behavior across the course of a day, week, and season as well as responses to events.

Cognitive Video Analytics—BRS Labs' AISight software exploits multiple black/white, color, and near infrared video imagery to monitor areas for abnormal activity. Using machine learning, AISight understands time-of-day, time-space-distance, and proximity factors. AISight is camera agnostic and works as well with four cameras as it does with 100.[133]

The gunner's Virtual Battle Buddy detects a distant anomaly, but it does not distract the gunner with a warning because the gunner's duty is to protect the patrol from near threats. Instead, the gunner's agent routes the alert to the patrol leader's agent. Acknowledging the alert, Colonel Maxwell views video of the suspicious activity. As he radios back his intentions to investigate, his Virtual Wingman comprehends the plan change and proactively plots the least provocative and lowest threat route to position the patrol for dismounted investigation. Upon entering the village, the Virtual Wingman calculates and color-codes a three-dimensional village rendering, made from numerous drive-throughs and RPA overflights, that highlights likely ambush and sniper positions and cones of fire.[134]

Dismounted Operations

Before reaching the dismount point, the Virtual Wingman has reactivated the suspended agent in Colonel Maxwell's helmet and gear. Soon after dismounting, a Coalition Texan II counterinsurgency light-attack plane enters the airspace and broadcasts its presence. The Virtual Wingman agent back in the Stryker II notifies the patrol leadership of the aircraft's availability over the local CR network and initiates a two-way data link with the Coalition Texan II. Unfortunately, the targeting data link is not connecting. The Virtual Wingman initiates a software check and determines the coalition Czech Texan II is running a newer targeting system version than what the host nation Texan IIs uses. Not being able to quickly download a new version, the Virtual Wingman begins to auto-code and test a middleware solution to translate between the old and new versions.

Meanwhile, crouched behind a garden wall, Colonel Maxwell and the Army first sergeant activate the helmet look-through visor monitors. As they move their heads, they can see the village market "through the wall," albeit from a bird's-eye view. Helmet position cues the RPA's sensor turrets. The merger of line-of-sight head position to imagery builds a sense of relational position between the viewer and the image. This is less disorienting than relating flat-screen panned images to physical space.

Shaded in flashing yellow is a congregation of teenagers looking out of place and nervous on the far side of the market square. Over the local wireless network, Colonel Maxwell, the flanking squad Army lieutenant, and the first sergeant coordinate a plan. Having fixed the enemy's location, the lieutenant and sergeant lead their squads into position. Rather than using a map to navigate the alleys, their Virtual Battle Buddies guide them using a mixture of audible, visual, and tactile cues. If something goes wrong, precalculated panic directions will guide them safely back to the Stryker IIs.

At "go," one of the Stryker IIs raises a boom with a microwave dish, aims at the teenagers, and pulses them with a burst.[135] The youths reveal their weapons in involuntary response to the shock. The boom operator, seeing this through the RPA video, starts pulsing the youths into disorientation and stunned shock. As the secured youths recover, a few start talking in a language foreign to the patrol's host nation sergeant. The lieutenant's Virtual Battle Buddy initiates streaming audio back across his agent's negotiated data link to the main operating base's supercomputer for translation. Meanwhile, an Army specialist photographs each captured youth with a smartphone camera. The gigapixel camera captures and forwards details, such as partial retina images.[136]

An FOB intelligence analyst initiates a facial/retina search within the Federal Bureau of Investigation worldwide identity record bank and returns a match.[137] Using a locally created app to search and pull information from local host-nation reports, a human intelligence report from last week links three of the youths to a previous attack. The analyst forwards a summary report to the patrol along with a public relations message automatically translated into local languages by the Virtual Wingman per standard operating procedures established during joint FOB stateside training. As the prisoners are being loaded, the Stryker II's loudspeakers broadcast the translated public affairs message: "The captured youths are responsible for killing 16 women and children last week at a neighboring village market."

As the patrol begins its return trip, recorded mission data streams back to the FOB. The collected video refines the cognitive video analytics rule sets, and conversation and troop movement recordings support after-action analysis.

Battle of Administrivia

After completing the after-action debrief and getting some chow, Colonel Maxwell wages a successful campaign against endless waves of administrivia (the necessary administrative paperwork after mission completion). Fortunately, his Virtual Wingman has already mapped the links and downloaded the patches that allow him to view Air Force forms from the Army host network. As Colonel Maxwell saves and closes his new training brief for the wing commander, his Virtual Wingman, detecting the completion of a task, interrupts with two alerts. His children's bedtime is approaching, and Valentine's Day is in two days. A list of hometown florists that deliver follows the second alert. Colonel Maxwell initiates a personal virtual machine guest on his computer, makes a video call home, orders flowers, and kicks back to play a game of Madden Football 2035 against the cocky battalion commander who beat him last week.

Choices and Consequences

This scenario demonstrates how unstructured data and systems can be harnessed. Technology does play a significant role, but success comes not from rote application of advanced technology but by weaving technology and practices into the fabric of the Airmen's lives. Rather than manipulating technology to make up for weaknesses, Airmen work with technology as a trusted collaborator stitching solutions together. This subtle distinction differentiates the Virtual Wingman scenario from today's operational employment of advanced technology. Success is born from allowing personnel to provide their own support tools and entrusting them to innovate and exploit ICT to its fullest potential.

Currently, the DOD stands at a crossroads on how to embrace and use technology. There are four choices, three of which are unacceptable. The first shuns advanced ICT and maintains centralized control of ICT development and use. The result is people at all levels drowning in information. Without informational efficiency, more information will be available, but there will be no means to make sense of it. Savvy adversaries will adapt to DOD tactics and capabilities and routinely operate inside the DOD's decision loop.

The second choice is to delay accepting new technologies and practices. This forces lone-wolf pockets of initiative to buck the ICT bureaucracy and work within the seams of policy and doctrine to innovatively squeeze rigid institutional infrastructures, processes, and technologies for all they can deliver. Though they achieve short tactical victories, strategic success remains elusive because solutions are neither widely applied nor sustainable.

The third choice represents the DOD's current path of overambitiously embracing technology but bureaucratizing its development and application. The result is that specific technologies are either prematurely rushed, resulting in a capability miscarriage, or are quickly touted but delayed in implementation until they are either out of date or no longer relevant. The GAO found that "the JTRS program for ground vehicles and helicopters began system development in 2002 with none of its 20 critical technologies sufficiently matured and the requirements not clearly defined."[138] Conversely, the DOD's chiefs of information operations identified several useful commercial information management capabilities that are obsolete by the time the specific software or all of the supporting operating systems are installed. This was the case with Microsoft SharePoint's implementation at the National Reconnaissance Office.[139] The result is a costly and frustrating oscillation between premature insertion and catching up.

The fourth and only viable choice is to avoid costly ICT and system-of-systems collapse and to rapidly field capabilities to embrace new technologies and community practices as demonstrated in this paper. However, success requires another element—timing.

How to Harness Unstructured Data and Systems: Diagramming the Way Forward

Timing is an often overlooked element of success. If the timing is off, technologies and practices will not achieve their potential. Virtualization has been around since 1967 but only became widely accepted and used when the hardware to make up for its heavy processing demands became available.[140] Though still requiring much algorithm development, artificial intelligence awaits practical and cost-effective petaflops hardware.

Timing in developing and fielding technology and practices in relation to each other is crucial for success. DIMHRS and JTRS are not bad ideas; however, they underwent acquisitions before the enabling technologies and practices could support the objectives. Sometimes the capability is available, but its form does not fit people's lives, needs, or missions. In 1998 Spotlight Mobile created a laptop application that delivered information based on the user's location. Great idea, but the product flopped until a decade later when smartphones provided the requisite mobile platform.[141]

Similarly, a natural phasing order exists to realizing the Virtual Wingman's embodied capabilities. This relative order of progression can be shrunk or expanded without causing integration problems as long as the relative order is maintained. Figures 1 and 2 illustrate the links between critical maturing communities of practice that enable specific technologies to reach their potential.

This break from a traditional technology investment road map is intentional. The fostering of user communities is as important as funding the development of specific technologies. Without a viable and accepting CoP to create, support, and use specific technologies, needed technologies will remain only bench specimens and concept-of-operations theories.

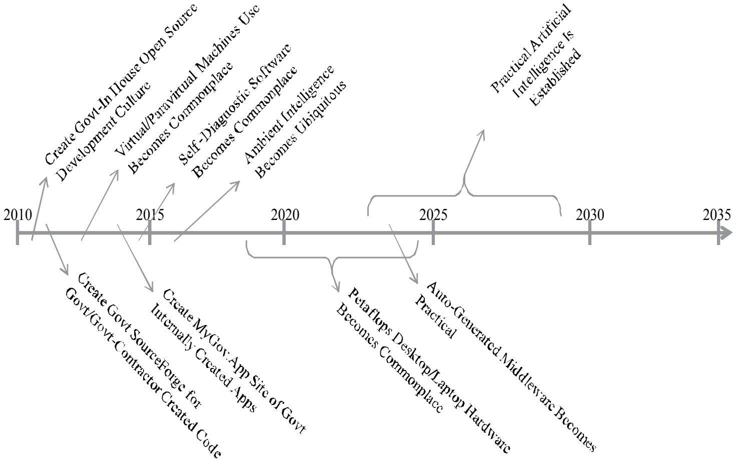

Create Govt-In House Open Source Development Culture
Virtual/Paravirtual Machines Use Becomes Commonplace
Self -Diagnostic Software Becomes Commonplace
Ambient Intelligence Becomes Ubiquitous
Practical Artificial Intelligence Is Established
2010
2015
2020
2025
2030
2035
Create Govt SourceForge for Govt/Govt-Contractor Created Code
Create MyGov.App Site of Govt Internally Created Apps
Petaflops Desktop/Laptop Hardware Becomes Commonplace
Auto-Generated Middleware Becomes Practical

Figure 1. Phasing of technology and practices

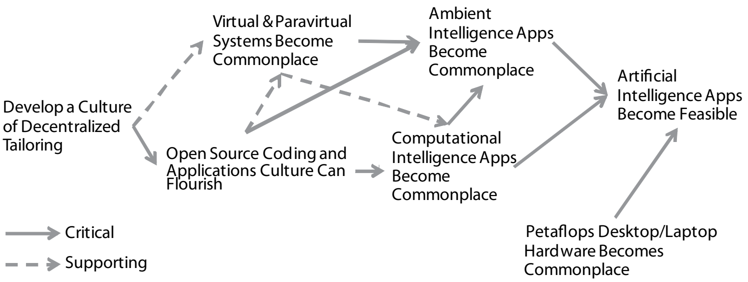

Virtual & Paravirtual Systems Become Commonplace
Ambient Intelligence Apps Become Commonplace
Artificial Intelligence Apps Become Feasible
Develop a Culture of Decentralized Tailoring
Open Source Coding and Applications Culture Can Flourish
Computational Intelligence Apps Become Commonplace
Critical
Supporting
Petaflops Desktop/Laptop Hardware Becomes Commonplace

Figure 2. Cultural and technical critical paths

Conclusion

In "How to Think Outside the Box," a *Business Week Online* article, Bill Buxton remarks that "our lack of attention to place, time, function, and human considerations means that these fancy new technologies fail to deliver their real potential to real people."[142] For the DOD, the answer to how it can best posture itself to harness the rapid growth of unstructured data and infrastructure to achieve mission success is tied not only to specific technologies but to specific practices, building CoPs, and timing the development and integration of the aforementioned pieces.

Virtualization and ambient and artificial intelligence are key technical enablers to focus on for investment purposes. However, these technologies will be made affordable and practical by ensuring open-source practices and a culture of sharing is widely embraced. To accomplish this, the DOD must reconsider the roles of centralized and decentralized acquisitions, development, sharing, and use. Only by enabling the tools to rapidly tailor capabilities and services can the DOD implement technology to tame modern infrastructure's complexities and exploit the infosphere's fog of information.[143]

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Fulghum, "Digital Goes Viral," 74.
2. US GAO, "Information Management," 4.
3. Ibid., 3.

4. US GAO, "Defense Acquisitions," 4, 6.

5. Mancini, "8 Reasons," 6.

6. Fulghum, "Digital Goes Viral," 74.

7. Ibid.

8. Jackson, "Direct Path to Dependable Software," 78–88.

9. Fulghum, "Integration Nightmares," 59.

10. Philpott, "New Pay, Personnel System," 1C, 3C.

11. Jackson, "Direct Path to Dependable Software."

12. Delgado, Laplanche, and Krishnamurthy, "New Face of Enterprise Search," 42.

13. Philpott, "New Pay, Personnel System."

14. Fulghum, "Integration Nightmares."

15. Delgado, Laplanche, and Krishnamurthy, "New Face of Enterprise Search," 42.

16. Gams and Hribovšek, "Intelligent-Personal Agent Interface," 354.

17. Custer, address, 2008 National Geospatial-Intelligence (GEOINT) Agency Conference.

18. Ibid.

19. Delgado, Laplanche, and Krishnamurthy, "New Face of Enterprise Search."

20. Ibid., 42.

21. Ibid.; and Li, Zhang, and Zhang, "Cooperative Strategy for Web Data Mining," 443.

22. Custer, address, 2008 GEOINT conference.

23. Ibid.

24. Ibid.

25. Ibid.

26. Carlson, "Verizon Unifies Communications," 1.

27. Bednarz, "Users Turn to Virtual Data Marts," 56.

28. Coombs, *Acquisition Leaders for Rapid Technology*, 2.

29. Custer, "Reach: Leveraging Time and Distance," 4.

30. Quote attributed to Daniel J. Boorstin in Gamarekian, "Working Profile," B6.

31. Chilton, "Cyberspace Leadership," 5–10.

32. US DOD, *National Military Strategy,* 13.

33. Ibid., 14.

34. Ibid.

35. Ibid., 18.

36. Joint Publication 4-0, *Joint Logistics*, I-5.

37. Dail and Jones, "Deployment and Distribution Command and Control," 168.

38. Mancini, "8 Reasons."

39. US GAO, "Information Management," 7.

40. Quote attributed to Daniel J. Boorstin in Gamarekian, "Working Profile," B6.

41. Kramer, Starr, and Wentz, *Cyberpower and National Security,* 346; and Mancini, "8 Reasons," 6.

42. Multispectral and hyperspectral imaging modes collect, respectively, tens and hundreds of different wavelength images per collection (the standard

color camera collects three wavelengths: red, green, blue). Many ISR assets also collect the near-infrared wavelength. Eshel, “Off-The-Shelf Black Ops,” 46.

43. Kramer, Starr, and Wentz, *Cyberpower and National Security*, 346.

44. Charles, “New Industry Norms,” 69.

45. Mancini, “8 Reasons,” 6.

46. Charles, “New Industry Norms.”

47. Michelis, Loregian, and Moderini, “itsme,” 71.

48. Ibid., 72.

49. Remagnino and Shapiro, “Artificial Intelligence Methods,” 393.

50. Rodríguez et al., “Agent-based Ambient Intelligence,” 201.

51. Ibid.

52. Vivienne Waller is a research fellow at the Institute for Social Research, Swinburne University of Technology, Melbourne, Australia. Robert B. Johnston is director of the Centre for Innovation, Technology, and Organization and a John Sharkey professor of information systems and organization at University College, Dublin, Ireland. Waller and Johnston, “Making Ubiquitous Computing Available,” 128.

53. Ibid.

54. Ibid., 129.

55. Rodríguez et al., “Agent-based Ambient Intelligence,” 205.

56. Waller and Johnston, “Making Ubiquitous Computing Available.”

57. Gomes and Buley, “PC Is Dead,” 51–53.

58. Cardwell, “Virtualization,” 26.

59. Naone, “Conjuring Clouds,” 54.

60. “Virtual Worlds,” 30.

61. Naone, “Conjuring Clouds.”

62. Lindstrom, “5 Laws of Virtualization Security,” 56.

63. Ibid.

64. Ibid, 57.

65. Cardwell, “Virtualization,” 26.

66. Gomes and Buley, “PC Is Dead,” 51–53.

67. Naone, “Conjuring Clouds,” 54.

68. Ibid., 56.

69. Ibid., 54.

70. Walko, “Cognitive Radio,” 34.

71. Ibid.

72. Ibid., 36.

73. Ibid.

74. Ibid.

75. Cardwell, “Virtualization,” 28.

76. Gomes and Buley, “PC Is Dead,” 51–53; and Lindstrom, “5 Laws of Virtualization Security,” 56.

77. US GAO, “Defense Acquisitions.”

78. Ibid., 6; and Bisker, “Progressively Smarter,” 94.

79. Bisker, “Progressively Smarter,” 94.

80. US DOD, *National Defense Strategy*, 19.

81. US GAO, “Defense Acquisitions,” 21.

82. Schley, “Stuck in the Middle,” 16.

83. Cardwell, “Virtualization,” 28.

84. Abejo, “An Opening,” 58–84.

85. Haefliger, von Krogh, and Spaeth, "Code Reuse," 180.

86. Ibid., 183.

87. Biggs, "Revenge of the Coders," 48–52; and Haefliger, von Krogh, and Spaeth, "Code Reuse," 180–93.

88. Haefliger, von Krogh, and Spaeth, "Code Reuse," 191.

89. Ibid.

90. Watson et al., "Business of Open Source," 41–46.

91. Biggs, "Revenge of the Coders," 48–52; and Haefliger, von Krogh, and Spaeth, "Code Reuse," 180–93.

92. Abejo, "An Opening."

93. Ibid.

94. Ibid.

95. Ibid.

96. Source Forge, http://sourceforge.net/about.

97. Haefliger, von Krogh, and Spaeth, "Code Reuse," 191.

98. Jeffries, "Kickin' Apps."

99. Ibid.

100. Ibid.

101. General Services Administration, "Apps.Gov."

102. Lieberman and Fry, "Will Software Ever Work?," 123.

103. Ibid.

104. Ibid., 124.

105. Chandler, "Rethinking Artificial Intelligence."

106. Ibid.

107. Mannings, "What Technology?" 13.

108. Ibid.

109. Castellano, Fanelli, and Torsello, "Computational Intelligence Techniques," 258.

110. Mannings, "What Technology?"

111. Castellano, Fanelli, and Torsello, "Computational Intelligence Techniques."

112. Ibid., 259.

113. Chilton, "Cyberspace Leadership."

114. Gams and Hribovšek, "Intelligent-Personal Agent Interface."

115. Ibid., 377.

116. Lindstrom, "5 Laws of Virtualization Security."

117. Provos, Rajab, and Mavrommatis, "Cybercrime 2.0," 46.

118. Ibid.

119. Krebs, "Internet Explorer Unsafe," and "Blogfight."

120. Chilton, "Cyberspace Leadership."

121. Lindstrom, "5 Laws of Virtualization Security," 57; Provos, Rajab, and Mavrommatis, "Cybercrime 2.0," 46; and Sweetman, "Net: Superglue," 43.

122. Lindstrom, "5 Laws of Virtualization Security."

123. Provos, Rajab, and Mavrommatis, "Cybercrime 2.0."

124. Lindstrom, "5 Laws of Virtualization Security," 57.

125. Ibid.

126. Ibid.

127. Ibid.

128. "Virtual Worlds," 31; and Lindstrom, "5 Laws of Virtualization Security."

129. “Virtual Worlds,” 32.

130. Lindstrom, “5 Laws of Virtualization Security,” 55.

131. Bolzani and Netto, “Engineering of Micro Agents,” 34.

132. Walsh, “Watch and Learn,” 25.

133. Ibid., 25–26.

134. O’Reilly and Battelle, “Web Squared.”

135. Air Force Research Laboratory Directed Energy Directorate, “High-Power Microwaves.”

136. O’Reilly and Battelle, “Web Squared.”

137. Weinberger, “Fingerprints International,” 22.

138. US GAO, “Defense Acquisitions,” 11.

139. From the author’s personal experience at the National Reconnaissance Office (NRO) while part of a working group to improve collaboration across the NRO’s various research and development, rapid prototyping, and fielding and sustainment organizations.

140. Naone, “Conjuring Clouds.”

141. Jeffries, “Kickin’ Apps.”

142. Buxton, “How to Think Outside the Box,” 24.

143. Quote attributed to Daniel J. Bonstin in Gamarekian, “Working Profile.”

Bibliography

Abejo, Jerry. "An Opening." *Mergers & Acquisitions: The Dealmaker's Journal* 43, no. 4 (April 2008): 58–84.

Air Force Research Laboratory Directed Energy Directorate. "High-Power Microwaves." US Air Force Fact Sheet, 9 April 2009. Accessed 1 April 2010. http://www.kirtland.af.mil/library/factsheets/factsheet_print.asp.

Bednarz, Ann. "Users Turn to Virtual Data Marts." *Network World* 21, no. 16 (19 April 2004): 1.

Biggs, Maggie. "Revenge of the Coders." *InfoWorld* 25, no. 37 (22 September 2003): 48–52.

Bisker, Jaime. "Progressively Smarter." *Best's Review* 110, no. 5 (September 2009): 94.

Bolzani, Caio Augustus Morais, and Marcio Lobo Netto. "The Engineering of Micro Agents in Smart Environments." *International Journal of Knowledge-Based Intelligent Engineering Systems* 13, no. 1 (March 2009): 31–38.

Buxton, Bill. "How to Think Outside the Box." *BusinessWeek* (31 March 2009): 24.

Cardwell, Travis. "Virtualization." *J@pan Inc.* no. 74 (November 2007): 26–30.

Carlson, Caron. "Verizon Unifies Communications." *Network World* 21, no. 16 (19 April 2004): 1.

Castellano, Giovanna, Anna Maria Fanelli, and Maria Alessandra Torsello. "Computational Intelligence Techniques for Web Personalization." *Web Intelligence and Agent Systems* 6, no. 3 (September 2008): 253–72.

Chandler, David L. "Rethinking Artificial Intelligence." *MIT News*, 7 December 2009. Accessed 1 April 2010. http://web.mit.edu/newsoffice/2009/ai-overview-1207.html.

Charles, Sherry. "New Industry Norms Give Rise to Abundant Opportunities." *Global Telecoms Business* no. 110 (December 2009): 69.

Chilton, Gen Kevin P. "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities." *Air and Space Power Journal* 23, no. 3 (Fall 2009). Accessed 29 September 2009. http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/chilton.html.

Coombs, Lt Col Christopher M. *Acquisition Leaders for Rapid Technology Insertion Programs*. Blue Horizons Paper. Maxwell AFB, AL: Air War College, December 2007.

Custer III, Maj Gen John M, commander, US Army Intelligence Center. Address. 2008 National Geospatial-Intelligence Agency (GEOINT) Conference, Nashville, TN, 29 October 2008.

———. "Reach: Leveraging Time and Distance." *Military Review* 83, no. 2 (March 2003): 3.

Dail, Lt Gen Robert T., and Lt Col David E. Jones. "Deployment and Distribution Command and Control." In *Joint Campaign Planning AY10 Coursebook.* Edited by Sharon McBride, 161–69. Maxwell AFB, AL: Air Command and Staff College, January 2010.

Delgado, Joaquin, Renaud Laplanche, and Viswanathan Krishnamurthy. "The New Face of Enterprise Search: Bridging Structured and Unstructured Information." *Information Management Journal* 39, no. 6 (November 2005): 40–46.

Eshel, David. "Off-The-Shelf Black Ops." *Defense Technology International*, November 2009, 46.

Fulghum, David A. "Digital Goes Viral." *Aviation Week and Space Technology*, 9 November 2009, 74.

———. "Integration Nightmares." *Aviation Week and Space Technology*, 5 October 2009, 59.

Gamarekian, Barbara. "Working Profile: Daniel J. Boorstin, Helping the Library of Congress Fulfill Its Mission." *New York Times*, 8 July 1983, B6. Accessed 15 December 2009. http://www.todayinsci.com/QuotationsCategories/F_Cat/Fog-Quotations.htm.

Gams, Matjaz, and Borut Hribovšek. "Intelligent-Personal Agent Interface for Operating Systems." *Applied Artificial Intelligence* 10, no. 4 (20 July 1996): 353–83.

General Services Administration. "Apps.Gov." Accessed 31 January 2010. http://apps.gov/cloud/advantage/main/start_page.do.

Gomes, Lee, and Taylor Buley. "The PC Is Dead." *Forbes* 184, no. 12 (28 December 2009): 51–53.

Haefliger, Stefan, Georg von Krogh, and Sebastian Spaeth. "Code Reuse in Open Source Software." *Management Science* 54, no. 1 (January 2008): 180–93.

Jackson, Daniel. "A Direct Path to Dependable Software." *Communications of the ACM* 52, no. 4 (April 2009): 78–88.

Jeffries, Adrianne. "Kickin' Apps." *Oregon Business Magazine* 32, no. 8 (August 2009): 20–25.

Joint Publication 4-0. *Joint Logistics*, 18 July 2008.

Kramer, Franklin D., Stuart H. Starr, and Larry K Wentz. *Cyberpower and National Security*. Washington, DC: Potomac Books, Inc., 2009.

Krebs, Brian. "Blogfight: IE vs. Firefox Security." *Washington Post Online Blog*, 29 January 2009. http://voices.washingtonpost.com/securityfix/2009/01/blogfight_the_truth_about_ie_v.html.

———. "Internet Explorer Unsafe for 284 Days in 2006." *Washington Post Online Blog*, 4 January 2007. http://voices.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html.

Li, Yuefeng, Chengqi Zhang, and Shichao Zhang. "Cooperative Strategy for Web Data Mining and Cleaning. "*Applied Artificial Intelligence* 17, no. 5/6 (May 2003): 443.

Lieberman, Henry, and Christopher Fry. "Will Software Ever Work?" *Communications of the ACM* 44, no. 3 (March 2001): 122–24.

Lindstrom, Pete. "5 Laws of Virtualization Security." *Baseline* no. 84 (May 2008): 54.

Mancini, John F. "8 Reasons You Need a Strategy for Managing Information." *Infonomics* 23, no. 5 (September 2009): 6.

Mannings, Robin. "What Technology Will Managers of the Future Be Using?"*British Journal of Administrative Management* no. 58 (April 2007): 12–13.

Michelis, Giorgio De, Marco Loregian, and Claudio Moderini. "itsme: Interaction Design Innovating Workstations." *Knowledge, Technology & Policy* 22, no. 1 (Spring 2009): 71–78.

Naone, Erica. "Conjuring Clouds." *Technology Review* 112, no. 4 (July 2009): 54–56.

O'Reilly, Tim, and John Battelle. "Web Squared: Web 2.0 Five Years On." San Francisco, CA: Web 2.0 Summit 2009. Accessed 29 September 2009. http://www.web2summit.com/web2009/public/schedule/detail/10194.

Philpott, Tom. "New Pay, Personnel System Dumped as a 'Disaster.'" *Montgomery Advertiser*, 21 February 2010, 1C and 3C.

Provos, Niels, Moheeb Abu Rajab, and Panayiotis Mavrommatis. “Cybercrime 2.0: When the Cloud Turns Dark.” *Communications of the ACM* 52, no. 4 (April 2009): 42–47.

Remagnino, Paolo, and Daniel Shapiro. “Artificial Intelligence Methods for Ambient Intelligence.” *Computational Intelligence* 23, no. 4 (November 2007): 393–94.

Rodríguez, Marcela D., Jesús Favela, Alfredo Preciado, and Aurora Vizcaino. “Agent-Based Ambient Intelligence for Healthcare.” *AI Communications* 18, no. 3 (September 2005): 201–16.

Schley, Stewart. “Stuck in the Middle.” *CED* 35, no. 10 (October 2009): 16.

Source Forge. Accessed 16 February 2010. http://sourceforge.net/about.

Sweetman, Bill. “The Net: Superglue.” *Defense Technology International*, February 2010, 43.

“$250 Million Supercomputer Headed to Petaflop Rates.” *Machine Design* 79, no. 3 (8 February 2007): 36.

US Department of Defense (DOD). *National Defense Strategy of the United States of America.* Washington, DC: DOD, June 2008.

———. *National Military Strategy of the United States of America.* Washington DC: DOD, May 2004.

US Government Accountability Office. “Defense Acquisitions: Department of Defense Needs Framework for Balancing Investments in Tactical Radios.” *Report to the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives*, GAO-08-877, August 2008.

———. “Information Management: Challenges in Implementing an Electronic Records Archive.” *Testimony—Statement of Linda Koontz, Director, Information Management Issues*, GAO-08-738T, 14 May 2008.

“Virtual Worlds.” *SC Magazine: For IT Security Professionals*, October 2009, 30–33.

Walko, John. “Cognitive Radio.” *IEE Review* 51, no. 5 (May 2005): 34–37.

Waller, Vivienne, and Robert B. Johnston. “Making Ubiquitous Computing Available.” *Communications of the ACM* 52, no. 10 (October 2009): 127–30.

Walsh, David. “Watch and Learn: Cognitive Video Software Detects a Range of Threat Behaviors.” *Defense Technology International*, February 2010, 25–26.

Watson, Richard T., Marie-Claude Boudreau, Paul T. York, Martina E. Greiner, and Donald Wynn, Jr. “The Business of Open Source.” *Communications of the ACM* 51, no. 4 (April 2008): 41–46.

Weinberger, Sharon. “Fingerprints International.” *Defense Technology International*, November 2009, 22–23.

Abbreviations

AI	artificial intelligence
AmI	ambient intelligence
apps	applications
CI	computational intelligence
COTS	commercial-off-the-shelf
CR	cognitive radio
DIMHRS	Defense Integrated Military Human Resources System
DOD	Department of Defense
EO/IRI	electro-optical/infrared
FCC	Federal Communications Commission
FMV	full motion video
FOB	forward operating base
GAO	Government Accountability Office
GIS	geographic information system
GOTS	government-off-the-shelf
IC	intelligence community
ICT	information and communication technology
IEEE	Institution of Electrical Engineers
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
JTRS	joint tactical radio system
Mbps	megabits per second
mil-spec	military specifications
MIT	Massachusetts Institute of Technology
NMS	National Military Strategy
OPR	officer performance record
OS	operating systems
PC	personal computer
PRF	promotion recommendation form
RPA	remotely piloted aircraft
SDR	software-defined radio
SIGINT	signals intelligence
SOA	service-oriented architecture
USTRANSCOM	US Strategic Command

AU PRESS
http://aupress.au.af.mil