Released Online
25 February 1999

CONTENTS

Introduction

A Revolution in Military Affairs

Being on a Knowledge Grid

Issues

Who Gets What?

And For What in Return?

How Open Should it Be?

Frustrating Abuse

Concluding Considerations

virtual Diplomacy

WWW.U.S.DoD.Com

Martin Libicki

Introduction

Over the past decade, information superiority has become widely acknowledged as the future source of continued U.S. military power.

Information is a force multiplier and a time accelerator. Knowledge leads to better decisions made faster. Always-scarce resources can be leveraged with greater precision and thus greater effect. Those who know less can be outmaneuvered and outgunned.

As an input to military power, information has been considered analogous to other inputs: ammunition, manpower, or petroleum products. Typically, therefore, the warfighter wants to have more of it with its adversaries having less. Intelligence entities, traditionally the vanguard of the state's and military's information apparatus, assiduously seek out information (particularly information that no one else has) and jealously prevent adversaries from getting it, or at least, for getting it straight. The very concept of information warfare, as such, rests on the assumption that the possession of good information is a zero-sum game.

Yet, turning from the world of war to the world of commerce reveals that information plays a far different role. Consider the information in an advertisement; owners go to great lengths to put it before one and all (and while some of its content may be false, its economics would be the same were it all true). In the world of high technology, detailed information about the specifications of a hardware or software product is distributed to increase its value to potential end-users and help suppliers and downstream value-added integrators prepare supporting wares -- all of which collectively make the original product more valuable. Motorola, for instance, releases the specifications of its integrated circuits well in advance of releasing the chips themselves so that vendors can prepare products which incorporate them. Wal-Mart has even gone so far as to integrate its own inventory-accounting systems with those of its primary suppliers. Thus, Proctor & Gamble would know when to resupply soap to Wal-Mart warehouses almost before Wal-Mart knew it needed some. Even rivals exchange information for the purpose of creating information technology standards (e.g., those that govern computer modems). Granted, not all information is released for benign purposes; IBM used to announce wonderful features of products that were months and years away from being available in order to keep customers from being swayed by the siren songs of competitors. And, of course, some information, such as proprietary research results or bid strategies, is closely protected. But, on the whole, businesspeople tend to think of information as something that can be released for gain, while warfighters see information as something to be squirreled away.

Are warfighters correct in having different attitudes than businesspeople do toward information? Both compete and both seek advantage where it can be found; in that sense, they are in similar lines of zero-sum work. But statecraft -- of which military power is just one instrument -- is not a zero-sum game. Indeed, in today's geo-strategic climate, a passion for stability that manifests itself in a live-and-let-live attitude is much more pervasive than it is in high-tech industry.

Indeed, the laws of information may have more fundamental roots. Either their economics have changed

or, as Carl Shapiro and Hal Varian argue in Information Rules, the major parameters through which the eternal laws of economics apply have changed. Key principles should hold whether the competition occurs among firms striving for profit or states (as well as super-, sub- and non-state organizations) seeking power and security.

Businesspeople may simply be ahead of the curve because they must adapt rapidly to survive as long as the technical foundations of their businesses keep shifting in Internet-time. Literally billions of dollars are being invested in order to find a good business model for the World Wide Web -- which, after all, is a construct for giving away large quantities of information. In hopes that it has, the stock market has rewarded Yahoo.com, Amazon.com, America On-Line, Ebay.com, and Microsoft even after it has poured money into model-wannabes notable only for mistakes. Warfighters can be as intelligent and adaptive (compare 1991's Desert Storm with 1995's Bosnian air operations with late 1998's Desert Fox). But in today's largely peaceful era, reliable feedback on how to position information for strategic advantage is hard to come by. So warfighters cannot help but look over their shoulders at those who live and die by feedback.

And so the U.S. military may ask how it would use information -- in today's vast quantities -- as businesspeople do. It should seek to use it not just operationally -- to improve its own warfare capabilities -- but strategically, to shape its environment vis-à-vis allies, friends, coalition partners, and even unaligned powers (presumably, sworn enemies are beyond shaping). This essay will examine one possible approach: that the United States establish what would be, in effect, the world's "coolest" Web site, illuminating the world in ways that make aggression and surprise particularly difficult. In doing so, The Department of Defense (DoD) should take seriously strategies at home in Silicon Valley: attracting visitors, gaining user confidence, converting portals into corridors, enticing partners, fostering a structure of value-added products and services in which it holds the center position, but all the while co-opting and thereby preempting rival capabilities.

This possibility is explored in three parts. The first is a quick spin through the current revolution in military affairs (RMA) to explain the new relationship of information to military capability. The second lays out a rationale for how to make information available outside DoD. The third raises several issues that would affect the architecture of the site to accommodate approved information dissemination.

A Revolution in Military Affairs

Twenty years ago, then-Undersecretary of Defense William Perry predicted that the United States would soon be able to kill everything that it could hit, hit everything it could see, and see virtually every important target on the modern battlefield. With the usual caveats about how soon is soon, he appears to be correct.

For the most part, the instrument that makes information so deadly is the precision guided munition (PGM). PGMs include (1) human-guided weapons such as Tube Launched Optically Tracked Wire Guided Missile (TOW) antitank rounds or laser-guided bombs and shells, (2) seeker-guided munitions such as antiaircraft or antiship missiles (and torpedoes), and (3) point-directed ballistic and cruise missiles, including those that use global positioning system (GPS) receivers to guide themselves to a predetermined latitude and longitude. New weapons may even be made to follow a continuously updated set of externally calculated points to hit a moving target.

Whether a munition is provided with a precise end-point or finds the end-point itself is more than an engineering detail; it determines how information plays in warfare. To hit fixed targets, PGMs need to do little but receive (rather than determine) their end-points (unless exacting precision -- when being off by ten feet is too much -- is called for or GPS is too vulnerable). It is still unsettled whether and when it makes more sense to have the weapon's internal sensors find moving targets as opposed to having sensors external to the weapon do so and then tell the missile where to go. Clearly, though, the more precisely the target's position is known in advance, the smaller the area that a PGM must search, the easier the job it has, and the more likely it is to hit its target. Ultimately, a weapon that needs only to compare its own position to with that of the target is likelier to be cheap. Internal sensors -- the major part of a PGM's cost -- tend to be expensive largely because they must be squeezed into a very small container: the PGM's head. Against a robust defense, saturation attacks by expensive PGMs may be unaffordable, and so cheap weapons, which are externally directed, may be the only way to go. The greater the importance of accurate external guidance (i.e., the ability to spot each tank rather than the tank column as a whole), the greater the need for precise illumination that distinguishes targets from their backgrounds.

Illumination, in turn, is a matter of scanning the environment, sifting through it for telltale indicators and worthwhile targets, and sorting through the findings to determine what should be struck. Information can

be collected from human sources such as intelligence operatives, warfighters in contact with enemy forces, and third-party witnesses. Increasingly, though, information is collected from sensors to take economic advantage of ever-cheaper silicon, generate digital data for subsequent manipulation, see from the right vantage point, and minimize the potential for casualties. Sensors come in all types, from electro-optical (e.g., cameras) to infrared, laser scanner, millimeter wave, radar (including synthetic aperture radar that can see through clouds), acoustic, and biochemical. They sit on spacecraft, aircraft, unmanned aerial vehicles, ships, submarines, vehicles, soldiers, and even wherever they land on the ground. With every year, sensors get better -- more accurate, faster, and more acute. The denser the environment or the more cover and concealment that is being used, the greater the profusion of sensors necessary to get a good reading of the battlespace. The mirage of the all-powerful, do-it-all, stand-alone sensor is exactly that; future sensors are more likely to become an element of a larger sensing fabric -- a contributor to a knowledge base rather than its creator. Almost needless to add, the information sensors provide achieves its highest value only when it can be routed to shooters while the target is still exposed, and, if necessary, to weapons in real time.

All these developments are hastening the transition of the U.S. military from a platform-centric structure, through its evolving network-centric incarnation, and ultimately to what may be termed a knowledge-centric organization. Knowledge, in this case, refers to the best continuous estimate of what is where in the battlespace. Fed by various sensors and reporters, such knowledge becomes the foundation for all subsequent actions -- the common reference point for decision and the source of shared situational awareness among warfighters.

Where does this knowledge base reside? Perhaps it is contained in one big box. More likely the knowledge base is virtual -- bits and pieces of it are contained on various servers. It comes together in different combinations depending on what question it has been asked. (It would help if such information were universally self-consistent, a feature that any large heterogenous knowledge base can approach but probably never reach.) More attainable is having such information globally accessible, so that disparate pieces can be fused into a coherent whole; failing that, differing estimates of the same phenomenon can be looked at and compared by users. Indeed, the purpose of being able to look at the battlespace through many differing lenses, so to speak, is that what is good at spotting may be poor at tracking; what may be good at identification may be poor at differentiation; what is fooled by camouflage may be corrected by what is not; uncertainties from one vantage point may be resolved from another, and so on.

If the secret of seeing the battlespace is to look with many eyes operating in many media, the pointlessness of constructing a synoptic view by assets belonging only to separate ground, naval, air, or space forces is obvious. With the increasing range of both sensors and weapons (plus the shift of the U.S. Navy from blue- to brown-water operations), each of the various services is in each other's business. One may imagine littoral operations being planned from satellite-collected information; swiftly augmented by an air picture collected by over-the-horizon Aegis ships and AWACS aircraft, and further refined by imagery collected from unmanned aerial vehicles, U-2s, and JSTARS; supplemented by data from scattered ground-based sensors; correlated by local intelligence sources; and interpreted with the help of special operators, Rangers, and Marines. Correlation and fusion would be the hallmarks of this information environment just as they are in the real world where people amass their insights from whatever comes their way -- without being bothered about who owns what source. If seeing and hitting replaces force on force, then the platforms around which services were organized lose their pride of autonomy. Networks are being used to bring platforms together to realize synergies; indeed, networking embodies today's vision of jointness. Knowledge is joint; in a knowledge-based world, separate services are the artifact. The DoD's emerging Common Operational Picture reflects that fact.

Being on a Knowledge Grid

Now take this picture one step further, and posit the same littoral operation conducted, not only by U.S. forces, but by North Atlantic Treaty Organization (NATO) member forces. The variety of users necessarily increases. When allies have information capabilities of their own, the variety of contributors also rises. In an informaticized world, a knowledge base that covers NATO is key to warfighting.

Seamlessness counts. Exactly which components (sensors, switches, processors, or data files) of a knowledge base are owned by whom ought to matter less than such features as reliability, accessibility, interoperability, and security. Data from a British Unmanned Aerial Vehicle's (UAV's) electro-optical sensor can be linked through a U.S. network to readings from Dutch microphones, so that the data flows can be fused with the help of a French-hosted software agent and compared with a German-provided

database of marine templates to provide targeting guidance to a topside gun on an Italian frigate. All this requires information to be mutually accessible, unhindered by unnecessary classification, and similar enough in format to be exchanged -- even if U.S. forces typically collect most of it and NATO forces tend to be users. Finally, as long as the doctrines and equipment of NATO allies vary from what U.S. forces are used to, it would be useful if each of the allies could use the common knowledge base to construct for themselves realities that answer the questions they have, rather than some standard set that Americans may presume everyone has.

In many ways the engineering and cultural challenges of pulling together a combined knowledge base are straightforward. The U.S. Army may more easily work with its German counterpart with which it has exercised for a half-century than with the U.S. Marines, much less the U.S. Navy. Within NATO, arrangements to standardize equipment and share certain types of information have been ongoing for several decades. Great pains have been taken to ensure that equipment is rationalized, standardized, and interoperational across nations.

But the politics of pulling together a combined knowledge base may be more daunting. Jointness has painfully come together, in large part, through the empowerment not just of the Office of the Secretary of Defense, but joint agencies and newly powerful Commander-in-Chiefdoms. It helps that all DoD budgets have to pass through the same wickets and all major programs have to adhere to the same checklist. No common instruments of comparable strength characterize NATO, where every member nation must ante up its own resources. Intelligence agencies, which contribute a large share of the required information, are themselves very nationalistic. Thus a common NATO knowledge grid cannot simply happen through low-level coordination; there must be explicit policy guidance and, in some cases, explicit international agreement.

This example is not limited to NATO. Bilateral alliances such as those with Japan and Australia may merit access to a similar common knowledge base. Further extension to pick up allies of the third world must also be considered. The United States has fought three major theater wars since V-J Day, all of them alongside and in defense of nations with which it was not formally allied before fighting started. Tomorrow's allies will need not just firepower but information; after all, they are likely not only to have systems of their own to be fed, but also precision weaponry that requires precision information to be effective. The support the United States would get from allied forces would be greater if they could access the U.S. knowledge base -- even if no arrangements had been made in advance for them to tap into or contribute to it.

Coalition operations follow a similar logic. So far, Bosnian operations have made do with ad hoc arrangements because the intensity and scale of military operations have been modest. But even the mostly benignly begun peace operations can turn ugly fast (e.g., Mogadishu). Thus, the requirement for an up-to-the-minute knowledge base may arise whenever coalitions are formed.

Perhaps it makes sense to keep such combined illumination on in peacetime, not only to get day-to-day practice with potential partners but also because illumination in general feeds transparency that may ward off war. Transparency, notably human-scale transparency (i.e., with one meter resolution, give or take a factor of three) makes it more likely that the large moving objects with which nations have historically attacked and controlled other nations' territory can be reliably and precisely seen -- and thus made more vulnerable. By contrast, the weapons that would destroy them tend to be smaller, need not intimidate passersby to have psychological effect (and thus need not draw attention to themselves), and can be hidden within the large expanses defined by their range (i.e., a missile with a 20 km range can be placed anywhere within a circle of 1,250 km with its center as the target -- a circle roughly the size of Maryland's Montgomery County). Transparency is friendlier to the weapon than the platform. Illumination, for instance, could make some future demilitarized Golan Heights harder to violate without invaders risking lethal consequences.

Furthermore, to the extent that preparations for certain kinds of conflict necessarily take place outdoors, illumination that stretches back from the border into the hinterlands may deter the mobilization that is prefatory to war. As a general rule, factors that penalize surprise make war -- even pre-emptive war -- less attractive. Similarly, as Cold War negotiators assumed, transparency supports the building of confidence, which reduces tensions when neither side has an interest in building them up.

Transparency that obtains because at least one party can see everything is better than no transparency at all. During the Cold War, the United States kept the Soviet Union under surveillance with its very highly classified systems and the Soviet Union, in turn, kept the United States under close watch. But mutually assured transparency -- of which Open Skies is one form -- may be both more efficient and a surer path to building confidence. The UAV that flies at will can see more than one that must stop at the border. Although space-based remote sensing need acquire no nation's permission, airborne assets can often see better, provide real-time coverage, and acquire information that cannot traverse any type of

vacuum: acoustic, pressure, and/or chemical traces. Ground-based sensors add further detail, and while it may sound far-fetched to have countries accept internationally monitored ground sensors within their borders, such a network has actually been established for seismic events (e.g., nuclear tests).

The threat of transparency may have benign effects even before indications and warnings are received. A nation that resists disclosure and evades illumination surely must have something to hide; one that facilitates it (or even monitors itself and broadcasts the results) is either unbelievably clever, or more likely, not doing anything it purports not to be doing. In a world with more than two nations, mutual and public transparency helps reassure others that what looks like competition is not a cover for bilateral connivance against the rest of the world (e.g., China's or India's comments about membership in the superpower or nuclear club). Needless to add, the exchange of data among friends, contributes much less to stability than the exchange of data among those who otherwise regard each other with gimlet eyes. Confidence-building is a valuable exercise precisely among those who would otherwise enjoy little confidence in each other.

An information infrastructure fed from robust sensors, maintaining detailed data bases, and hosting rich capabilities for geographically based analysis may also serve civilian purposes. Unaligned nations may be initially more interested in cooperating on disaster relief, environmental monitoring, public health assessment, transportation control, land-use regulation, and law enforcement than on defense. International cooperation among civilian bureaucrats is a good way to bind nations into mutually reinforcing relationships. Will such relationships ensure stability? There is little guarantee that the civilians can overrule national security bureaucrats in matters of state, but they do constitute an interest group that can lobby on behalf of keeping lines open. Computer lines, because of their powerful capabilities, are yet one more tie that may bind. Suspicious nations may feel more comfortable accepting such lines if the salespeople represent other communities; trading data to work global issues may make parallel cooperation on international security issues an easier sell down the road.

Were nations to put themselves on this knowledge grid, acquire confidence in each other through mutual transparency, and use the common frame of reference to facilitate working together in military operations, the benefits to DoD could outweigh the costs and risks of extending itself. But the United States would be even better off if, close friends aside, other nations felt enough confidence in what they get for free to abjure investing in their own C4ISR (command-and-control, communications, computers, intelligence, surveillance, and reconnaissance) capabilities, or structure them so that they achieve their greatest utility only through the knowledge grid (e.g., by relying on certain specialized capabilities found there). After all, the alternative to reliance is duplicating such capabilities themselves -- a proposition that is difficult for any nation that lacks economies of scale or has a late start in establishing comparable capabilities. However, if nations are to rely on this knowledge grid, it must itself be reliable, not just technically, but politically. It must be continually available, especially when storm clouds arise. It ought to be withheld only under the most exceptional conditions. This means that the United States, for its part, keeps up the links in all crises short of war (e.g., the face-off with China during the Straits of Taiwan incident), and even if recipients make what the United States considers improper use of the information (e.g., violate human rights, as many third world militaries do).

Demonstrated reliability is a tall order that requires considerable self-restraint not only from the DoD but from Congress. Realizing that others may learn to take what they would normally buy also requires great patience. Conversely, no great-power wannabe will immediately give up its independent C4ISR powers upon linking to the knowledge grid. Indeed, the first nations likely to cut back are those that have the greatest confidence in the United States -- and thus whose capabilities are most likely to benefit the United States. Any strategy for interdependence must count on the persuasive powers of tight-fisted accountants who would rather not throw money into buying what is available free by plugging in. It may take a decade or more before the overall balance of curtailed expenditures favors U.S. interests (and knowing whether other nations have built some capabilities on the side will not be easy).

Other nations may demand, in return, that the United States become dependent on them as well -- so that the U.S. ability to wage war is diminished if formerly cooperating nations withdraw their own contribution (e.g., a sensor, database, or service). But this demand may rebound to the U.S. advantage if the United States could show that it, too, could not act unilaterally without the consent of others. The public demonstration of unavoidable self-restraint may make other nations relax (of course, ostensible and actual dependence of the United States may not be identical).

Even if nations were to treat the knowledge grid as a complement to rather than substitute for their own C4ISR capabilities, the broader benefits of opening up DoD's information flows should not be underestimated. At a time when the United States appears intent on kicking in its afterburners and widening its already impressive military lead over everyone else, it helps to remind the world that goals of U.S. military policy are consistent with overall international security, rather than an expression of its narrow national interests. Spreading the benefits of its information superiority tools to others is an act of

unprecedented generosity that pays off by persuading other nations not to unite in opposition to what they would otherwise perceive as the reigning hegemon. It never hurts to leave subtle hints indicating that what the United States admits to being able to see and interpret is amazing, but there is far more that it knows and is not showing.

Issues

To recapitulate, a knowledge grid is a global utility that gives others access to (1) data files and objects (complex data structures), (2) channels of real-time data flows, (3) other users (for communications and collaboration), (4) selected controls (e.g., to request that sensors pick up specific information, to filter information and thereby create newsfeeds), (5) services (external systems management, a security monitor), and (6) applications (e.g., models, simulations, displays, advanced processing which may be applied to self-contained or user-supplied data). All in all, one very cool Web site -- the literal embodiment of Microsoft's "Where do you want to go today?" (The knowledge grid need not be on the Internet if it works just as well as a stand-alone network with hard-wired links to other national governments.)

Description is easy; what is hard is structuring the knowledge grid to make it an attractive site for others to take from and give to, without removing it from U.S. control. The purpose of examining some selected issues -- what to show and how, what to get back, how to stay open and yet in control, and how to police the system -- is not to show how critical design issues can be solved but to suggest that they can be.

Who Gets What?

Some data (e.g., signals intercepts) are for no one's eyes. Some data (e.g., weather reports, national management data) can be for anyone. The rest depends on who is listening. Better friends enjoy better access. Clearly, there is no reason not to show data that others can get with their own assets or through commercial means today. But what about data superior to what than others can get today but not necessarily better than what they can get tomorrow? If the goal is to preempt others (be they other nations or other corporations), then some advanced material has to be offered to at least enough users in to bleed away enough potential customers and thereby block a critical mass for alternative investments. An original image that may be accurate to 0.2 meters may be fuzzed to 0.5 meters for friends, 1.0 meters for those sophisticated enough to buy such capability on their own, and 2.0 meters for everyone else. Similar gradations may be applied to sophisticated analytic capabilities.

Putting out a knowledge grid is also giving away implicit knowledge. Foreign users cannot help but understand how U.S. warfighters think by continuously accessing the system -- even if the precise details of what, for instance, U.S. warfighters are looking for (e.g., by focusing their cameras here rather than there) can be masked. But the United States has rarely made much secret of its doctrine mainly because its stock in trade has been the ability to adapt to surprise, often in unforeseen ways.

In the long run, continual access to the knowledge grid may influence its users to think as U.S. users think because they both are looking at the same phenomena with essentially the same silicon eyes. Any U.S.-developed knowledge grid would focus on what the United States fears most (e.g., arms of a rogue state), pass over irrelevancies (e.g., political dissidents), and look away from the United States' abundance (e.g., satellites, stealth, submarines). Buying into the knowledge grid implies buying into these priorities. The easy availability of certain analytical tools, the availability of presentation templates, the differential opportunities for collaboration, and the way knowledge is organized and indexed all influence the way the world is perceived. Others can more easily look for what the United States is looking for and may be frustrated looking for what the United States avoids highlighting.

And For What in Return?

What should DoD expect in return for giving out access? Information made available to all can hardly induce a quid pro quo. However, information given to neutral countries should come with a stipulation that they make themselves at least somewhat transparent and even contribute information from comparable local assets. Friendly countries, because they could enjoy less restricted access, should expect to offer even more, and perhaps even shoulder the burden of converting their own information flows so that they can be used more easily.

Vendors may complain that DoD is giving away what they could have sold (e.g., data, analysis capabilities, applications). In the past, the philosophy was that all information should be privately marketed. With the ubiquity of the World Wide Web, government data do not have to be marketed to be distributed. If outside corporations (i.e., those not paid by DoD for their services) add real value to data, then they can market what they add even if the underlying data are free (if the value-added data cannot be sold as long as the raw data were free, then how much value was added anyhow?). As for work done by private contractors, if it serves national security to give it away freely to others, why not? The defense industry exists to serve national security, not the other way around.

True, some vendors, deprived of export sales, may raise the price of what they sell to DoD. But much of what they supply never gets exported anyway (because it is highly classified). Other vendors may conclude that, even when DoD makes the underlying software available for all, they can make more money on follow-up customization. After all, the information and services that the U.S. military collects may not prove so useful to others -- with differences in culture, doctrine, geography, equipment, and strategies -- without extensive massaging. Customization requirements may work to DoD's benefit. The more money and sweat equity foreign customers put into learning to adapt to DoD's offerings, the greater their psychological commitment to a continued relationship. The more time U.S. vendors (and they are the ones likely to produce the bulk of the applications that call for customization) spend with overseas militaries in the process of customization, the better insights they acquire on how those militaries think -- invaluable intelligence on nations that may not be friendly forever.

How Open Should It Be?

An open system is one whose interfaces and encodings are publicly known; if the latter are publicly determined they can be said to be standard. The Internet is a prime example of an open system: Its specifications are published and vendor-neutral; anyone can plug and play. Openness has many virtues. Users can meld their contributions into the whole more easily. Existing data streams (e.g., commercial remote-sensing satellites) and applications (e.g., network security suites) can be more easily absorbed. Open systems are often more trusted because the developer has a harder time manipulating them. Users can more easily believe that capabilities absent in the original can be inserted by third parties. Standard hardware is far less expensive than proprietary hardware; it is easier to find people who can provide training and maintenance for it.

Yet, national security hardly benefits if others use the knowledge grid, reverse-engineer features of it that they could not generate on their own, and use what they learn to create a parallel structure that not only frees them from U.S. ties but also permits them to attract erstwhile U.S. friends to it. In 1981, when IBM introduced its Personal Computer, it licensed Microsoft to develop the operating system, selected an Intel microprocessor, and, thinking it owned the core piece, wrote its own integrating code (basic input-output system, or the BIOS). Microsoft and Intel went on to lock up their own niches, but the BIOS that IBM was counting on for its lock on the market was easy to duplicate. This situation left IBM very little of the value-added from personal computing. If unwary, DoD may blithely supply the architecture -- the central pieces and the instructions on how these pieces join and link up with other pieces -- and let others supply much of the data, the applications, and the user customization. Then, clever users might figure out how to build the whole thing themselves and DoD's enduring technology advantage -- systems integration -- would have been given away. The trick, therefore, is to permit plug and play but not subsequent disassembly.

Where should lines be drawn? Some aspects of openness, such as standardizing networking interfaces (e.g., TCP/IP), are givens. The credibility of a system that will not connect except with specialized machines is virtually zero. Insofar as user contributions (e.g., the outputs of India's space satellites) are important, open APIs (application protocol interfaces) are essential (standard APIs work even better).

Yet, some key pieces of DoD-supplied applications (e.g., software to generate air tasking orders or to automatically recognize features within images) ought to remain available only from DoD servers (leaving the entire application on the servers may mean that tasks process too slowly and that program-to-program links on client systems are too difficult to engineer). Dropping the entire application and all its supporting services onto the client workstation (e.g., as Java code) leaves it open for capture. Delivering large volumes of data without letting users duplicate them probably requires that the data's encoding algorithms have a critical piece that never leaves a DoD server. Or, applications and the data may both reside on the client workstation, but a key service that lets the two work together stays behind (e.g., an artificially intelligent data cleaner that is too large or too dependent on gigantic constantly changing databases to send forward to clients). Ultimately, however, users have to be happy with the arrangement; otherwise they are unlikely to develop and contribute products and services that they cannot count on using later.

Frustrating Abuse

Any system that opens itself up to the militaries (and intelligence operatives) of other countries is subject to abuse. Some forms of abuse, such as using access to get into and subvert U.S. command-and-control systems, can be controlled through good security engineering (e.g., running the knowledge grid as a separate system with message-only links to its U.S. counterpart). Other forms may try to supply poor or false information. Yet quality is always an issue. Relying on unsigned submissions from people who lack a history of reliability and are not backed up with second-party corroboration is generally a poor idea. Consistently poor or corrupted information can be ignored as long as its source can be reliably tracked. Cheaters may fall short of their quid pro quo promises, but cheating is only one of many reasons that promises are not kept.

Nations awarded access to sensitive aspects of the knowledge grid may also abuse such information to pursue deleterious policies or turn over such information to terrorists, criminals, or other unsavory types. Guidelines on the proper use and management of information ought to be part of any quid pro quo, and violations thereof can be brought up. How would one know exactly when information has been abused? Precedents from the world of print may help. Specific data sets (e.g., imagery), may be digitally watermarked so that each user gets slightly different data. Data sets recovered from the unauthorized possessor can be traced back to whoever first pulled it from the knowledge grid. To echo what the compilers of the Oxford English Dictionary supposedly did, the knowledge grid's architects can sprinkle some erroneous information into the pile. Such information should be irrelevant to authorized users lest they start to make mistakes, but tempting to unauthorized ones (e.g., throw in a treasure map and see who starts digging) who may reveal themselves by how they react.

Concluding Considerations

Information has always been used as an instrument of power, jealously guarded and released only for tidbits of equal value. Those who tout information superiority as a leitmotif and information warfare as its operational forté must therefore hold such tendencies all the more strongly. Thus, for the United States to turn on the tap and hose the rest of the world in data is a new way of looking at this resource. To say it requires a cultural shift for intelligence agencies is considerable understatement. That time may nevertheless have come.

The challenge remains knowing what to reveal, to whom, and for what price. Ultimately, the United States benefits if as many nations as possible rely on a shared information utility that the United States has established to meet its own requirements for international security. Making such a utility work requires a subtlety in (1) engineering the knowledge grid to be open enough to welcome the contribution of others, but not so open that it can be duplicated and the United States taken out of the loop, (2) overlooking the misdeeds of others so that the larger threats to peace may be deterred, and (3) seducing nations into failing to develop or even giving up their independent information capability. In the end, as New Economy reminds us, it is possible to receive by giving away in the hopes that one has created enough mind-share and a sufficiently robust standard to leave one in control. The future of national security information may owe more to the habits of the world's Bill Gates rather than its Bob Gates.

It is a cliché to say this idea needs more study (whether it merits more study is up to readers to determine) -- but not too much more. The window during which the United States can bind others into its knowledge grid is limited. Between the robust development of the World Wide Web and the burgeoning demand for space and UAV sensors, the means to build such a utility without U.S. rules grows. The odds of signing up the currently nonaligned may never be better. Russia, China, India, and Indonesia, among others, are predisposed to get along with the United States at least in certain matters, confidence-building not least among them. Whether they will be equally disposed five or ten years hence is not a given. A world of competing networks each of whose owners vie for friends and power would vitiate a rare, perhaps unprecedented opportunity to exploit the information age for long-term international security.

United States Institute of Peace -- 1200 17th Street NW -- Washington, DC 20036
(202) 457-1700 (phone) -- (202) 429-6063 (fax)
Send Feedback