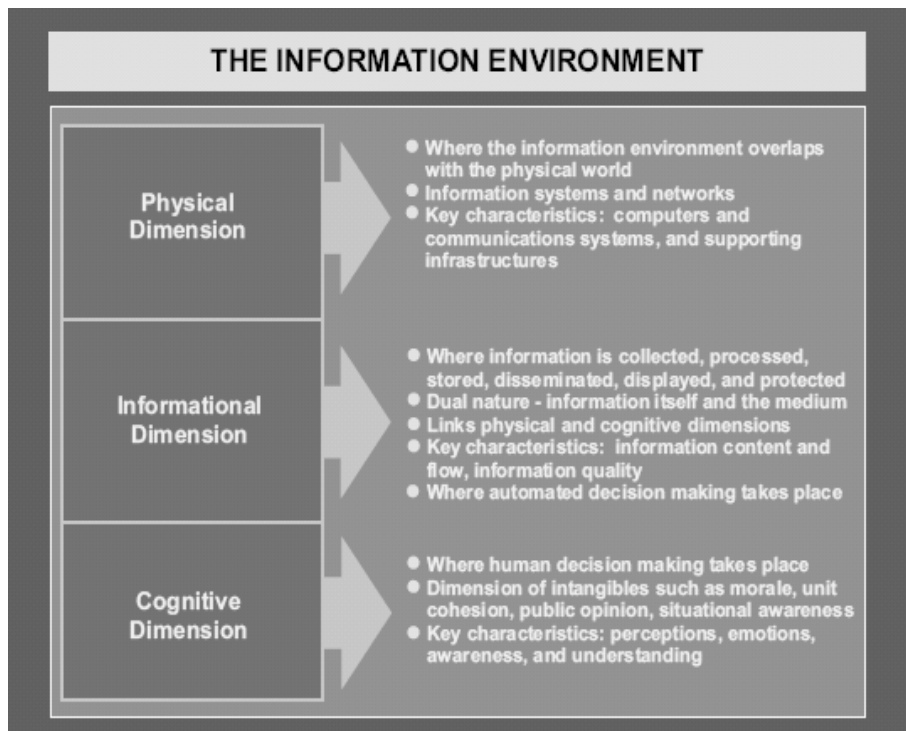


## Info Ops: The Importance of Electronic Warfare

*Scott Curtin*

Addressing the changes in society over the past decade will ultimately bring any discussion to the technology behind those changes. So much of what society does on a day-to-day basis is tied to ones and zeros that provide binary systems the information necessary for them to act. Like Latin, the binary language is rarely understood but critical to the functioning of society. The military is tasked with protecting national security against all enemies and U.S. Strategic Command (USSTRATCOM), in particular, is tasked with our national security concerns within cyberspace. Although cybersecurity, cyberwarfare, and cyberpolicing are terms that are gaining more media attention recently, there has been a concerted effort to address concerns within the digital realm since the original Internet was created. Today a large part of this effort in the military is found in Information Operations (IO).

While the definition above is understood by military members, to most readers it can be difficult to wrap oneself around all of the different ideas included. In simple terms, IO is the protection of friendly information environments and the undermining or destruction of the enemy's information environment. The 2006 release of Joint Publication (JP) 3-13 – Information Operations has helped the military to break down the information environment into three interrelated dimensions that can be acted upon in order to be successful. The information environment is defined in JP 3-13 as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.



**Information operations** — The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 1-02)

While these documents and definitions focus on addressing the concerns facing the military today, they will help address the future concerns of the military as well. While the physical and informational dimensions will change in the future, the changes will be supported by business models that can easily be analyzed and integrated into a

course of action. The only area that will need further study and consideration will be the military's definition of operations in the cognitive dimension, and, more important, the integration of non-military partners, such as local, state, and federal policing, into effecting the cognitive aspects of the information environment.

The importance of the informational environment and its dimensions when discussing information operations cannot be understated. All military actions require a common perspective of the operating environment in order to best decide on multiple courses of action. Unlike conventional actions of the military, the environment of cyberspace cannot be viewed on a map or built into a scale model. Information operations, both offensive and defensive, require an unconventional ability to function in a semi-organized vacuum and discern the nuances of multiple cultural and technical players simultaneously. The future will contain enemies that are on par with or exceeding in their abilities to utilize the cyber domain to further their aims. The primary reasons for this capability edge are reduced technology costs and the lack of management oversight on cyber-based activities. Consider the hypothetical description in the adjacent text box.

To win the future IO battle, both within the United States and abroad, the military must embrace three concepts: 1) intelligence gathering and forensic sciences are the same within the information environment; 2) business and cybermarketing techniques are more useful than traditional information operations in the

virtual community; 3) identifying centers of gravity both in the information environment and in the real world must lead to corresponding and fitting actions in both.

Intelligence gathering and forensic sciences have many similarities in the real world. Within the digital world, those similarities disappear, and the arts of both intelligence and forensics become one and the same. All intelligence must be looked upon from a crime perspective, and all forensic material must be used for developing intelligence. Although many would say that this already occurs or that the two work well with each other, it only takes an organization chart to see that the two functions are almost always shown separately. Fusion of experts in both traditional fields must begin at the organizational level with immediate replication in the training realm. The future demands that we correctly capture the forensic data in order to properly prosecute or attack a threat, but that the same data serve to create personality

Financially, policing faces an uphill battle with regard to technology. The enemy is better resourced and less constrained in the usage of new technology. A cell of 5 terrorists can better communicate, collaborate, and execute crimes in the virtual and real world by simple economics. Five reasonably priced laptops will cost no more than \$5000. Connectivity is provided by wireless fidelity (WiFi) in free hot spots (Starbucks, Panera, and some gas stations). Advanced hacking tools can be downloaded for free off of many Web sites and used to gain the advanced intelligence for a crime. Some cheap and effective methods can be utilized to mask the users from tracking and remove digital fingerprints once they leave. The manuals to build weapons can be downloaded from known terrorist Web sites, and online courses can be utilized to help the terrorists know how and where to buy components needed to assemble a bomb to include those that use Chemical, Biological, Radiological, and Nuclear (CBRN) elements. If they are rather inept, they can actually get online assistance and troubleshooting on other terrorist web sites from experienced bombers. For less than \$10,000, a terrorist team can set up shop in Anywhere, U.S. In contrast, police entities must purchase standardized equipment through a procurement process that raises the typical computer price to a premium, with outdated or disparate integration with existing or legacy systems. Systems are often not customized for the operations required and include many useless add-ons that can reduce the functionality of the system. Cross-jurisdictional issues also apply because of local, state, and interstate funding sources leading to ineffective management and collaboration in geographically related areas. The extremist, non-state actors already have an upperhand when it comes to cyberspace.

models, orders of battle, cultural understandings, and identification of communities that can be encouraged to support or targeted for deception operations.

The WWW (World Wide Web) serves as a source of entertainment for many, news for others, and economics for still others. Many people utilize it for all three and more. For this reason, the WWW is a large medium for business style marketing. Where people visit, spend, and add information on the WWW are all easily tracked and analyzed for targeted marketing. This construct is essential to future information operations because it allows military and cultural experts to identify, exploit, and recruit from the right sources. Imagine a future when the forensic/intelligence fusion allows information operations to target an extremist group with the messages necessary to keep them from escalating to violence or providing the necessary targeting to recruit and train others to do the same without direct links to the United States. While there have been some forays into online recruitment for the military, the lack of targeted marketing reduced the benefits that could have been reaped. The future use of the Internet to help provide national security must be supported by and targeted at a younger community than is currently used by the military. With age comes maturity, but it also reduces the level of marketing savvy necessary to address and target the growing youth bulge in the troubled regions. Most marketing firms look to younger recruits to keep them plugged in to the pulse of fashion, music, and other entertainment concerns. The firms have also begun to use emerging digital mediums to solicit ideas, poll audiences, and hook their buying public. The majority of users in the information environment get their

news online (not from newspapers), express their interests in blogs and “wikis” (not in diaries or notebooks), and search for guidance in life among the many online resources (not in their neighborhood church, synagogue, or mosque). To be successful, the military must continue to look for the next new forum and begin to collaborate more with the marketing culture.

Center of Gravity - The source of power that provides moral or physical strength, freedom of action, or will to act.

JP 1-02

While the concept of “centers of gravity” elicits active debate, within this discussion the definition provided in the adjacent textbox will be used. Focusing only on real-world centers of gravity or only on digital centers of gravity is a misuse of resources and personnel. The future will create greater dependency between the two environments and a failure to address both simultaneously would be akin to pulling off a single leg from a centipede and believing that you have immobilized it. The growth of a digitally savvy enemy has surprised many, and the future will better empower those that are willing to immerse themselves on the fringes of societal norms. The proof of cellular organizations within terrorist groups being a successful model in the real world is mirrored in their practices and organization within the virtual world. This model of success will become the model for future criminal and extremist activities. The marriage between real and virtual models also ties together the groups’ centers of gravity and offers an opportunity to act with greater impact against these groups. However, many efforts focus on using the virtual intelligence/forensics to act within the real world, without taking action

against the other parts of the cell in the digital realm, and vice versa. The future requires that we determine those centers of gravity that effect the real and world organizations simultaneously and create multiple second and third order effects.

A cell of terrorists is controlled and contacted by one higher person through cell phones or digital messaging (emails, chat rooms, etc.). While investigating the terrorist cell, the military determines that the person who receives the information is the same all of the time. By monitoring communications they are able to determine the funding methods and isolate other members of the cell. Continued analysis helps to create a greater organizational and process-based model of the cell. Where the lines cross becomes a possible center of gravity. If funding goes to the primary cell leader and is deposited in a single online banking account, then an arrest of the cell leader and his upper-level contact, the simultaneous draining of the cell leaders bank account, and beginning a trace of activity on the upper level contacts bank account produces immediate and long-term ripples in the organization.

The military model for determining centers of gravity has helped to produce effects that support the national security mission and also reduce our enemy's capacity to effectively operate against us. Once the model is adapted and acted upon in both worlds, the rates of success and length of impact will increase dramatically.

The discussion of this paper has focused on the military model today and forecasts for the future. However, the question most likely to be asked is how it applies to policing. The military definition of the information environment, the dimensions of the environment, and how information operations will need to adapt for the future all have common sense applications to policing. The difference is in culture and not in concept. The military model was developed for the military, and any adaptation of the model

to policing must include an analysis and modification for the culture of policing. The benefits of adopting the military model within the policing community are as numerous as those that the military will gain, but the policing-adapted model will require multiple adjustments to meet local, state, and federal laws and restrictions. Collaboration within the model will face the same cultural and physical barriers that policing faces between jurisdictions today, and those must be met with political and legal efforts to change authorities and laws. Finally, police adoption and adaptation must be integrated into the training models so that the next few generations of officers grow up with the mind-set of information environments and operations. Resistance is futile when we discuss globalization, and the failure of policing to immerse itself into the information environment will lead to a chasm between the community and the police.

*I think we're critically dependent on the Internet today, and the depth of that dependence is constantly increasing. Aside from the obvious media and entertainment use of the Internet, from which we derive pleasure, the Internet is now central for communications, for commerce, for government, and for defense and utility industries. Pretty much all sectors of our society today have embraced the Internet and are now critically dependent on it -- and this will only increase going forward. – Professor*

Tom Leighton (Gardner,  
2006, June 2)<sup>1</sup>

The military and policing have a role in the future of security operations within the information environment. While mission focuses will often be different, they will also likely overlap in many areas. As policing has been active in cyber-related activities since the World Wide Web first became public, much of the efforts to remain relevant in that effort are developed locally and fail to create a united front. The future requires that we adopt a collaborative nature between policing and the military.

---

<sup>1</sup> Gardner, D. (2006, June 2). Full transcript of Dana Gardner's briefings: Direct podcast on Akamai and cyber security. Message posted to <http://briefingsdirect.blogspot.com/2006/06/full-transcript-of-dana-gardners.html>.