

Special Edition 2008

IO SPHERE

The Professional Journal of Joint Information Operations

THE WORLD VIEWS IO



Joint Information Operations Warfare Command



From the Editor's

Col J.R. Roberts, USAF, and Mr. John W. Whisenhunt	2
The Challenge of Information Operations: International IO Seminar	
Mr. Timothy L. Thomas	3

FEATURE ARTICLES

The Information Revolution and Information Security Problems in Russia	
Dr. Vitaliy N. Tsygichko	4
An Overview of Information Operations in the Indian Army	
Brigadier General Sapan Kumar Chatterji, Indian Army	10
A Discussion of Information Warfare From a Taiwanese Perspective	
Major General Tschai Hui-chen, Republic of China Armed Forces	15
China's Comprehensive IW-Strategy Link	
Mr. Timothy L. Thomas	22
The Rise and Decline of Bulgaria's Interest in Information Operations	
Dr. Todor Tagarev	26
Ukraine: Information Operations in Countries of the Former Soviet Union	
Dr. Georgii Pocheptsov	32
Australia: Current Developments in Australian Army Information Operations	
Major James Nicholas, Australian Army	38
Canada: Information Operations	
Commander Derek Moss, Canadian Navy	36
Israel: Information Operations Threats and Countermeasures	
Mr. Tomer Ben-Ari	49



Credit and thanks for our cover design go to our graphics editor,
Ms Denise Maloney.

Printed by the Air Force Intelligence, Surveillance & Reconnaissance
Agency Print Plant.

Maj Gen John C. Koziol, USAF
JIOWC Commander

Staff

COL Mark H. Johnson, USA
JIOWC Deputy Commander

Col John R. Roberts, USAF
Executive Editor

Mr. John W. Whisenhunt (SAIC, Inc.)
Editor

Ms Denise R. Maloney
Layout/Graphics Editor



FEATURE ARTICLES (Continued)

Information Operations in Senegal

Colonel Antoine Wardini, Senegalese Army 53

Argentina: The Challenge of Information Operations

Dr. Javier Ulises Ortiz..... 57

Chile: A Vision of Information Operations

Mr. Igor Carrasco Neira 64

ANNOUNCEMENT

Air Force Symposium 2008: Cyberspace

Air University Cyberspace Information and Operations Study Center 68

Bibliography/references for all articles are on the IO Sphere Home Page at: <https://www.jiowc.osis.gov/Publications/IOSphere/index.cfm> Click on the "updates" link under the Special 2008 issue.

QUARTERLY SUBMISSION DEADLINES: 28 FEBRUARY, 31 MAY, 31 AUGUST, 30 NOVEMBER

IO Sphere welcomes submissions of articles regarding full-spectrum IO, including its core, supporting and related capabilities and the integration of intelligence support.

SUBMISSION GUIDELINES

TEXT - Microsoft Word or Adobe Acrobat format

CHARTS/GRAPHS - TIFF or JPG format (if not 300 DPI please provide scannable hard copy)

PHOTOGRAPHS - TIFF or JPG (if not 300 DPI please provide scannable hard copy)

FORMAT/LENGTH - 1,500 - 4,000 words, double spaced

Please place graphs/photographs/charts on separate pages or as file attachments.

See the *IO Sphere* website from your .mil or .gov domain: <https://www.jiowc.osis.gov> or via Intelink at https://www.intelink.gov/wiki/IO_Sphere

Send Letters to the Editor, Articles & Editorials to:

iosphere@jiowc.osis.gov

Joint Information Operations
Warfare Command
2 Hall Blvd, Suite 217
San Antonio, TX 78243-7074

Phone: (210) 670-2676 x42
FAX: (210) 977-4166 or
(210) 674-5069

Disclaimer Statement

This Department of Defense publication (ISSN 1939-2370) is an authorized publication for the members of the Department of Defense. Contents of the *IO Sphere* are not necessarily the official views of, or endorsed by, the US Government, the Department of Defense, or the Joint Information Operations Warfare Command. The editorial content is edited, reviewed for classification, prepared, and provided by the J7 Office of the Joint Information Operations Warfare Command. All photographs are the property of the JIOWC, unless otherwise indicated. Send articles, *Letters to the Editor*, or byline editorials to Joint Information Operations Warfare Command, Attn: *IO Sphere* Editor, 2 Hall Blvd, Ste 217, San Antonio, Texas 78243-7074 or E-mail: iosphere@jiowc.osis.gov

Articles in this publication may be reproduced, with permission. If reproduced, *IO Sphere* requests a courtesy line or source citation.

In Search of the Greater IO Perspective

Welcome to the first-ever Special Edition of *IO Sphere*. It's our privilege to bring you, the greater information operations community, something extra for 2008. You may ask why a quarterly journal would chose to field an "out of sequence" product? The simplest answer is that we're offering something different enough to warrant a little extra attention. On the facing page you'll read how representatives from twelve countries produced something extraordinary, and that the J7 "futures division" felt you might find worth a closer look.

As representatives of IO practices and philosophies, the Joint Information Operations Warfare Command, guided by our US Strategic Command headquarters, looks at a range of ways to assist DOD and Coalition influence planners. This means we're listening to many voices and world views, across a wide range of cultural and historic perspectives. Understanding the complexities of modern influence operations requires both the broadest range of knowledge, and the most granular detail we can determine. Sourcing such formidable needs can be tough, yet sometimes all we need to do is ask. Joint and Service partners are fortunate to have long-standing relationships with a number of graduate, post-graduate and professional institutions—especially those who host sizable international faculty, advisors and students. Similarly, diplomats and military members on the ground in current campaigns are developing increasingly greater regional expertise. Combined with booming open source database efforts, the IO community can access knowledge, experience and lessons learned from almost anywhere. Notably, this means an even greater number of voices.

The international circulation of this journal continues to grow, especially among NATO countries, as do article and editorial contributions by authors outside the US. This is welcome on many levels: helping build a professional community; helping educate new and developing IO staffs;



and sharing views from outside traditional North American boundaries. Sometimes critical flashes of insight come from those farthest from the normal expert's chair, in the same way history enthusiasts may find the most interesting observations from non-traditional sources. A writer from south Asia may provide a fresh perspective on the battlefields of the US Civil War, while a west African soldier may give a US IO planner cause for reflection. Some in the IO community would say that given DOD's reputation as people of action, a time for reflection is the hardest thing to determine.

Relationships change, sometimes very rapidly, and may enhance or harm IO planners' abilities. Yet in the strategic communications business, with more frequent talk of dialog—even among traditional adversaries—opportunities are growing. Sometimes an invitation is the toughest step. The Foreign Military Studies Office and their international guests took up one such offer, and we hope you'll find the results both valuable and enjoyable.



-- Col J.R. Roberts, USAF
Executive Editor

-- Mr. John W. Whisenhunt
Editor

In 2007 the Foreign Military Studies Office (FMSO), a subordinate unit of the US Army Training and Doctrine Command (TRADOC), hosted an International Information Operations Seminar at Fort Leavenworth, Kansas. Twelve countries from six continents participated: India, Russia, Ukraine, Bulgaria, Senegal, Taiwan, Israel, Argentina, Chile, Canada, Australia, and the US.

The IO perspectives provided are solely those of the authors and not those of the nation he or she represents. All discussions were conducted at the “unclassified” level. Chatham House rules were in effect, meaning that what was said at the seminar cannot be attributed to any individual speaker or their affiliation/organization. This also means the seminar discussions will not be published, only the prepared texts found in this journal.

Each representative was asked to answer three questions: How have information operations changed in their respective countries over the past ten years? How can countries neutralize an extremist’s use of the Internet? And what new ideas in regard to information operations or other cyber-related issues are emerging from their countries perspective? In addition to the twelve countries noted, FMSO attempted to answer the same questions based on Chinese materials.

Some representatives were able to easily answer all three questions while others, due to other priorities in their defense departments or simply due to a lack of cyber capabilities and thus cyber experience, were limited to answering only one or more questions in detail. Each country focused on different aspects of IO according to its particular IO context and perspective. There is no FMSO comment on these. Rather the reader must judge for him or herself whether the recommendations and points of interest offered by each speaker are worthy of further consideration.

A few general conclusions can be drawn from this short summary of the country representatives prepared presentations. First, there are still many different ways to define IO. While some

“The Challenge of Information Operations” International IO Seminar

of the countries’ definitions clearly were modeled after the US definition developed years ago, there were several countries (Ukraine and Australia in particular) that are moving in different directions. Bulgaria is working on an effects-based frame of reference as much as on an IO frame of reference, it appeared, as it strives to work closely with NATO. Second, several countries highlighted (such as India did) the economic aspect of IO. This is a point of concern to several countries. According to one Chinese author, who was not a part of this seminar, “war with the objective of expanding territory has already basically withdrawn from the stage of history, and even war with the objective of fighting for natural resources is now giving way to war with the objective of controlling the flow of financial capital.” It appears that the integration of civilian and military systems and the focus on critical infrastructure protection has caused serious concern in the future economic

perspective of several countries. Third, two items appear to have the interest of all participants: first, that critical infrastructure protection is of paramount concern (Chile, Argentina, Taiwan, etc.) and second, that nations have to do more to control extremist’s use of the Web (as highlighted by Canada and Israel in particular). Fourth, one nation, Russia, called for expanded definitions of the term information weapon and for expanded use of the United Nations to control these “weapons.” Finally, Senegal highlighted the wide gap in complex information system development between nations. That country focuses mainly on the psychological operations aspect of IO and not on computer network operations as others are doing.

FMSO thanks these authors for their outstanding support and for the thought and time put into these presentations.

-- Mr. Timothy L. Thomas
Foreign Military Studies Office



L to R: Mr. Tim Thomas, Dr. Todor Tagarev, COL Antoine Wardini, Dr. Georgii Pocheptsovy, MG Tschai Hui-chen, Dr. Vitaliy Tsygichko, BG Mark O’Neil (CGSC Commandant), CDR Derek Moss, BG Sapan Kumar Chatterji, Dr. Javier Ulises Ortiz, Mr. Igor Carrasco Neira, Mr. Tomer Ben-Ari, MAJ James Nicholas. (US Army FMSO)

The Information Revolution and Information Security Problems in Russia

By Dr. Vitaliy N. Tsygichko

Editorial Abstract: Dr. Vitaliy Tsygichko states the global community must define “what is an information weapon” and must develop an international convention to limit their use. This should be done under United Nations (UN) auspices in order to prevent the proliferation of information weapons and effectively resist the threats of information warfare, information terrorism, and information crime. Dr. Tsygichko lays out Russia’s position on this issue in the form of recommended elements of an international convention.

Introduction

The late 20th and early 21st centuries were marked by the next phase of technological change, notably, the introduction of information and telecommunications technologies (ITT) across nearly all vital activities—and the development of the World Wide Web. Information and telecommunications network technologies and the fast spread of local and global networks provide a new quality of information exchange, shape a new global information space, and impact all facets of public life: politics, economics, culture, international relations, plus national and international security.

Changes in the world information space act as a global development factor, and determine the key directions of social progress. Most important among these are:

- Acceleration of scientific, technological, economic, social, and cultural developments thanks to greater volume and speed of information exchange irrespective of distance.
- Opportunities for dissemination of new ideas and knowledge plus rapid proliferation of scientific and technological achievements.
- Creation of a basis for the elaboration and spread of a new scientific and philosophical paradigm for the 21st century based on understanding the many facets of the world and on the realization of humankind’s common global problems.
- Intensification of global integration trends, in particular in economic, political, information, technological, educational, cultural, and other areas.

- Creation of premises for the development and introduction of new forms and methods of ensuring global, regional, and national security.

- Progress in the areas of political, economic, production, military control, and international relations.



Insignia of the Russian Federation Armed Forces. (Wikimedia)

At the same time, the world community’s “computerization” breeds a whole set of negative geopolitical implications. First comes polarization of the world (resulting in the widening of the gap between rich and poor and between technologically backward and advanced countries) and the realization of a growing number of marginal countries along the roadside developing civilization. These countries are the main source of instability for current and future conflicts including those of a global character. Thus, the information revolution not only accelerates civilization’s progress, but gives rise to new national, regional,

and global security threats—primarily terrorism.

The Information Revolution in Military Affairs

New IT changes are most radical in the military. Recent developments clearly point to the fact that military power still remains the key argument behind global and regional policies. Moreover, the significance of military force keeps increasing. After the Cold War the world entered a period of regional wars and political instability as the number of large-scale military operations of a global, regional, and national character increased sharply. Attempts to curb nuclear proliferation failed. Under these circumstances, the US—the recognized leader of the Western world—and their allies set out to cope with these security challenges and defend their national and group interests by establishing and maintaining a “new world order” based largely on threatening the direct use of military force. This US implements this strategy primarily by building up military power, through reorganization of the armed forces in line with the tasks and supply issues associated with a new generation of arms. All of these make wide use of new information technologies. Desert Storm operations, actions in the former Yugoslavia, and the current war in Iraq, illustrate this strategy in practice.

The wide introduction of new information technologies greatly increases combat capabilities of conventional arms and defense-related technologies. Information technologies foster qualitative changes in reconnaissance and communication,

producing manifold increases in the speed of processing huge arrays of information that decision-makers require. This permits the transition to new methods of troop and weapons control at all levels—from strategic to tactical. New information technologies made it possible to sharply increase the combat capabilities of electronic warfare equipment and to develop a radically new type of armament: information weapons designed for destroying the defense and civilian information infrastructure of likely enemy threats, by breaking into their computer networks.

While resulting in dramatic increases in combat capabilities of troops, the military ITT revolution leads not only to changes in the forms and methods of conducting operations, but also alters the traditional armed struggle paradigm. Emergence of information weapons has drastically changed the pattern of escalation for military conflicts. Even selective utilization of information weapons against defense and civilian information infrastructure projects can put an end to a conflict in its early phase—before the start of active combat operations. Possession of information weapons, just as with nuclear ones, secures an overwhelming military advantage over countries who have none. In the near future, information and political parameters of “soft power” will dominate the older nuclear ones—if they are not already doing so today.

Realistically, we can refer to the consequences of applying wide-scale military information-technologies and information weapons as a new type of weapon of mass destruction—with all the ensuing realities and problems. The vulnerability of all countries to information weapons, in particular the highly developed ones, is particularly notable. Like nuclear weapons, the latter can serve both as a factor of political pressure and containment.

Clearly information warfare is not a virtual reality game, but rather a quite tangible tool for gaining victory in a military or political conflict. There is no doubt that information weapons are a major component of the military potential of a nation. Many countries, primarily

the US and China, are persistently and actively preparing for the conduct of information warfare. The paradox is while a serious military conflict between developed nations is unlikely today, modern weaponry appears hardly effective against the global threat of international terrorism. The latter makes wide use of information technologies—the Internet in particular—for its own ends.

Terrorism and the Civilization Factor

The developed countries’ preparedness to rebuff international terrorism is due largely to the civilization factor, which is gaining in significance along with the evolution of civil society. As a complex, multifaceted, and extremely negative socio-political phenomenon, terrorist activities have long since crossed national boundaries, turning into a huge threat to the security of all humanity.

It is a mistake to assume terrorism is composed of separate acts committed by loners or individual terrorist organizations. Clearly, Islamic extremists draw their followers from among the countries preaching Islam. Numerous fundamentalist organizations, quite active in virtually all countries, are recruiting their adherents from among young people. As a rule, these organizations are under the secret patronage of a number of states, and a significant segment of the population in the Arab world sympathizes with their activities. Islamic fundamentalist movements are generously financed and guided by highly influential and rich radical layers in the Muslim world. The extremist propaganda machine is quite efficient at putting ideas in the heads of Muslims of the necessity of Islam’s confrontation with the rest of the world, and the inevitability of a war between the two civilizations. Apparently, the Western world will have to wage a protracted ideological struggle for the Muslim mind, as well as economic and military fights over liquidation of sources of terrorism, and creation of economic and socio-political conditions where terrorist threats are minimized.

Extremists chose terrorism as their main and rather effective weapon for war with an unprepared world. The 11 September events in the United States exposed a considerable vulnerability of Western civilization, even to isolated terrorist acts. Political and socio-economic transformations over the past two decades have led to a sharp increase in—and frequently to a dominance of—the “civilization factor” in the developed democracies’ perceptions. Chief among these are the purposes, conditions, forms, and consequences of military force utilization.

The civilization factor is defined as an attitude toward the value of human life established in each concrete community (state, religious, or ethnic). This attitude is determined by historical, cultural, and religious traditions; living standards; form of political system; the dominating ideology in each state; the level of development of democracy; and democratic institutions in each society. For example, in Afghanistan under the Taliban regime, human life was of no value—while in Western countries human beings are treated as a basic value of society, and all government institutions are called upon to defend them.

In advanced democratic nations, strengthening of the civilization factor is linked primarily with evolution of civil society as the key socio-political force bearing upon domestic and foreign policy. These include defense, and exercising public control of authorities. The core value in civil society is human life—the rights and security of the individual. Though the process of civil society’s formation is ambiguous and frequently controversial, it would be safe to say that it tends to deepen and spread across an ever-wider range of countries in a persistent and irreversible manner. The military way of handling foreign policy problems is unacceptable for civil society if combat operations may result in considerable losses of both one’s own citizens, and the enemy’s civilian citizens. Of course, this holds only for those situations not threatening the state’s existence. In case of aggression against them, battle casualty attitudes

will be quite different, when they will no doubt make sacrifices for the sake of retaining their sovereignty and independence. But the current geopolitical situation is such that these nations/alliances dominate the world in economic, political, and military respects, and they are facing no direct military threat. Today's terrorist threat is quite real, and the West may accept certain sacrifices while fighting it. As civil society gets entrenched, it becomes more difficult to use military force in situations not threatening the state's existence. So, as far as advanced democratic nations are concerned, it is the civilization factor—the level of admissible casualties in handling foreign policy problems by military means—that is attaining ever-larger significance. In recent decades, experience gained in military conflicts of a different scale in reveals the level of admissible losses amounts today to only scores of human lives. This becomes one of the major factors restraining these nations from use of military force.

This factor manifested itself most fully in the still smoldering Balkans crisis. Military-political implications of the former Yugoslavia conflict made it necessary to radically revise many strategic assessments linked to the use of force in local conflicts. Notably, NATO operations in Yugoslavia deadlocked in mid-May 1999, with the alliance on the brink of a split over two key issues: continuation of bombing; and the possibility of a land operation. NATO air operations failed to produce the desired results, and the Yugoslav army retained most of its combat capability. It was prepared to put up heavy resistance against NATO use of land forces in case of a ground invasion. Aerial bombing—carefully targeted as it may be—inevitably resulted in civilian casualties which sharply undermined the operational support of European public opinion. In fact, Greece was against the military operation, and the Italian and German governments faced problems within their respective parliaments. Even under threat of the alliance's



The Russian Federation. (Univ. of Texas)

disintegration, public humiliation, and in effect, revision of the outcome of the Cold War, NATO was unprepared for a ground operation. Such is the influence of the civilization factor. Though within the boundaries of the European “province,” NATO operations demonstrated the impossibility of realizing military power, even in a small military conflict.

The civilization factor is also behind the deadlock in Iraq, which is experiencing a civil war with no prospects for an end in sight, despite the presence of a big foreign contingent and attempts to regenerate the Iraqi Army. Deaths of Western alliance soldiers and Iraqi civilians keep mounting, reaching a level where public opinions in Coalition countries are more and more persistently urging to pull their units out of Iraq. This in spite of the fact it may lead to yet another victory of Islamic radicals over the civilized world, and to a further escalation of their activities in other regions, including Russia.

In the rest of the world, outside the club of developed nations, the civilization factor does not yet play a significant role. Regional military conflicts of a different scale and character do not generally take the value of human life into consideration. The 1980s Iran-Iraq war, practically all wars in Africa,

the civil war in Afghanistan, the China-Vietnam conflict, the armed struggle of Kurds for independence from Turkey, —and other military conflicts associated with the huge loss of human life—are all examples.

Disregard for human life is specifically characteristic of Islamic extremism, where principles of self-sacrifice in the struggle with “infidels” provide terrorists with huge advantages in their war against Western civilization. The latter is incapable—by its very nature—of sacrificing its citizens, and answer terror with terror. Effective counterterrorism is possible only through joint efforts on a global scale. The entire world community must coordinate its anti-terrorist activities, to include those in the area of information terrorism.

Information Terrorism

As an integral part of technological terrorism, the spread of information or cybernetic terrorism poses a serious global threat. Though this type of criminal activity is not yet a widespread, practical terrorist activity, there is a rather high near term danger. Terrorists make use of the civilized world's openness for attaining their ends. In the past, it was more difficult to arrange and execute terrorist acts because of the associated

distance and the coordination difficulties. Today, the Internet has practically erased both of these problems. New “network terrorists” are increasingly coordinating doctrinal, conceptual, and organizational level activities using the latest technological advances.

Characteristic features of information terrorism are “cheapness,” and difficulty of detection. By linking computer networks across the globe, the Internet has altered the rules concerning sophisticated weapons. Internet anonymity allows a terrorist to become invisible—and practically invulnerable—in the course of his or her criminal action.

New age high-tech terrorism is capable of causing a systemic crisis for the entire globe, at least in the countries boasting a developed information infrastructure. Terrorists will target computers and special computer-based systems (banking, exchange, archive, research, management, and communication facilities) from TV and communication satellites to radio-telephones and pagers. Electronic mass media facilities such as information agencies and services, computerized radio and TV centers, and publishing complexes are especially attractive for terrorists.

Extremists exploit many network features: relative low cost and accessibility; opportunities for secret development; accumulation, and introduction; and extraterritoriality and anonymity. All of these factors enable uncontrolled proliferation of information weapons, especially if they fall into the hands of aggressive or extremist regimes.

Need for an International Information Security Legal Regime

The emergence of information weapons places the information security problem on a par with other global problems such as nuclear, chemical, and bacteriological weapons proliferation; international terrorism; and drug trafficking. All of these problems are

of a global character and none are amenable to solution by one or even several countries.

Thanks to Russian initiatives at the UN, the world community is fully aware of the national and global threats of information war, information terrorism, and information crime. Russia is prepared to adopt practical steps towards their neutralization. Countries sometimes take rather tough measures when countering information security threats, but these are often ineffective due to the anonymous, trans-border nature of the violators. No country is safe fighting information threats on their own. Only installation of an international information security regime, plus the concerted efforts of its participants, can prevent the proliferation of information weapons—and effectively



Russian Federation leadership monitors the strategic picture. (MOD Russia)

resist information warfare, information terrorism, and information criminal threats.

Yet the practical steps towards an information security legal regime run into specific problems, making it nearly impossible to draw on past experiences to create regimes capable of banning or limiting weapons of mass destruction. The intrinsic properties of information weapons and their utilization make this problematic.

Firstly, negotiations on international information security issues are hindered by the vagueness and ambiguity of both the subject and object of negotiations. The negotiation subject—ensuring information security—and negotiation

objects (information weapons, information warfare, information terrorism, information crimes, and the like) are interpreted differently in different countries. Hence, elaboration of a uniform, universally acceptable frame of reference is the first extremely important step.

The main problem lies in defining the term “information weapons” and developing principles for their identification. What means of armed struggle use information weapons? What are the distinctive features of information weapons? What reasonable arguments can serve as a basis for the definition and classification of information weapons? There are still no satisfactory answers. No uniform basic terminology for holding constructive negotiations on international information security is possible without these answers.

There are two main approaches to defining the term “information weapons.” The first treats the capability of some traditional (kinetic) means of destruction to affect military and civilian information infrastructure as the key attribute of information weapons. Following this logic, any type of arms—including conventional means of destruction—can be referred to as information weapons if they are capable of damaging information infrastructure components. This is also the main shortcoming of such an approach. Indeed, it makes no difference in the final count if the municipal services control system was disabled by a program code-based weapon, a powerful electronic pulse, or a direct hit from a conventional bomb.

The second approach suggests all means of destruction and armaments making use of information and telecommunications technologies (ITT) be termed information weapons. But virtually all sophisticated weapons systems employ ITT, and it would be impossible to finely discriminate between information weapons and the entire arms arsenal on the basis of this characteristic.

Some groups attempted to combine the two approaches, such as the suggestion to call means of information infrastructure destruction which use ITT “information weapons.” However, such combined approaches fail to alleviate uncertainties in identifying information weapons.

According to these approaches, only software designed exclusively for disrupting information infrastructure (viruses, etc.) can be unconditionally called information weapons. All other modern means of armed struggle incorporating ITT are multi-purpose, designed not only for destroying information infrastructure but also for other combat missions. These means differ from past generation weapons given their higher selectivity and accuracy. They are in a sense “humane” weapons, and are not classified as weapons of mass destruction.

Countries possessing sophisticated weapons, reconnaissance, communication, navigation, and control based on the wide-scale application of ITT, have a decisive military advantage. Naturally, such countries will never become parties to any agreements limiting this advantage. The current US stance clearly illustrates this thesis; this nation bluntly refuses to negotiate on issues associated with information weapons, and resists such discussions in the UN Disarmament Commission. The US is only prepared to consider information terrorism and information crime-related issues.

However, Russia would like to know if it is possible to develop criteria for identification of information weapons (apart from software) that are acceptable to all negotiating parties. Could information security problem criteria only limit multi-purpose weapon systems used against civilian information infrastructure projects, instead of banning them? This raises the question of whether the very issue of banning or limiting manufacture, proliferation, and use of information weapons is feasible at all.

Such negotiations may largely concern only single-purpose weapons

designed for affecting the information infrastructure components (weapons based on program codes such as different types of viruses and their means of delivery). However, the universality, secrecy, surprise application, possible wide-scale trans-border utilization, efficiency, and high effectiveness not only make such weapons an extremely dangerous means of destruction, but may significantly hamper installation of a relevant international control system. Further, the overwhelming majority of modern ITT—usable for military, terrorist, and criminal ends—are developed in civilian sectors, hence control of their development and proliferation is highly difficult.

At the same time, the threat of information weapons is real for us all, especially developed nations where the complex information infrastructure supports all vital activities. We are witnessing a situation where only concerted international community efforts can lower the threat. Today, identifying and agreeing on a list of key critical information systems (both public and private), whose functions are critically important for ensuring vital activities plus international security, is a necessity. Identification of this class of information systems will make it possible to develop more effective protection measures, including the right to take retaliatory measures. This will also permit elaboration of international emergency threat response mechanisms, as an IW attack will likely affect the national security of various countries.

Real steps toward pooling global information security efforts would seem to be found through international elaboration and endorsement of a convention (treaty) providing the following:

- Renunciation of information warfare and the development and use of information weapons designed for the destruction of the information infrastructure, including arms based on programmed codes
- Harmonization of national laws governing information security counteractions;

- Elaboration of legal, organizational, economic, military, technological, and other international measures, plus mechanisms for resolving conflicts in the information security area, to counter information warfare, information terrorism, and information crime;

- Development of mechanisms for parties-to-convention interaction in collectively countering information security threats. This would involve the permanent exchange of situation reviews, information on potential adversaries, and emergencies associated with information infrastructures, all with a view to designing adequate countermeasures;

- Compiling a list of critically important national information infrastructure projects, whose destruction may lead to large-scale man-made disasters and casualties;

- International laws for protection of critical information infrastructure projects, with attacks on them considered as a crime against humanity;

- Development of convention-related international control and information security monitoring systems;

- Accountability of convention violators.

In order to prevent a single country or group of countries from unfair or advantageous use of the convention provisions, it would be reasonable to adopt declarations to refrain from:

- Actions leading to dominance and control within information space;

- Denying access to the most sophisticated information technologies, (to counter technological dependence in computerization that could lead to the detriment of other states).

Such declarations would dispel doubts in developing countries as to the non-discriminatory nature of the convention.

The first step toward elaboration and adoption of such an international information security convention could be the establishment—within the framework of the UN—of an international team of experts to analyze the following:

- Scientific elaboration of an agreed frame of reference, including fundamental notions such as “information warfare,”

“information terrorism,” “information crime,” “information weapons,” etc.;

- Compilation of a list of threats to information security, their classification, and how an adversary might implement them;

- Development of information weapon classification principles and identification criteria;

- Compilation of a list of critical information infrastructure projects, and a description of possible effects of their disruption;

- Compilation of a list of possible information security countermeasures;

- Key principles for the development and functioning of an international system of ensuring information security;

- Compilation of voluntary obligations assumed by convention signatories, and possible measures to be taken against convention violators.

The first of these international teams of experts could develop a method for ensuring international information security, which would determine subsequent team efforts, and serve as a basis for the main provisions of an information security convention.

The concept of ensuring international information security should cover:

- A common perception of information security problems;

- Uniform terminology and a frame of reference;

- An evaluation of the current information security situation;

- An assessment of current and potential threats to information security

- The international community's goals and objectives with respect to ensuring information security;


- A description of problems associated with shaping an international information security legal control regime;

- Measures for countering information security threats;

- Potential information security interaction mechanisms;

- Recommendations regarding developmental principles and key provisions for an international information security convention.

Conclusion

International elaboration of an information security convention could become an important practical step in dealing with the complex information weapons issues. Creation of an international legal regime could go a long way in governing the development, proliferation, and use of information weapons; preventing information wars; and ensuring an effective counteraction to information terrorism and information crimes. 



Dr. V.N. Tsygichko, Colonel, Russian Army, Ret., is a full member of the Russian Academy of Natural Sciences, and since 1985 the chief researcher at the Institute of Systems Analysis of the Russian Academy of Sciences (ISA RAS). He is currently the Russian Federation's Ministry of Foreign Affairs expert on information security problems. Since 1967 he has served the Central Research Institute of the Ministry of Defense, working on mathematical simulations of military operations. From 1988 - 1991 he headed an autonomous Center for Research into National Security Problems. Dr. Tsygichko's range of scientific interests embraces methodological and systematic problems of modeling socio-economic processes; decision theory; applied systems analysis; the theory and methods of socio-economic forecasting; ensuring national security and strategic stability; information security problems; and geopolitical problems. He has authored over 200 papers and 6 books. Dr. Tsygichko is a founder of a new national school of mathematical simulation and forecasting of complex social processes in military and socio-economic areas. He has developed principles and methods of systems theory application, introduced an information theory of statistically unreliable decisions, and developed a scenario approach to researching and forecasting socio-economic processes. Some of his papers include: "On Decision Making for Managers" (1992), "Information Challenges to National and International Security" (2001); and "Models as Part of the Strategic Military Decision Making System in the USSR" (2005). He is a permanent author of journals such as *Military Thought*, *Military Bulletin*, *Independent Military Review*, and a number of foreign publications. He is a graduate of the Ryazan Artillery Military School, the Dzerzhinsky Military Academy, and holds a Doctor of Science (Engineering).

An Overview of Information Operations in the Indian Army

By Sapan Kumar Chatterji, Brigadier General, Indian Army

Editorial Abstract: Brigadier General Chatterji believes India's IO methods differ only slightly from those used by many Western nations. Such distinctions include methods such as economic information warfare, in which one nation could strangle another's access to external data, thereby removing the benefits associated with exchange of information and thereby crippling the economy. He believes India has other independent initiatives that have expanded the overall meaning and use of IO, including the topic of sub conventional operations.

Information operations (IO), as a concept, are as old as man's quest for warfare and his dependence on information. However, its role has increased tremendously due to the exceptional growth in technology over the past few decades. Indian mythology circa 5000 BC is replete with examples of the innovative and effective use of information warfare as a war winning effort. The announcement of the death of Ashwathama amidst the beating of drums (jamming), and various other tactics of Lord Krishna to gain information superiority, are just a few of the numerous epic examples.

Today, the importance of IO during recent conflicts and the ongoing counter-terrorism operations in Jammu & Kashmir [Indian provinces] have undisputedly created a new dimension of battle. IO has become the fifth dimension of warfare. This article covers the concept of information warfare in the Indian Army, as well as certain counterinsurgency initiatives India has taken in the past few years. The discussion covers: the objective and principles of information warfare; the terminology of information warfare; the forms of IW; the necessity to deny use of the Internet to terrorists; and the role of information warfare in sub-conventional operations.

Objectives/Principles of IW

IW is utilized to achieve all or any of the following objectives:

- Develop and maintain a comprehensive information base of an adversary's capabilities, and forecast their likely actions.
- Deny information about one's own and other friendly forces, and deny

information about operations conducted against enemies and adversaries.

- Influence perceptions, plans, actions, and the will of adversaries to oppose our own/friendly forces by the use of offensive IW.
- Influence noncombatant and neutral organizations to support friendly missions, or at least not resist friendly activities.
- Protect friendly decision making processes, information, and information systems.
- Degrade adversaries' information systems.

IW is the result of competition brought about by the convergence of a number of evolving technologies, including imaging, remote sensing, precision guided munitions, stealth, directed energy weapons, and above all digital communications & computer networks. During conflict, these technologies are in direct confrontation.

Terminology

Terms used here include:

- Information Operation (IO) - Actions taken to affect adversary information and information systems, while defending one's own information and information systems;
- Information warfare (IW) - Action taken during all forms of conflict, to achieve information superiority over the adversary by adversely affecting his information and information systems while protecting one's own information and information systems;
- Information Assurance - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-

repudiation. This includes providing protection, detection, and reaction capabilities;

- Information Superiority - A state achieved when a competitive advantage is derived from the ability to exploit a superior information position.

Forms of IW

IW is not a distinct type of warfare but exists in different forms. IW can be applied at every level of war, across all phases of an operation, and encompasses the entire range of military operations. The Indian Army defines seven forms of IW:

- Command & Control Warfare (C2W)
- Electronic Warfare (EW)
- Cyber Warfare (Cyber W)
- Network Centric Warfare (NCW)
- Intelligence Based Warfare (IBW)
- Psychological Warfare (PSYWAR)
- Economic Information Warfare (EIW)

C2W

C2W implements information warfare on the battlefield, and integrates it with physical destruction. Its objective is to decapitate the enemy's command structure from the body of forces. C2W aims to influence, deny information, degrade, or destroy enemy C2 capabilities, while protecting one's own C2 systems against such actions. C2W is the war fighting application of IW in military operations.

The foundation of C2W lies in efficient command, control, communications, and computer (C4) systems, coupled with seamless information and intelligence support. C2W consists of the following:

- **OPSEC** - A process of identifying critical information and one's own actions that can be observed by enemy intelligence systems, determining indicators an enemy could interpret to derive critical information on one's own forces; and selecting and executing measures that eliminate the vulnerabilities of one's actions to enemy exploitation;

- **Military Deception** - Actions executed to mislead enemy commanders as to one's capabilities, intentions, and operations;

- **Psychological Operations** - The purpose of PSYOP is to induce enemy attitudes and behavior favorably to one's objectives;

- **EW** - Military action involving the use of the electromagnetic and directed energy spectrums in order to control the electromagnetic spectrum;

- **Physical Destruction** - The application of combat power to destroy or neutralize hostile C2 targets.

EW

EW is a set of military actions taken to deny the use of the electromagnetic spectrum to hostile forces while retaining the ability to use it. The endeavor is to deny, degrade, delay, or disrupt information in order to create a false picture so that incorrect action results. Major components of EW :

- **Electronic Support Measures (ESM)**
- **Electronic Counter Measures (ECM)**
- **Electronic Counter-Counter Measures (ECCM)**

Cyber Warfare

Cyber warfare entails techniques to destroy, degrade, exploit, or compromise the enemy's computer based systems—including attacks on computer networks. In contrast to physical combat, these attacks exploit known lapses in a systems security structure. Cyber warfare includes the following actions:

- Techniques to destroy, degrade, exploit, or compromise the enemy's computer based systems;

- Attacks on computer networks;
- Hacking/breaking into computer networks to include defacing websites;
- Intercepting and monitoring classified information on networks, corrupting and manipulating stored data, and injecting viruses likely to cause irreparable losses;
- Cyber security, including encryption.

Network Centric Warfare (NCW)

NCW focuses on the combat power that can be generated from the effective linking or networking of war fighting machinery/organizations. The basic elements necessary to generate the required shared battle space awareness to achieve the Commander's intent are:



*Indian soldiers raise their national colors.
(MOD India)*

- A virtual sensor or "surveillance" grid that would provide a "grid of capabilities" overlaying the battle space instead of a series of independent single sensors;
- A communications grid that would leverage the strength of the worldwide telecommunications infrastructure. This would enable communications to be considered as virtual grids overlaying the tactical, operational, and strategic areas;
- An abstract grid of weapons or "tactical grid" available to commanders, sorted by suitability and availability against a hostile order of battle.

Intelligence Based Warfare (IBW)

IBW occurs when intelligence is fed directly into operations, instead of being used as input for overall command and control. As sensors grow more accurate and reliable, proliferate in type and number, and as they become capable of feeding fire control systems in real-time and near-real-time, the task of developing, maintaining, and exploiting systems that sense the battlefield, assess its composition, and send results to shooters assumes greater importance for tomorrow's militaries.

IBW is about conducting warfare in a transparent battlefield environment. However, while increasing the transparency for one's own functioning, an important consideration should be to decrease it for the enemy. The need is to create an asymmetry in the level of transparency or situational awareness, in relation to the enemy.

Psychological Warfare

Psychological Warfare encompasses the use of information to influence the human mind. It is also defined as actions carried out during peace, crisis, or wartime situations, so as to influence the attitudes and behavior of enemy, friendly, or neutral audiences, towards fulfillment of political and military objectives.

Psychological operations can be used over the entire support spectrum of military operations, wherein all agencies work in synergy to achieve the desired end state. The aims of psychological operations from a military point of view are:

- Create of doubt, dissidence, and dissatisfaction within the ranks and thereby lowering the morale and reducing the efficiency of adversary forces;
- Reinforce the feeling of friendly target audiences and influence opinion makers;
- Gain support and cooperation of uncommitted or undecided audiences;
- Help achieve conflict prevention, resolution, and achieve a desired end state.

Psychological operations are divided into four distinct but overlapping categories:

- **Strategic Psychological Operations** - This is PSYOP at the national level, conducted predominately outside the military arena. It utilizes all national assets and is directed at all types of audiences. Objectives are long term. The primary aim is to reduce the war making capability of the adversary;

- **Operational Psychological Operations** - This type is conducted during both war and peace time in the operational area to promote the operational commanders aims and objectives. These operations are launched in consonance with military operations, throughout the military operational area. All assets in the operational area are utilized;

- **Tactical Psychological Operations** - These are conducted in the tactical arena, in consonance with tactical missions and objectives;

- **Counter Psychological Operations** - The aim of this type of PSYOP is to safeguard one's own forces and friendly population from an adversary's psychological operations. One must simultaneously carry out counter psychological operations, identifying an adversary's broad pattern of operations, to include the technical means and medium of dissemination. Countermeasures are then instituted, including informing the audience about the adversary's malicious agenda.

The most popular non-military and military mediums used for the dissemination of psychological operations are print, television, radio, and cyber. Print is one of the most effective and widely used media, which has been used extensively in all psychological campaigns to target educated target audiences. Newspaper, magazines, leaflets, posters, pamphlets, and books are associated with this medium.

Television, with its ever-increasing popularity, is one of the most powerful, flexible, and immediate means of influence. It has become a very important psychological tool, as effectively demonstrated during the Gulf Wars and

the 1999 Kargil operations. Television was an extensive part of the psychological campaign, and instrumental in achieving the final military objective.

Radio has been used as an important psychological operations tool since World War I, due to its reach and capability to affect target audiences. It can penetrate inaccessible areas to target insurgents, enemy soldiers, and at the same time help in the psychological conditioning of one's own forces.

Finally, there is the cyber dimension. The Internet has become a very important media tool. The numbers of Internet users are increasing rapidly, and in time will be one of the most powerful means of dissemination for one's own psychological operations. At the same time, this medium is also available to

of information, and thereby crippling the economy. Nations would also struggle with one another to dominate strategic economic industries.

Denying the Internet to Terrorists

With terrorists using cyberspace to communicate and coordinate their activities, denying them this medium is certainly an important issue. However, there are a large number of factors that impede nations from undertaking serious and immediate steps, since these could easily violate individual privacy—and affect the performance of knowledge-based industries.

Monitoring of Data

It is impossible to monitor every byte transaction on the Internet because the volumes are simply too huge. Unless explicitly warranted, democracies should not resort to monitoring. However, most nations need to consider or implement selective monitoring. This is achievable through liaising with Internet service providers on explicit state orders. Such monitoring can be done at gateways and routers, or the "last mile" stubs (i.e. switches / routers) where specific intelligence is available.

Who to monitor, where to filter, or which switch/router to monitor can only be determined through hard intelligence. Therefore, it is extremely important to establish coordination between various intelligence agencies for this specific purpose. Methods include using certain keywords for the purpose of filtering/identifying intelligence data.

Cyberspace monitoring can reap rich dividends if a state obtains hard intelligence. Further, the threat arising from cyberspace needs analysis and planning. For this purpose, Risk Mitigation Plan / Disaster Recovery Plan (DRP) development are the best recommendations. At the national level such a contingency plan helps ensure that should critical resources be damaged, emergency measures and services are in place. India needs to put the DRP in action, and exercise it periodically.



*Indian Armed Forces Emblem
(Wikipedia.org)*

adversaries and terrorists, hence there is a need to monitor and counter malicious propaganda.

Economic Information Warfare

This form of warfare is only conducted at the national level, as a combination of IW and economic warfare. It can also be understood as a variant of an economic blockade, wherein the well being of societies will be affected by information flows of economic data, instead of the flow of material supplies as they are today. In this form of warfare nations would strangle another nation's access to external data, removing the benefits associated with the exchange

Cyber Laws Dealing with Mail / Blog / Portal Service Providers

Communications between terrorists would usually take place through standard mail portals, chat rooms, etc. States need laws need to enact and duly amalgamate international laws, to provide understanding and cooperation, so that should a nation request transaction details or trace back details for any user, ISPs will provide answers. Such actions must be transparent through international boundaries, based on the need to fight this menace jointly at the international level. In addition, since terrorists use the Internet for recruitment through misinformation, some of the steps we could take in this direction are:

- Exchange information pertaining to websites, blogs, chat rooms, etc. between nations that might contain offensive material;
- Block such websites in our national interest;
- Host websites (as a part of Psychological Operations) containing actual, factual information that might be used to influence, and sway away potential targets, or from embracing terror activities;
- Track down offensive websites and close them if hosted in our countries.

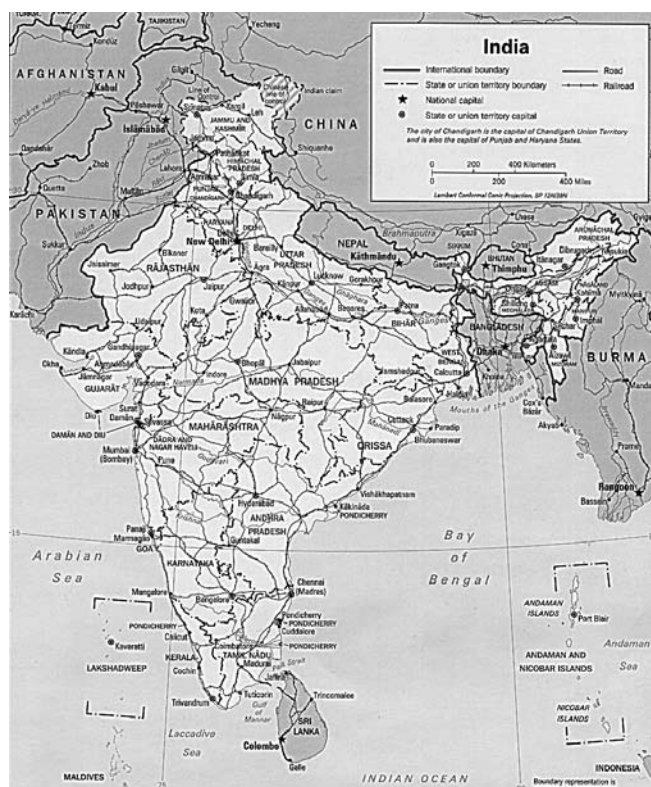
An international treaty of this kind, enacted and enforced, can help ensure we deny terrorists space for hosting such sites.

Cyber Policing

To detect and annihilate the terrorists' Internet attack planning and coordinating medium, we need to develop Cyber Policing Organizations. Hard intelligence must be gathered from cyberspace to provide enough clues to allow for the tracking of criminals and terrorists. The capabilities to handle multiple protocols, encrypted algorithms, code breaking, and so on should be incorporated into our monitoring agencies.

Building a Cyber Forensic Capability

India needs to establish a Network Cyber Forensic capability to enable trace



India in its south Asian context. (Wikimedia)

back of messages, attacks, and other malicious activities. The international community needs to develop IT laws that support state sponsored cyber forensics, not only for the purpose of tracking down terrorists, but for use as legal exhibits in a court of law. PC-based forensics designed for data recovery can help to wean out intelligence captured from terrorists. Similarly, India needs to compile a cryptology analysis capability, so we can crack encrypted traffic and break passwords. This requires long term government-sponsored initiatives, say at academic institutes or at research institutions. However, this too is a expensive and longer range activity.

Sub Conventional Operations

Sub conventional warfare is a generic term encompassing all armed conflicts above the level of peaceful coexistence amongst states, and below the threshold of war. This includes militancy, insurgency, proxy war, and terrorism when employed as a means in an insurrectionist movement, or undertaken independently. Border skirmishes

also fall within this category. Sub conventional warfare entails protracted struggle. It could also be characterized by asymmetry of force levels between regular forces and irregulars, wherein the force applied and the violence generated depends on the modus operandi of the weaker side—and the laws of the land which bind the actions of the Armed Forces. For this discussion we'll consider counterterrorist operations, and public information and perception building operations.

Counter Terrorist Operations

Information operations in the context of the sub conventional spectrum address the following:

- Countering adverse effects of counterterrorist (CT) operations;
- Supporting the goals and operations of one's own forces;
- Defeating malicious propaganda;
- Eroding the terrorists' support base;
- Helping justify one's own operations and projecting the "human face" of the Armed forces

• Winning the hearts and minds (WHAM) of the local population, thereby lessening popular support for terrorist causes;

• Publicizing incentives to the local people in return for information on terrorist activities;

• Persuading terrorists about the futility of their goals against one's own military might.

Military Civic Action

Military Civic Actions (MCA) include programs such as WHAM activities aimed at people in insurgency affected areas, as part of the strategy for conflict prevention. WHAM operations form a major concomitant aspect of counterinsurgency operations. They are integral to the Army's psychological strategy as well. Civic actions include a wide range of activities, across the entire spectrum of development, and demonstrate the Army's "human face." The focus of WHAM operations are quality education, empowerment of women, community development, health care, and infrastructure improvement.

There are several elements associated with the MCA concept. The "iron fist with a velvet glove" concept involves relentless operations, undertaken with a firm resolve against foreign terrorists, and at the same time encouraging terrorists to surrender. These are intelligence driven surgical operations. In addition, forces adopt a people friendly approach, aiming to 'win hearts and minds' and to project the Army's image as "people with a human face." WHAM projects are usually small scale, but generally appreciated, afforded maximum visibility, and very popular.

A second element associated with MCA operations involves centralized planning and decentralized execution. Countries identify civic action projects in consultation with local community leaders, administration, and execution agencies. The plans evolve following a top down (priorities, broad allocation of resources) and bottom up (identification of projects and resource bids) approach. The focus of the projects at the village level is on women and youth. The maximum use of indigenous labor—both

skilled and unskilled—goes a long way toward dissuading youths from joining the ranks of terrorists.

Other elements involve providing assistance in the planning and extension of technical assistance, and providing material resources and supervision. When the projects are completed, they are handed over to the civil administration/village councils for operations, maintenance, and upkeep.

The focus of WHAM activities in an insurgency prone area includes:

- Causality Evacuation and Rehabilitation during Natural Calamities

- Vocational Training
- Health Care
- Community Development
- Infrastructure Development
- Education Facilities

Public Information and Perception Building Operations

Public Information Operations to influence perceptions of various players in the conflict zone should be undertaken in accordance with developed themes. At the operational level, these themes could be:

- The futility of the armed struggle and secessionist designs;
- The efforts of the government regarding relief and rehabilitation

schemes to restore normalcy;

- The erosion of the credibility of terrorists and secessionist elements;


- The importance and efficacy of one's own operations;

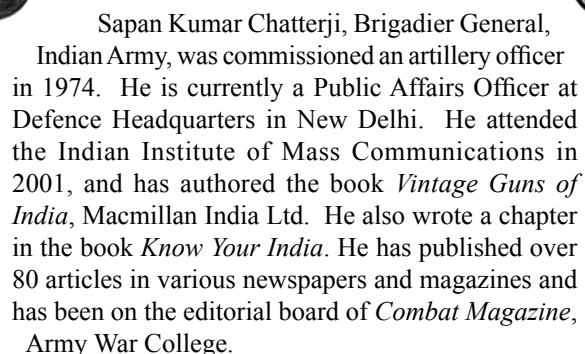
- A people friendly Army approach and its efforts to alleviate suffering that was caused by the terrorists;

- The importance of peace for the overall prosperity of the people and details of the government's peace initiatives.

Conclusion

This article has attempted to briefly provide insight as to how India understands information operations, as well as certain of our own initiatives for directing the future of IO. Overall, India's doctrine and methods differ only slightly from those used by many Western nations. With regard to certain independent initiatives that have expanded the overall meaning and use of IO, our nation adds the topic of sub conventional operations as but one example.

Today, information is one of the most powerful tools available to nations during a conflict. The nation that attains information superiority stands to gain immensely. Nations who work together toward common information goals stand to gain the most. 



Sapan Kumar Chatterji, Brigadier General, Indian Army, was commissioned an artillery officer in 1974. He is currently a Public Affairs Officer at Defence Headquarters in New Delhi. He attended the Indian Institute of Mass Communications in 2001, and has authored the book *Vintage Guns of India*, Macmillan India Ltd. He also wrote a chapter in the book *Know Your India*. He has published over 80 articles in various newspapers and magazines and has been on the editorial board of *Combat Magazine*, Army War College.

A Discussion Of Information Warfare From A Taiwanese Perspective

By Tschai Hui-chen, Major General, Republic of China Armed Forces

Editorial Abstract: Major General Tschai Hui-chen outlines the characteristics of Taiwan's IW concepts, discussing control of an enemy, mobilization mechanisms, and "using energy to release changes in patterns." She addresses important aspects of China's IW capability, such as the concept of "network psychological warfare," in which Chinese "Internet opinion personnel" impersonate regular users in Internet discussion forums.

Introduction

With the advent of the information-based society there are also new forms of criminal activity, featured by endless security incidents such as hacker attacks on networks. This has an enormous impact on governments, economies, militaries, and psychologies in countries all over the world. The use of information technology in military operations and weapon systems has fundamentally changed traditional ways of thinking about military operations. The concepts and related theories of information warfare have become the mainstream in modern thinking about war. Even more so, terrorists make use of platforms afforded them by networks as tools to attain their objectives. For example, B.W. Dearstyne holds that management of information and intelligence in American society provided the 9/11 attackers with their opportunity, due to how easily they acquired information.

This article looks at the development of information warfare (IW) and information security in Taiwan from a Taiwanese perspective, and considers the potential risks and challenges presented by the Internet. It explains how Taiwan can make use of its strengths in the area of information technology, to make an effective contribution and put forth its efforts in today's fight against information terror and extremism.

The Development of Information Warfare in Taiwan

Taiwan's Ministry of Defense established the Strategic Commission for Information Operations in 1999, opening the door to the development of information warfare. Developments

in theoretical research and principles subsequently led to the establishment of dedicated units in these areas.

The results of a Research, Development, and Evaluation Commission survey under the Executive Yuan showed that Internet access in Taiwan increased from 70.6% in 2005 to 74.5% in 2006. This indicates information networks in Taiwan are quite widespread. Symantec's Internet Security Threat Report noted the United States experienced the most activity involving malicious programs in the first half of 2007, while Taiwan was ranked eighth. This shows network attacks have increased as networks themselves have become more universal. Attacks on military facilities will incur the greatest impact, which is why development of information security and information warfare is a required strategy to prevent and control malicious attacks.

Definition of Information Warfare

The development of information warfare in Taiwan can be defined both broadly and narrowly. The broad definition involves conflict and war between two antagonists, to gain a strategic advantage (or the advantage in war) using the means of information technology in the areas of politics, economics, society, science, technology, and military affairs. The narrower definition includes the following:

(1) Use of information technology to conduct explorations and surveys on the opposition, as well as countermeasures involved in said actions, such as reconnaissance, interference, and disruption;

(2) Combat actions undertaken against the reconnaissance, command,

control, communications, information analysis, camouflage, deception, attacks, and destruction activities of the enemy;

(3) Preventative measures undertaken against the interference, disruption, and countermeasures perpetrated by the enemy.

These illustrate that the scope of information warfare includes any measure taken against an enemy, such as information intervention, interference, disruption, breakdown, countermeasures, and counter-countermeasures.

Characteristics of Information Warfare

By contrast with traditional warfare, one could say that information warfare results in victory without firing a shot, or gaining a decisive victory from many miles away. The various IW characteristics illustrate this:

(1) Attackers on an information battlefield do not require enormous financial means, and do not need to purchase expensive equipment. Instead, they need only be able to use and operate the tools of attack (such as Trojan Horses) to be victorious in information warfare—or even inflict severe injury on the opponent;

(2) Traditional distinctions between war and peace, military and non-military, nation and place, and even attacking and defending have become obscured;

(3) The distinction between peacetime and wartime is fading away. Any security leak in an information system can attract an information warfare attack;

(4) Information warfare presents great difficulties for command and control. Battle rhythms move fast, which is why decision-making models

and systems are adjusting to meet these challenges. From the decision-making perspective, the objective in information warfare is to influence (and even break down) the enemy's decision-making mechanism.

Offensive Information Warfare

From an organization and implementation perspective, recent regional conflict actions describe the main features of information warfare at the strategic, campaign, and tactical level. Type actions include:

- (1) Long-term and frequent full-scale wars;
- (2) Tangible and intangible battle lines in total wars;
- (3) Special wars which determine victory or defeat in open conflicts.

Weapons of attack primarily include various types of software viruses, and logic bombs to disrupt computer and communication systems.

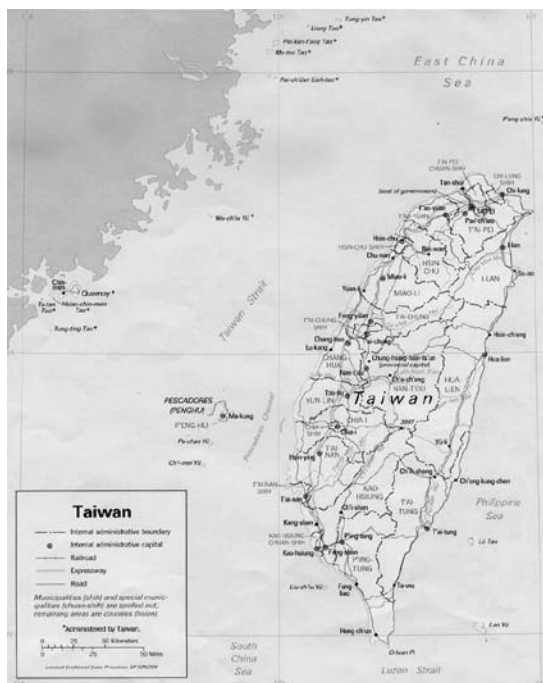
Defensive Information Warfare

Defensive information warfare primarily means information security. Security of information and information systems can be measured through the following properties:

- (1) Information confidentiality: Ensuring that information is not leaked to unauthorized persons;
- (2) Information integrity: Preventing unauthorized tampering, and ensuring that true information is transmitted to its destination without being distorted;
- (3) Information authenticity: Information sources can be correctly identified;
- (4) Information availability: Ensuring information and information systems are accessed by authorized users and authorized management, which prevents denial of service caused by computer viruses or human actions;
- (5) Non-repudiation: Ensuring people performing information activities cannot deny their own activities.

Military Deception

Military deception involves the utilization of electronic interference,



*Taiwan, Republic of China
(Wikimedia)*

camouflage, deception, and network piracy, then integrating them with military force and firepower to create an enormous information attack momentum or threat. Or, it may involve rendering the enemy unwilling to act rashly by “feinting to the east but attacking from the west,” giving the appearance of formidability, making secret war plans, tricking the enemy into action, or threatening the enemy psychologically. Potential deception measures include:

- (1) A balanced information flow;
- (2) Spreading false information in order to deceive the enemy's intelligence, reconnaissance and information gathering;
- (3) Making use of terrain and geographical features to secretly allocate and camouflage installations and facilities;
- (4) Creating false targets, signals, platforms, and positions, as needed or according to plan.

Taiwan's Developmental Policies for Information Warfare

On the basis of the “Total Civilian Defense” policy of 2002, the military buildup transformed from a passive to a proactive policy, and the strategic vision known as “a resolute deterrence

and an effective defense” changed to an aggressive defense vision of “an effective deterrence and a resolute defense.” The overall military communications and electronic information plan in the Republic of China involves the objectives of attaining information superiority, solidifying national defense, controlling the enemy, and seizing the initiative based on the strategic guidance of and demand for joint operations for “an effective deterrence and a resolute defense.” At the same time, the government promotes the following policies based on the concept of the integration of peacetime and wartime activities:

- (1) Building up an information infrastructure for national defense: The primary task is coordinating various promotional programs for building a national information infrastructure, and exerting every effort toward advancing the information infrastructure buildup for national defense. This involves constructing networks connected to the military information transmission trunk, as a means of providing the transmission and exchange of systems information for war intelligence, command, management, human resources, logistics, and finances; and utilizing various networks and local linkups to exchange information.

- (2) Establishing operational capabilities based on information superiority: The objective for information warfare in Taiwan is to protect communications for national defense, information systems, and network security. Guided by priority protection and quickly seizing the initiative, Taiwan will adopt all measures of proactive surveillance and reconnaissance and aggressive protection. We will set up protective communications and information capabilities, which will include early warnings, and adjustments according to changing circumstances.

- (3) Effectively integrating communications and information networks: In order to meet the demands of future operational tasks, Taiwan will continue to advance the formation of new generation military communications,

information installations, and equipment, along with the overall planning for and integration of communications resources. We will strengthen integration of the operational environment and platforms for communications and information systems. We will construct a joint operations communications system featuring operational compatibility, with the goal of integrating the different military services and joint warfare networks.

(4) Integrating command, control, communications, information, intelligence, surveillance, and reconnaissance systems: As a means of exploiting Taiwan's new generation of fighting power, the nation is concentrating its efforts on construction of an integrated command, control, communications, information, intelligence, surveillance, and reconnaissance system (C4ISR) to link up the joint operations command and control system with weapons platforms. This will enable prompt synchronized exchange of intelligence and information, improve transparency on the battlefield, eliminate the fog of battle, and initiate the buildup of an instantaneous command and control system which can see, hear, and command. This will be a key goal in establishing information superiority in Taiwan and exploiting the nation's information operations capabilities.

(5) Strengthening electronic warfare operations capabilities: In response to future forms of war and the demand for joint operations, Taiwan is putting all of its efforts into reorganization of defensive equipment for electronic warfare. This includes EW combat capabilities, and frequency spectrum management capabilities for both attacking and defending. We must ensure communications discipline and information security protection as a means of enhancing IO combat power.

Guided by these policies, Taiwan will formulate a three-phase developmental plan for information warfare:

(1) First phase: Establish information research organizations and formulate information warfare educational programs. Plan for the buildup of infrastructure for national defense information. Draw up an outline for information warfare.

(2) Second phase: Build up the infrastructure for national defense information and set up an information strategy research center. Integrate resources at the Chung-shan Institute of Science and Technology to research and develop IW technology. Establish an information warfare research unit at National Defense University and set up an information warfare team and command mechanism.

(3) Third phase: Integrate national resources and finish planning for a mobilization mechanism for information warfare. Concentrate information combat power in the military, and support Taiwan-Penghu defensive operations.

The Evolution of an Information Security Strategy in Taiwan

The Executive Yuan [Republic of China executive branch of government] passed the "National Communication and Information Infrastructure Security Mechanism Plan" in January 2001, and established the National Information and Communication Security Task Force (organizational structure given in Figure 1) as a means of aggressively promoting its national information and communications security policies. The group integrates, coordinates, and effectively utilizes the resources of relevant government agencies, in order to accelerate construction of a national security environment and enhance national competitiveness. In addition, these act establish of an information security protection system, provide for inspection of information security contingency capabilities, and the establish a sound developmental environment for information security. The following summary of current information and communications security actions shows how Taiwan is meeting swift-growing trends in science and technology, as well as dealing with developments on both sides of the Taiwan Strait:

1. Promotion of Awareness of Information and Communications Security, Personnel Training, and International Collaboration. Considering international developments and the current domestic environment, promoting information and

communications security awareness (and training personnel) joins international collaboration as a necessary future trend. Strengthening participation in international information security activities will help establish regional and global joint defense mechanisms for information security. Working together to attack network crime and aggressively promoting global information security are especially important.

2. Aggressive Promotion of Information and Communications Security Operations for Key National Infrastructure Institutions. Electronic information and technologies afford us the ability to closely link critical internal infrastructure and administration in the Taiwanese government, including security, financial services, energy facilities, the water supply, telecommunications, postal services, transportation, shipping, medical care, and other important national economic and security activities. This exposes more potential weak points, presenting opportunities to those with malicious intent, or those not be averse to attacking Taiwan with armed force. As such, Taiwan must build on the foundation of existing national information and communications security efforts by strengthening critical national infrastructure and institutions. This will include the establishment of information security notifications and contingency mechanisms, information sharing mechanisms, establishing information security technology and inspection service teams, providing technology and inspection services, managing the critical infrastructure buildup of information security systems, promoting widespread security education and training, and promoting information security management system verification. This will be effective in providing the best security safeguards during the build-up of infrastructure

3. Widespread Application of Wireless Networking and the Flourishing Development of ISP Providers. Wireless communications have developed rapidly ever since the discovery of electromagnetic waves at the end of the nineteenth century. Wireless communications are an inescapable part

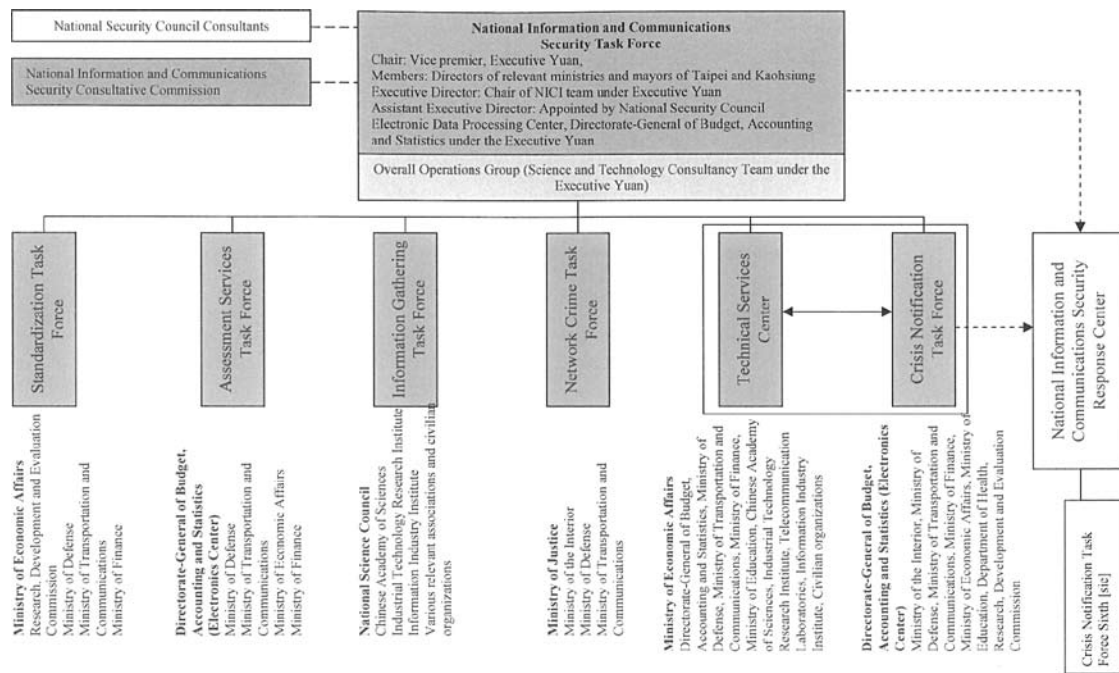


Figure 1. Structural organization of the National Information and Communications Security Task Force (National Information Security and Communications Task Force, Taiwan)

of life, whether in military or commercial applications, or in one's daily life. While enjoying the benefits that wireless technology brings, we cannot ignore associated security issues. In addition to technical administration, we must promote administrative measures, such as formulating wireless network security policies thorough examinations of equipment, security contingencies, and investigations. This will reduce risks to an acceptable level, as a means of striking a balance between enjoying the benefits of technology and maintaining concern for security. Preventing and controlling criminal activity in networks requires that we enact laws and regulations, regulate ISP providers, and keep historical audits and usage information as necessary. But it also means strengthening self-defense and accommodating the investigations into equipment, technology, and personnel performed by law enforcement agencies.

4. Contingencies for Potential Threats of Hacker Attacks and Information War. While enjoying the benefits of the Internet we are also exposing ourselves to threats. Interested people can pilfer our personal information by means of penetration or monitoring. Hacking incidents are

increasing as Internet access becomes commonplace almost everywhere. Increasingly, average users are placing higher demands on the prevention of illegal attacks. This is why Taiwan emphasizes use of human resources to advance various security means, in order to achieve its comprehensive anti-hacking objectives.

5. Establishing Sound Regulations for Information Security. Taiwan's laws and regulations for information and communications security can be traced back to April 20, 1987. The Executive Yuan enacted a directive entitled "Standards for Maintaining Computer Equipment Security and Confidentiality of Information for Agencies under the Executive Yuan" (Tai Ching Tzu No. 7501). The Internet was not yet prevalent, so the directive primarily regulated computer equipment security, information confidentiality, and the control of information operations. It was superseded by the "Regulations on Information Security for the Executive Yuan and its Subordinate Agencies" on September 15, 1999.

6. Primary Developmental Trends in the Regulation of Information Security.

(1) Enact technical standards for information and communications security;

(2) Enact regulations and reference guides for operations related to information and communications security performed by various government agencies;

(3) Plan and build test technology for information and communications security;

(4) Plan and build authentication procedures for information and communications security.

Threats and Challenges

In a speech to high-ranking People's Liberation Army cadres, Chinese Communist Party Chairman Hu Jintao stressed that the PLA must strengthen its information warfare capabilities, to ensure it will be able to win regional wars featuring high technology, in any potential conflicts. In response to the PRC's advancements in capabilities, Taiwan's 2007 *National Defense Report* noted the Chinese Communists' potential to attack Taiwan in the future will include multidimensional modes: complete information and electronic paralysis; long-range precision strikes; rapid warfare; in addition to carrying out

potential measures such as deterrence, paralysis, and strategic warfare.

Chinese Communist research into information warfare began with the experiences of the United States in the First Gulf War. The Chinese Communists' understanding of information warfare is mainly that it is a new form of war, and that it uses energy to release changes in patterns. In particular, the Chinese Communists believe future military operational space will be "five-dimensional," and that cyber warfare and space warfare have become the new frontiers for competition between countries. So-called "five-dimensional" operations refer to the realms of "land, sea, air, space, and electromagnetics," along with the idea of taking war from the conceptual level to the level of reality.

Widespread utilization of information systems means that information and network security have become ever more critical national security issues. As such, information and network systems and facilities are now key infrastructure. In addition to general sorts of commercial, hacker, and criminal attacks, information security faces organized network attacks perpetrated by China. These have become a daily occurrence, and are a major threat to information security:

1. General Information Security Threats. Information security incidents such as hacking websites, tampering with Web pages, and stealing information are frequent events. Types and means of threats include:

(1) Spreading malicious code: This includes viruses and Trojan horses, as a means of sabotaging computer operations and stealing information.

(2) Unauthorized access: Account passwords are stolen and system security leaks are exploited or passwords are cracked to infiltrate computer hosts in order to delete, alter, or steal information.

(3) Setting up fake websites for organizations or fake network services. "Phishing" refers to obtaining users' private information such as account numbers, passwords, and identification files by deception.

2. Threats from Strategic Information Warfare.

(1) Information warfare is not limited to attacks on information and network systems. Information warfare achieved importance as early as the 1990-91 Gulf War. American think tanks proposed the idea of "strategic information warfare," using of the news media and psychological propaganda in addition to attacks on information and network systems themselves. Perception management is utilized to influence the masses' political perception of their governments. In other words, it refers to both information content and information conflicts being broadcast.

(2) Based on its views of "asymmetric war," China has for a long time aggressively been putting resources into IW research and development. In addition to emphasizing attacks on information networks, China is combining public opinion, psychological, and legal warfare in an organized and systematic fashion, stressing its so-called "Three Warfares." The PRC has unleashed strategic information and message attacks, and is attempting to break down Taiwan's defensive strengths by misleading the masses, confusing our perception of who is an enemy and who is a friend, and weakening the morale of the people.

3. Security Threat Posed by China's Emphasis on Information Warfare. China's utilization of information warfare is extensive in both attacking and defending. When it comes to defense, China has assembled a dedicated team of "network police" to perform surveillance of the activities of Web surfers, and has set up its "Golden Shield Project" (dubbed the "Great Firewall") for comprehensive surveillance and control of the content and flow of network messages. The Information Industry Ministry has a new regulation requiring website owners register with the government, or their websites will be shut down. Even foreign companies must submit to network surveillance, otherwise China prohibits anyone from investing in them. In terms of attacks, Communist China has used following means against Taiwan:

(1) Organizing a large-scale network force: The explosive growth

in Internet use in China has not only attracted investment from information industries throughout the world; China has taken this opportunity to develop its information warfare capabilities. It has established what it calls a "Cyber Army," which gathers intelligence on foreign governments and enterprises. Further, it becomes an attacking force when necessary, paralyzing opponents' computer networks. In fact, many western countries, along with Japan and Taiwan, have been subject to frequent network attacks. While some of them have been perpetrated by hackers working independently, the majority originated in specific domains within Chinese territory, and were clearly organized actions.

(2) Network psychological warfare: One could say China is the only country engaging in large-scale Internet and public opinion warfare. In addition to the defensive and control measures noted above, China has been even more aggressive in organizing professional "Internet opinion personnel." These number upwards of fifty-thousand people whose main task involves impersonating regular users in Internet discussion forums. When opinions arise which are unfavorable toward the Chinese government, they defend the government views, and even launch counterattacks. Their primary goal is to manipulate public opinion. In addition, China has incorporated cell phone communications within the sphere of control, so that all text messages are monitored.

Opportunities and Turning Points in the Fight against Information Terrorism

Criminal activity and attacks in the information realm are increasing, and they are problems of great concern. In particular, terrorists have moved from traditional ways of thinking to using the broad reach of network platforms to achieve their ideals and objectives. Today's democratic nations need to consider and pay particular attention to this issue. There is a critical need for policies to meet this new and unprecedented crisis. Before we think about how to approach information

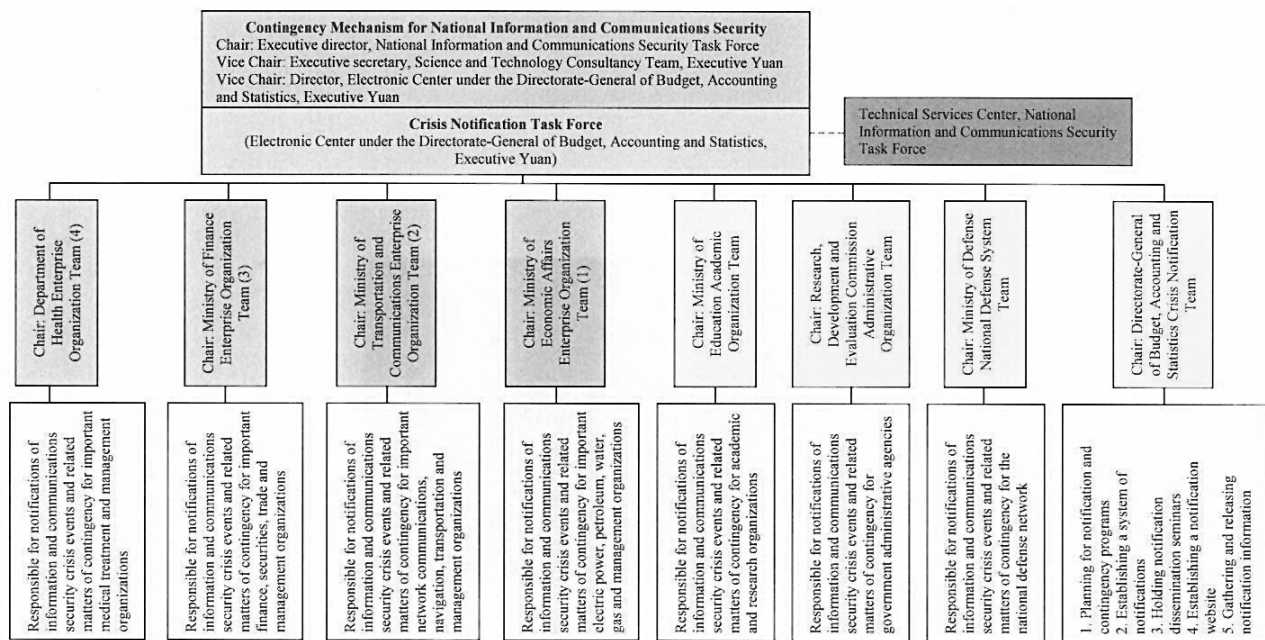


Figure 2. Structural organization of the National Information and Communications Security Contingency Center (National Information and Communication Security Task Force, Taiwan)

terrorism, we need to understand how terrorists make use of information to achieve their goals:

7. Methods of Information Warfare Used by Terrorists. Only by understanding the IW methods available to terrorists, and knowing the enemy as you know yourself, can we achieve victory. Terrorist tactics are mostly similar to those used by the average computer criminal, but there are notable differences:

(1) Most computer criminals will attempt to erase their tracks after committing crimes, so that they can escape scot-free. By contrast, if the terrorist's objective is shock effect, he will typically attempt to create as large a public impact as possible when he paralyzes a system;

(2) Most computer criminals are in it for their own pecuniary benefit. Alternately, terrorist attackers typically consider themselves to be righteous, and very few act for pecuniary benefit for fear of getting involved in disputes. Nevertheless, terrorists often make use of networks to launder money;

(3) Unless they are engaged in retribution, very few computer criminals aim to destroy computers and other support equipment. Information

terrorists may attack and destroy physical equipment.

8. Methods of Information Terror Attacks. Having reviewed the differing modes of attack, one can imagine that the terrorists' methods of attack would include the following:

(1) Stealing confidential information: Terrorists make use of network attacks, social engineering, and human contact to steal important classified or sensitive information;

(2) Paralyzing systems: Terrorists make use of malicious code such as viruses, Trojan horses, and worms. They also paralyze systems, make information disappear, and engage in denial of service attacks;

(3) Physical destruction: Terrorists engage in the sabotage, especially government information systems (military, economic, defense, diplomatic, etc.) as a means of paralyzing government operations.

9. The Contribution Taiwan Can Make in the Fight Against Terror. Once we understand terrorist information warfare tactics and methods, what kind of contribution can Taiwan make in the war against terror using our existing information technology?

(1) Taiwan's legal efforts in the War Against Terror have produced its Anti-Terror Activities Act;

(2) Taiwan has formed anti-terror organizational structure that combines various national security systems and the Executive Yuan;

(3) Taiwan's potential contributions include:

1. Taiwan has never had any terrorist activity nor the conditions for its presence. However, terrorism as a form of organized crime crosses borders to obtain funding. These criminal activities include smuggling drugs, human trafficking, money laundering, and other inappropriate financial operations. These are important security issues for Taiwan. With ample evidence of terrorist crimes, plus clues for tracking their activities, we could pursue these criminals. Taiwan could also establish cooperative mechanisms, and strengthen existing ones, to help other countries prevent terrorist activities.

2. In the future, regional terrorist groups might wish to use Taiwan as a gateway for their support or planning activities, in order to strengthen their disruptive activities in other Asian countries. Taiwan can effectively prevent terrorist elements from entering

and leaving the country by strengthening its overall security control capabilities. Rigorous surveillance actions can show evidence of terrorist activities, and provide early warning.

10. Opportunities are Turning Points. Taiwan ranked sixth among 64 countries surveyed in the “IT Industry Competitiveness Index” released by the Economist Intelligence Unit in 2007. However, Taiwan is first in the area of IT labor productivity and third in the area of environment for research. This illustrates Taiwan’s notable information and network technology strengths.

In his book *The World is Flat*, Thomas L. Friedman describes “*the rise of Netscape and the dotcom boom that led to a trillion dollar investment in fiber optic cable; the emergence of common software platforms and open source code software enabling global collaboration; and the rise of outsourcing, offshoring, supply chain planning, and insourcing (also known as insourcing where internal business is taken on).*” Friedman held that these flatteners converged in 2000 and “*created a flat world: a global, web-enabled platform for multiple forms of sharing knowledge and work, irrespective of time, distance, geography, and, increasingly, language.*” This is why we believe that even though the Internet world is full of dangers, it contains opportunities and turning points.

(1) Opportunities

Even though every corner of the world is different, due to geography, culture, religion, and economics, the rise of the Internet has shortened the gaps between people. Every second that the clock ticks, various types of information speed along fiber-optical cables and via microwaves to every corner of the Earth. The concept of the global village has taken shape, so every country in this new century has an opportunity for collaboration. Taiwan holds an important strategic position which is pivotal in the Asia-Pacific region. We have already constructed a Contingency Mechanism for National Information and Communications Security, allowing our nation to share information, and collaborate with any country in the area of network security.

(2) Turning Points

In the future, the world will be highly information-based. Rapid and instant information will be the key to survival. “The Earth is round, but the world has been flattened by the information highway.” Taiwan is situated within this torrent of information. Based on its efforts and guided by the right policies it will emerge as a major information power.

1. We have excellent and indispensable technical human resources—we were the first to discover the method behind the zero-day attack.

2. We are open and willing to share our practical experience with friends.


3. We never fail to do the right thing.

Taiwan can make use of the incredible reach of the Internet to make its contributions in the elimination of global extremism. The distance between countries has been shortened by information networks, and utilization of the Internet to eliminate terrorism will be the turning point in the struggle for world peace.

Conclusion

World trends are even harder to fathom now that we have entered the era of information networks. Their gradual application throughout the world brings

a new kind of international influence. At the end of 1999, a United Nations appeal recommended the Internet be seen as an effective tool for global justice, and as the communal wealth of humanity. However, in the “New Economy” where information technology and knowledge innovation are used to create value, is still the privilege of wealthy countries. Most developing nations are still “information poor, left behind by the “digital divide,” and may be cast further to the margins of the global economy. The War on Terror is a struggle which never ceases, and nobody knows when the next disaster is going to happen. As such, we will rely upon government policy, buildup of network infrastructure, and improvements to information security to minimize damage—or even prevent terrorist attacks from happening again.

Future wars will tend to be multifaceted. Rapid and instant information will be the key to overall victory or defeat. Information warfare is a new pattern of conflict which has developed against the backdrop of this trend. Recent terrorist incidents have occurred in major cities in several countries, turning terrorism into the major focus of attention, and making it very apparent that our anti-terror actions cannot be delayed. 



Major General Tschai “Jane” Hui-Chen currently serves as the Director, Information Assurance (IA) Division, Deputy Chief of the General Staff for Communications, Electronics, and Information (J6), Taiwan Ministry of National Defense. She is responsible for directing and overseeing the strategy, policy, and program development of MND’s information assurance and information warfare programs. Since 2000, she has served as the Deputy Director of the Information and Communications Security Technology Center (ICST). While serving as the Director of the Training Institute for the Joint Information Operations Command, she was also assigned to organize, equip, and operate the Information Warfare Center (IWC), the first such IO task force in Taiwan. MG Tschai holds a Ph.D in Computer and Information Science from Syracuse University, New York.

China's Comprehensive IW-Strategy Link

By Timothy L. Thomas

Editorial Abstract: Mr. Thomas describes how China's Internet reconnaissance capability is central of establishing the strategy of "winning victory before the first battle." Associated actions include China's focus on collecting technical parameters of other systems from which Chinese specialists develop countermeasures. A review of current Chinese IO theory reinforces their preemptive cyber strategy policy.

Introduction

Information operations offer the Peoples Liberation Army (PLA) a new vector for the Chinese military's transformation from an industrial to a modern day force. Recent Chinese White Papers on national defense describe this vector as the requirement to informationize the armed forces. The 2006 White Paper, for example, states the RMA is developing worldwide and, based on informationization, military competition is intensifying. This document adds that informationization will be used as the main criteria to measure the qualitative improvement of the PLA; that for China to build a strong defense, it must build informatized armed forces and be capable of winning informatized wars by the middle of the twenty-first century; and that the PLA has built virtual laboratories, digital libraries, and digital campuses to support the training and teaching needed to field this informatized force.

How IO Has Changed in China over the Past Few Years

The basic definition of information operations has evolved slowly over the past ten years. Only two of scores of definitions will be discussed here, albeit two proposed by very influential people in the Chinese IO arena. In 1999, IO specialist Yuan Banggen stated that information operations are specific information warfare (IW) operations. He added that IW is the core of informationized warfare, whereas information operations are the manifestation of information warfare on the battlefield; that IO means information wars in the narrow sense, that is the military field; and that IO includes integrated, high technology countermeasures. According to Yuan,



People's Liberation Army flag.
(Wikimedia)

IO's theoretical system is formed from two levels, basic and applied. Basic theories consist of concepts such as its organizational structure and technological equipment, command and control for IO, and so on. He categorizes applied theories into offensive IO and defensive IO; strategic, operational, campaign, and tactical levels; and into peacetime, wartime, and crisis-period IO. IO's two missions are preparation and implementation. Yuan notes that principles are centralized command, multi-level power delegation, multi-dimensional inspection and testing, timely decision-making, and the integration of military and civilian actions with a focus on key links. Overall, Yuan states that all activities of IO focus attention on command and control.

A 2005 book, *Study Guide for Information Operations Theory*, offers several definitions of IO, and these have progressed over time. Dai Qingmin, an IO specialist and former chief of a General Staff Directorate, and his co-workers note:

At present there are three main definitions for information operations. The first is as follows: 'Information operations refer to operations used to gain and maintain control over information.' This definition expands

the domain of information operations, as there are quite a few ways to gain and maintain control over information. Second, 'Information operations refer to a series of operational actions employed by two sides in a conflict in which the enemy's information systems are used or destroyed and one's own information systems are protected as a means of gaining the power to acquire, control, and use information.' Third, 'Information operations refer to a series of operational actions undertaken to gain and maintain information superiority on the battlefield or control over information. The two sides in a conflict use electronic warfare or computer network warfare to use or destroy the information and information networks of the enemy and protect one's own information networks as a means of acquiring, controlling, and using information.'

Clearly, the targets of information operations are information itself, information systems, as well as peoples' cognition and beliefs. IO means employed include information (both information media and information content) and weapons and equipment dedicated for attacks on information systems. Information operations involve both attacking and defending.

Dai and his co-workers added one more definition of IO in this book. The description lists the targets of IO and the means employed, stating:

Information operations are defined as a series of countermeasures employed by two sides in a conflict in which information or weapons and equipment controlled by information and dedicated to the destruction of information systems are used in order to influence and destroy the enemy's information, information systems, and cognition and beliefs, along with preventing the influence and destruction of one's own information,

information systems, and cognition and beliefs in the same manner by an enemy.

China's emphasis on countermeasures is a significant deviation from Western definitions. When the PRC collects technical parameters of other systems, they develop countermeasures as a sort of asymmetric response. China's 2006 White Paper, when discussing army projects, noted information countermeasure units were one of three organizations requiring priority development. The primary reason behind this force may be to construct IW countermeasures.

Neutralizing the Internet Against Extremism

China's police are starting to use cartoon police characters on domestic Internet sites to warn users against using illegal content. At the moment these friendly looking male and female cartoon character alerts walk, bike, or drive across the screen at half hour intervals on 13 of China's most popular portals. According to the Beijing Public Security Ministry, these virtual police are expected to populate all registered websites in China in 2008.

While these animations warn users that someone is watching, such warnings are a far cry from neutralizing an extremist's use of the Internet. With 137 million users at present, and an Internet population expected to surpass the US in two years, the challenge could be a stiff one. The common tactic is to simply close down domestic websites deemed extremist or subversive or to intercept emails with words like "Falun Gong" or the "Dalai Lama." Email services in China are obligated to hand over user data and communications to Chinese security officials if asked for such material, which is another way to help neutralize an extremist's use of the Web.

In order to stem the tide of Internet crime, China reportedly increased the size of its Internet police force in 2000 to some 300,000 personnel. While this

figure is difficult to comprehend, these crime fighters are part of the Ministry of Public Security and, thus, may have jobs other than fighting crime (espionage, etc.). The Internet police are mainly responsible for carrying out supervision, analyzing information content flowing through local communication systems or the Internet, fighting computer viruses, cracking down on Internet crimes, and stopping the spread of "harmful information." It is the influence of the latter, of—the extremists and nationalists—that China wants to limit inside its borders. However, very little has been written in China on the Internet war in Iraq, and the fight against extremism worldwide.

China wants to make this a joint effort. Reserve, militia, PLA, and civilian forces are conducting joint



The People's Republic of China in its Asian context.
(Wikimedia)

operations against notional intervening IW forces. This integration is underway in the form of a proposed 'cyber security force' (CSF). Qu Yanwen, a security specialist, proposes a unit composed of members of the PLA, the Ministries of State Security and Public Security, and technical specialists. Local authorities state Chinese political, economic, and military security is in danger due to the nascent stage of development of China's networks. Weaknesses exist in financial security; in defending against cyber attacks against information networks of key organizations and computer-based fund raising operations and scams; in information control over data that can affect the stability of public order; and in military information security. Within the PLA, the Shijiazhuang Army Command

College, the Navy Command Academy, the Air Force Command Academy, and the Second Artillery Corps Command Academy met in July 2007 to work out an overall joint teaching program for the three armed forces. They are trying to share information resources and exchange experiences via the Internet, among other issues.

According to one report, arrests and prosecutions for endangering state security have risen sharply overall since 11 September 2001. In the two-year period ending 31 December 2002, more than 1,600 people were prosecuted for endangering state security, most after the terror attacks on the US. Many of those arrested and prosecuted hail from Xinjiang, which Chinese sources characterize as an autonomous region in the northwest of the country, that is

home to a large and restive Muslim population. China's government has used the war on terror to crack down on those seeking greater autonomy, including those who do so by peaceful means.

What we do know about the domestic population arrested for political crimes is of interest. John Kamm, President of the Dui Hua Foundation ("dui hua" means "dialogue" in

Mandarin Chinese, and is a non-profit, human rights organization), wrote that about one-quarter of those arrested are non-Han Chinese, principally Tibetans and Uyghurs. Since China is more than 90% Han, the number of non-Han arrests is well out of proportion to the rest of the population. Kamm writes that sentences for non-Han Chinese are typically longer than those imposed on Han Chinese. With some candor, China's government recently released statistics on people arrested and prosecuted for endangering state security, the most serious political offence in the criminal code. China's top prosecutor, Han Zhubin, revealed that more than 3,400 people were arrested from 1998 to 2002 for such crimes as subversion, incitement to subversion, espionage, and trafficking in state

secrets. Kamm adds that “Internet dissidents” make up the fastest-growing group of political prisoners.

China has been concerned about Internet political movement activities since at least 1996. In that year the East Turkistan Information Center (ETIC) was formed, operating out of Munich, Germany. This site now delivers news to 114 countries in seven languages, and focuses on news, both positive and negative, about the Uyghur cause. Calling Chinese Communists “fascist authorities,” the website covers incidents reportedly aimed at robbing the Uyghur culture of its ideological roots, via a massive reeducation campaign. In 2004 ETIC also established a Uyghur Internet TV station.

In response to these events, on 15 December 2003 the *Beijing Xinhua* news service reported that China’s Ministry of Public Security identified the East Turkistan Information Center as a terrorist organization and its director, Abudujelili Kalakash, as a terrorist. A week later, the East Turkistan Information Center offered to disband, if the communist state offered freedom of expression and Internet access to Uyghur Muslim minorities. In 2005, a Beijing Communist Youth newspaper, *Zhongguo Qingnian Bao*, identified East Turkistan terrorist forces as the main terrorist threat to China.

The battle for control of the news has not stopped. China reported on an incident in January 2007 and provided its version of a scuffle between the PLA and “ethnic militants.” ETIC’s website reported the conflict occurred in a different area than that reported by Chinese TV, and that more PLA servicemen died than was reported by Chinese authorities.

What is Special About Chinese IO?

The key to understanding the Chinese approach to IO consists of two unique and noteworthy issues. The first is the extent to which the Chinese integrate strategy with IO. The second related

issue is the focus on countermeasures and reconnaissance.

Peng Guangqian and Yao Youzhi, editors of the popular Chinese book *The Science of Military Strategy*, note that the PLA must be “guided by the principles of military strategy in the new era to bring forth new ideas to push ahead the principles of strategic actions for local war under high-tech conditions...” This strategy-IO or strategy-technology integration was also highlighted by other authors. Perhaps the most notable comments were made by IW specialists Shen Weiguang and Dai Qingmin. Shen, the reputed father of information warfare in China, notes “The issue of information and network security, which accompanies the development of informationization, and the rise and increasing prominence



*People’s Liberation Army colonel points the way.
(Defense Link)*

of information warfare, the form of warfare that is invisible and non-violent, is an issue of technology, **but above all else it is an issue of strategy.**”

Major General Dai Qingmin, the former head of the information warfare directorate of the Chinese General Staff, offered a similar statement about the importance and probability of an IW/IO-strategic integration. He notes:

Laying all one’s hopes on technology is dangerous. The road to future losses may not be from a fall in technology, it may be primarily poor strategy. In reality the informationization of the forms of warfare has opened up an even broader space for playing tricks and using strategy and for using the indirect to gain the upper hand.

According to Shen and Dai, even conditions of technological superiority will not allow for success in all cases, if one overlooks strategy.

IO provides the PLA with a new means for applying strategy, one that enables a new information-based use of manipulation, deception, and soft (computer) destruction as much as hard (physical) destruction. Noted Chinese strategist Li Bingyan offered three observations: first, that collecting too much information can be blinding and can prohibit or stilt strategy; second, that weak information technology nations can successfully attack strong information technology nations with the use of stratagems; and third, that information technology can serve strategy as an effective deterrent and prevent war from

ever breaking out (the Chinese think the use of information technology at the Dayton talks to end the war in the former Yugoslavia is a prime example of winning without fighting). These are direct examples of how IO and strategy are being integrated into Chinese thinking.

Peng and Yao offer other strategy-IO paradigms in *The Science of Military Strategy*. They write about the strategic maneuver aspect of strategy’s applied theory, and stating the struggle in the information field may lead to changes in strategic maneuver. In particular, a “strategic information operations force may become a new form of strategic maneuver in future wars.” If such a type of maneuver actually does develop, then IO experts must also explore questions in the applied theory arena. Will there be cyberflanking, cyberpenetration, and other cyber activities? One would think so, based articles that have appeared in authoritative Chinese military journals.

The second special issue after the strategy-IO link is China’s focus on countermeasures and reconnaissance. By collecting technical parameters of other systems, China can use them to construct countermeasures, as a sort of asymmetric response.

The Chinese note that the US launched reconnaissance in the form of electronic warfare and intelligence warfare more than six months before the First Gulf War began. Such US actions are in line with Sun Tzu's concept that "the clever combatant seeks battle after the victory has been won." Chinese theorists have certainly bought into this concept of reconnaissance and intelligence warfare well before a battle begins. According to General Dai, China's vision of future war first involves information reconnaissance, to collect technical parameters. This will ensure victory before the first battle. Reconnaissance (consisting of electronic warfare, radar, radio technology, and network reconnaissance) fits perfectly with Dai's and Sun Tzu's concepts and stratagem.

Dai's writings focus not only on collecting technical parameters, specific properties of information weapon systems and electronic information products, but also on information attacks. This implies that collecting parameters and performing reconnaissance are two prerequisites for preemptive attacks. Computer network reconnaissance helps choose which opportune moments, which places, and which attack measures will result in maximum success—if war ever breaks out. Peng and Yao seconded this concept, stating that IO is directly linked to the gain or loss of the initiative in war and thus "priority should be given to the attack and combining the attack with the defense." Thus it appears information technology has enhanced Chinese thinking with regard to preemption. Chinese military academics state that those who do not preempt lose the initiative, in what may be a very short-lived IO war.

Conclusion

Combatants in present day conflicts may find it easier than at any other time in history to obtain their wartime objectives through one campaign, or one battle in the IO age. The idea of sudden attack has changed, especially if one side possesses high-technology equipment and the other side only low-technology means, which allows for better reconnaissance and insertion

of preemptive mechanisms (back doors in computer programs, etc.). "Attack" doesn't mean "surprise" in the old sense, but rather that one side can't correspondingly react if they're aware of the enemy situation. You may know where all of the forces are on the enemy side, yet your systems can't respond due to preemptive computer measures an enemy has taken in peacetime. If war does break out, then preemptive attacks focus on "striking the enemy's information center of gravity and weakening the combat efficiency of his information systems and cyberized weapons." This allows one to weaken the enemy's information superiority and reduce his holistic combat efficiency.

Perhaps the current emphasis on gaining the initiative, and on short wars that are over quickly, are the main reasons that Dai gives the impression that preemption is a necessity, noting:

Actions such as intelligence warfare, psychological warfare, and campaign deception in advance of combat seem to be even more important to the unimpeded implementation of planning and ensuring war. For this reason, information warfare must be started in advance of other combat actions before making war plans and while making war plans.

In a sense, it is the special features of IO tactics and techniques that enable

the increased emphasis on cyber attacks more than traditional ground, sea, or air warfare. For example, a weaker force can inflict much damage on a superior force with a properly timed and precisely defined asymmetric information attack. Such an offensive may be impossible by traditional means. Multiple information attack actions can be developed, the offense considered as defense, and information barrier methods developed—by both strong and weak opponents. Attack tactics include information deterrence, information blockade, information power creation (electronic camouflage, network deception, etc.), information contamination, information harassment, nodal destruction, system paralysis, and entity destruction.

China's specific understanding of the intersection of strategy and information technology, especially as it relates to conflict, is not based on a wartime scenario in a practical sense; China lacks recent combat experience. However, from a theoretical perspective and use of IO techniques in peacetime, China has written extensively on the use of information technology and preemption. Based on the number of attacks worldwide attributed to China, they have given much thought to these issues, and apparently have some recent practical experience. ☞



Timothy L. Thomas is a senior analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. Mr. Thomas received a BS from West Point and an MA from the University of Southern California. He was a US Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S-2 and company commander in the 82nd Airborne Division. He is an adjunct professor at the US Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations, the Academy of International Information, and the Academy of Natural Sciences.

Bulgaria: The Rise And Decline Of Bulgaria's Interest In Information Operations

By Dr. Todor Tagarev

Editorial Abstract: Dr. Todor Tagarev described Bulgaria's need to build selective IO capabilities that assist in the conduct of NATO's effects-based operations. In particular he recommends Bulgaria should work to define generic units that are relatively self-sustained and can bring useful capabilities to a multinational operation. Bulgaria is also exploring what specialties it can contribute to the European Union with regard to critical infrastructure protection, where it hopes to remain competitive and capable of providing useful contributions.

Opinions expressed are solely those of the author and do not reflect official positions of the G.S. Rakovski Defense and Staff College, the Ministry of Defense of the Republic of Bulgaria, or any other governmental institution.

Introduction

At the beginning of the 1990s the Bulgarian military found itself in a void. The country had no paradigm that would facilitate the post-Cold war transition, and no one in the old or emerging leadership had experience in devising national security and defense policies. The armed forces enjoyed very high prestige in the eyes of the people, who were—and still are—proud of Bulgaria's military traditions.

While a member of the Warsaw Pact, Bulgaria was part of a very highly centralized system of force planning and conceptualization. The officer corps was well trained and very efficient in following Warsaw Pact (i.e. Soviet) doctrine, operational concepts, and tactics, but had minor (if any) contribution to force planning and the development of innovative concepts of operations. Thus, Bulgaria lacked officers with experience to generate doctrine, force structure, and concepts of operations to fit the requirements of the new security environment. In addition, until the end of the 1990s there was no civilian expertise on defense matters, neither in the executive branch nor in parliament. Not surprisingly, from 1990 until 1998 Bulgaria adhered to its "inherited" force structure, while its military organization evolved primarily under the pressures of rapidly declining defense budgets.

In such a situation the institutes within the Ministry of Defense that may have otherwise been instrumental in devising operational concepts, adequate to meet the changing threat, technological, and business environment, did not respond to the challenge. On the contrary, research organizations were



*Bulgarian soldier raises his national colors during a NATO exercise.
(Defense Link)*

among the first to suffer from budget cuts resulting in a brain drain. Nevertheless, around the mid-1990s a few curious Bulgarian officers, on their own initiative, decided to study information warfare and information operations developments and were able to attract the attention of the senior military leadership. Based on this, Bulgaria adopted a comprehensive set of new doctrinal documents from

1999 through 2002. The first part of this essay examines the respective developments and outlines the country's understanding of information operations and its component parts. The second part briefly addresses Bulgaria's approach to the neutralization of the extremist's use of the Internet. The final part of the essay examines the need to incorporate innovative operational thinking in the force planning process, and explains the reasons behind the decline of Bulgaria's interest in information operations. The essay concludes with a reiteration of the necessity to build selective capabilities for conducting information operations as a component of the NATO Effects-Based Approach to Operations (EBAO) and related developments within the European Security and Defense Policy—a necessity that may be met through a more realistic policy and efficient capability management. It is possible (and appropriate) to examine other component parts of information operations such as the security of information and command and control systems (for the military) and critical information infrastructure protection measures for the civilian sector.

Bulgaria's View of IO

The impressive utilization of advanced communications, information, sensors, and navigation technologies by the US military during the First Gulf War, 1990-1991, allowed the US-led coalition to achieve quick and decisive victory over Iraq. This placed information warfare among the top research topics for defense establishments around the world. But in Bulgaria, given the

overwhelming problems in dealing with a Cold War force structure and size under declining budgets, the official defense establishment was not able to react properly.

Fortunately, as early as 1992 Bulgarian officers got the chance to study in Western military colleges, and rapid access to Internet sources provided information at previously unthinkable ease and speed. The combination of these two factors, plus the process of democratization of Bulgarian society enhanced the opportunities for curious individuals to collect information, analyze, synthesize, and reach broad audiences. Thus, in the mid-1990s, a venture of individual researchers with professional interests in military affairs and in particular the link between advances in IT and warfare, culminated in the publication of the book *Information Aspects of Security*.

The authors of this book examined a series of issues: the relationship between security and IT developments; conflicts related to the emergence of an information society; the main technologies providing for a competitive edge in information age conflicts; and main issues in managing the information environment. Of particular importance for this essay is the examination of information warfare—its principles, levels, domains, and components. In the book, Velizar Shalamanov and this author define information warfare as: a system of actions undertaken in order to create information space, in which one side has superior understanding and use of strong and weak points in the political, economic, military, social, and cultural domains of activity of a potential enemy and its dependence on friendly sources of power, and at the same time does not allow effective enemy actions. The authors identified information as a distinct domain, powerful weapon, and lucrative target in the evolution of conflict. They defined the term “information power” as the capacity created by advanced technologies, procedures, and organization. Further, they define the information campaign as the main tool, used in combination

with traditional military means and approaches, to achieve information superiority, and distinguished two levels of this campaign:

- A strategic information campaign which ideally tried to achieve paralysis of the OODA-loop of the opponent;
- Command and control warfare campaign which supported strategic objectives through effects against the ability of the enemy to make timely and effective decisions on the use of its armed forces.

According to Shalamanov and Tagarev, the operation for achieving information superiority has six elements:

1. Security of operations—not allowing the enemy to receive adequate information on us; includes communications security, computer security, emission control, etc.;
2. Deception;
3. Psychological operations;
4. Electronic Warfare;
5. Physical effects on enemy C4ISR systems;
6. Superior situational awareness through the fusion of all-source intelligence

In addition, the authors examined the offensive and defensive aspects of information operations, the role of the media, and information aspects of operations other than war. Importantly, in a forward to that book General Miho Mihov—at the time a three-star equivalent and Chief of Staff of the Air Force and later (1997-2002) Chief of the General Staff of the Bulgarian Armed Forces—presented his views on the role of information in modern conflict. The following is a brief summary of his main points:

- Warfare has moved out of traditional domains and into the information domain;
- Information superiority is the means that may dissuade an opponent, postpone aggression, and even prevent a war;
- Winning the information war predefines the outcome of “classic” military activities;
- A new balance must be found between information power and firepower;

- The country has no alternative, but to prepare for information war.

A series of articles by the *Information Aspects of Security* authors, in the Bulgarian Ministry of Defense/Bulgarian Armed Forces official theoretical publication *Voenen Journal*, raised IWs awareness among Bulgarian security and defense experts. Further, it facilitated the debate on possible objectives in the utilization of advanced IT under new operational concepts, and the balance of priorities in the development of the armed forces.

In 1998, on the wave of rising interest in the relationships among security, warfare, and technology, the authors began publication of *Information & Security: An International Journal* with the intention to cover “scientific, technical, and policy issues related to national and international security in the Information Age, C4ISR technologies and systems, information operations, command and control warfare, and information assurance.” The journal’s stated objective is “to bridge the IT and the security communities, presenting state of the art, new findings, ideas, and needs of one community versus the other, as well as to present the latest research conducted ‘on the bridge’ between the two communities.”

General Mihov—already Chief of the General Staff of the Bulgarian Armed Forces—contributed an article to the *Information & Security* pilot issue, conceptualizing in the context of the reform of the Bulgarian Armed Forces, and examining information warfare on the strategic and operational levels. He further reasoned that information operations were turning into a main supporting operation, and in the future, would be a distinct operation of the armed forces, to be conducted jointly with other governmental and public organizations. Paraphrasing the definition proposed by Shalamanov and Tagarev, General Mihov defined the term information operation as: a system of actions for the creation of an information space, in which one side has superiority in understanding and using the strong and weak aspects in the political, economic, military, ecological, social, and cultural areas of activity of

a potential enemy and its dependence on friendly sources of power, while at the same time not allowing identical activities on its side.

He saw the objective of the information operation as “changing the way of reasoning and decision making of the enemy in the direction of our interests.” General Mihov defined the term “information superiority” and linked information operations with other activities of the armed forces.

Coincidentally, all three Bulgarian authors mentioned so far played key roles in the development of the first national military doctrine: General Mihov as Chief of the General Staff; Dr. Shalamanov as Deputy Minister of Defense for defense policy and planning; and this author as a civilian Director for Defense Planning in the Ministry of Defense. The *Military Doctrine* was the first official document treating the issue of information operations and other information aspects of security. For example, the doctrine lists “information war/warfare” among the modern risks to security (articles 9, 11), and states the military threat to the country may be expressed, inter alia, via information attacks of another state against ‘national strategic systems’ (article 16). For the first time, it set achievement of information superiority as a military task. According to article 62, “the armed forces protect the country through the application of a military-strategic concept for defense of the national territory, a struggle for information superiority, control of the air and sea space, and defense of a threatened theater of military activities.” Respectively, the doctrine defined as the priorities in the [technological] modernization of the armed forces “the C4ISR, identification and navigation ... systems, the means and technologies to provide for interoperability with the armed forces of NATO countries, and the transition to an information society” (article 97).

The *Military Strategy*—a follow-up document—reiterated many of the postulates of the military doctrine, including its Article 62. Additionally, it listed the “reliable

provision of information” among the main requirements towards the reform of the armed forces and defined the “strategic defensive operation” as a joint operation of the country’s armed forces that includes, inter alia, information operations.

Bulgaria produced a number of additional doctrinal documents between 1999 and 2002. The 2001 *Joint Operations Doctrine* shed further light on official views of information operations. For example, the title of Section 5 in the chapter “Joint Operations in Armed Conflict” is “Information Operations” with the subtitle “Operations against C4I systems.” It defined information operations as “a set of information effects, attacks, and battles, with coordinated objectives, tasks, place and time, conducted according to a distinct design and plan for solving the tasks of an information battle in the theater of military activities or on an operational direction.” It states that IOs support strategic objectives through their influence on the ability of an enemy to make timely and effective decisions on the use of its armed forces. The doctrine defines two component parts of IO as well as other realms:

- Defensive—protecting the effectiveness of our own C2 system;
- Effecting – influencing, damaging, and destroying the enemy’s C2;
- Other IO realms;
- Security operations;
- Disinformation (with a set of measures on the strategic, operational, and tactical levels);
- Psychological operations;
- Electronic Warfare.

Further, the doctrine designates the J3 staff as responsible for planning and coordinating the conduct of security operations, disinformation, psychological operations, and operations against the enemy’s C2 systems, and the J6 staff for organizing the protection of information.

The 2002 *Air Force Doctrine* delineates between ‘subordinated’ and ‘supporting’ operations, with special operations and operations against C2 systems being part of the latter. As

components of operations against C2 systems it lists security operations, psychological operations, disinformation, and electronic warfare. It assigns the air force a number of tasks, including countering an enemy’s command and control, aerial intelligence, and ‘special activities in the interest of information superiority.’

The 2002 *Land Forces Doctrine* includes a requirement that the Special Operations Forces are trained to participate in psychological operations and to support information operations.

The *Main Guidance to Operations Planning*, issued in 2000, followed the respective NATO documents and included requirements for two annexes to plans of operations (in addition to the more traditional ones)—on Psychological Operations and on Information Operations.

The publications of three additional Bulgarian authors are appropriate to our discourse. The first, Prof. Tzvetan Semerdjiev, published *Information War* in 2000. In a comprehensive manner he examined risks and threats to national security at the doorsteps of the 21st century, emphasizing those resulting from the proliferation of information technologies and communication channels. He introduced the concept of “national information space” and reasoned that defense should be organized in a number of echelons. Prof. Semerdjiev made detailed studies of the concept of information power, and applied the classic principles of warfare to elaborate on the principles of information warfare and the utilization of advanced IT.

The second author is Colonel Mitko Stoykov, who in 2003 published a book on the meaning of the information revolution for terrorism, and the way in which we organize our security system. Colonel Stoykov—then assigned to the Situation Center of the Ministry of Defense—examined three recent concepts: cyberwar, information war, and netwar in a comparative study of primarily US sources. His chapter on information operations was based almost exclusively on US doctrine:

Joint Pub 3-13, *Joint Doctrine for Information Operations*; FM 100-6; and Joint Publication 6-0, *Doctrine for Communications System Support to Joint Operations*.

This was probably the last comprehensive treatment of the issue of information operations by a Bulgarian author, to date. The main reason is that while downsizing of the Bulgarian Armed Forces continued, Bulgaria became a Membership Action Plan (MAP) country after the NATO Washington Summit and then, at the 2002 NATO Prague summit, was invited to join NATO. On its path to NATO membership, Bulgaria had to cope with a variety of requirements; interoperability and the protection of classified information had the strongest impact on all information-related issues. In combination with other constraints, these requirements overwhelmed the force planning and management capacity of Bulgaria's defense establishment. Just one example is that all cited authors continued to work and publish intensely on defense issues, but with no one focused specifically on information operations.

Most recently, Brigadier General Boyko Simitchiev—Chief of the Communications and Information Systems Directorate (J6) of the General Staff of the Bulgarian Armed Forces and Chief Information Officer for the defense establishment—contributed a paper to the journal *CIO.bg* that again raises interest in IO. In his opening statement he emphasized that the challenges of future war—and information operations in particular—will have a very important impact on the generation of requisite capabilities of the Bulgarian Armed Forces for participation in NATO and European Union missions. Without referring explicitly to the evolving concept of effects-based operations, he underlined the importance of achieving information superiority, and psychological operations' place in gaining the support of the local population. While developing capabilities to conduct information operations, we need to study the stability of our own systems performance against information attacks. In his conclusions,

he emphasizes that in the near future the Bulgarian military must be able to plan and to participate in the conduct of information operations.

A novel element in General Simitchiev's paper was recognition of cyberspace as not only the place for military and governmental information operations, but also by terrorist organizations. Extremists aim to recruit members, disseminate propaganda, videos, brochures, and training materials, as well as to coordinate terrorist acts in an anonymous and interactive form. Echoing General Mihov, Simitchiev



General Zlatan Stoykov, Bulgarian Chief of Defence with Lieutenant General Atanas Zaprianov, Bulgarian Military Representative to the NATO Military Committee (NATO)

stated that cyberspace creates opportunities for spying, asymmetric impact, and propaganda that may lead to winning wars. Therefore, the next part examines approaches to countering use of cyberspace, and the Internet in particular, by terrorist and other extremist organizations.

Bulgaria's Approach to Countering Extremists' Use of the Internet

With the amendment of military doctrine in the aftermath of September

11th, the Bulgarian Armed Forces were tasked by the legislature to contribute to anti- and counter-terrorism activities. However, an examination of Bulgaria's legislative framework on terrorism shows, by and large, this is a breach of law. Law enforcement organizations have the primary role in countering terrorism. This also applies to terrorist and extremist use of Internet, for a variety of purposes.

The Ministry of Interior in Bulgaria's executive branch is responsible for law enforcement. It includes three national services: Police, Security (counterintelligence), and Fire Safety and Protection of the Population.

The first organization that plays a role in countering extremist use of the Internet is the one dealing with organized crime. The National Service Police are tasked to counter criminal activities of local and cross-border criminal groups or organizations, to prevent terrorist acts, and to neutralize terrorist and diversion groups. Its Chief Directorate for Combating Organized Crime (CDCOC), with units in the Regional Police Directorates, "carries out independently or jointly with other specialized bodies operation and search activities of an informational and organizational nature to combat organized crime" related, among other things, to:

- Monetary, crediting, and financial systems
- Terrorist activities
- Computer (or cyber) crime
- Intellectual property rights

Second, fighting terrorism and extremism is among the main tasks of the National Security Service. This civilian counterintelligence activity identifies and neutralizes destructive processes that threaten constitutional order, the unity of the nation, and its sovereignty and territorial integrity. It also counters international terrorism and extremism.

Recently the Bulgarian Government announced plans for a major reorganization of its security agencies through the creation of a "National Agency for Security." The new agency unites three organizations: the National Security Service (currently under the

Ministry of the Interior); the Security Service (Military Counterintelligence) under the Ministry of Defense; and the Financial Intelligence Service (currently under the Ministry of Finance), and to place them under direct control of the Council of Ministers. This measure will raise the effectiveness and the efficiency of the fight against terrorism, organized crime, and crime at the 'high floors of power,' e.g. high-profile corruption.

A third realm of IO-related activities is protection of critical infrastructure, and in particular critical information infrastructure. Organizational developments in that respect are rather complex, and will not be examined in detail here. We only note that Bulgaria, as a member of the European Union since January 2007, adheres to EU Critical Infrastructure Protection (CIP) policies in particular as related to the fight against terrorism.

Accounting for the trans-border nature of crimes, aimed at or facilitated by the Internet, Bulgarian documents consistently express the readiness of the country for international cooperation, in particular in the framework of NATO and the European Union, but also in the expanding network of partnerships of these alliances and on a bilateral basis.

From a legislative point of view, a decree issued in the aftermath of September 11th prohibited any form of assistance—active or passive—to organizations and persons involved in terrorist acts, including efforts to recruit members of terrorist organizations.

Curiously however, the first cases against cyber crime involved breaches of intellectual property rights, and the illegal dissemination of software through the Internet. In those efforts, CDCOC joined forces with the Bulgarian Office of Business Software Alliance (BSA) that protects copyrights of software producers. BSA's influence was so strong that, according to a recent article in the newspaper *Capital*, the CDCOC unit tasked to fight cybercrime is "to a considerable degree modeled after the BSA views." The same article claims that the Ministry of the Interior orders Internet providers to block access to



Bulgaria in its southeastern European context. (www.info.bg)

certain websites, i.e., to filter access to information.

The respective articles in Bulgaria's Penal Code form the legislative basis for such actions. Finally, the law on protection of classified information and related additional regulations prescribe principles and a complex set of measures for the prevention of unauthorized access to classified information created, processed, stored, and transported in automated information systems and networks.

Capability Management Challenges & Possible Developments

Any novel concept of operations is of practical importance only if incorporated in defense planning and force development processes. Furthermore, implementation of any information operations approach hangs on proper definition and development of respective capabilities.

Briefly summarized, in capabilities-based planning, required capabilities are defined against tasks to be performed under specified conditions, and requirements to produce concept-driven effects. For this purpose required effects are decomposed and matched with component capabilities. Then capabilities, at levels defined during the force planning process, are

developed through the introduction of adequate procedures (or doctrine), organization, personnel policy, training, and technologies.

The implementation of this planning approach is extremely challenging, especially in the period after the year 2000, when the Bulgarian Armed Forces were downsized, and at the same time had to meet diverse interoperability requirements while sustaining its participation in Iraq, Afghanistan, Bosnia, and Kosovo operations. Bulgaria was even called upon to expand such participation in both its number of operations, and the numbers of soldiers deployed.

This combination of factors caused the relative decline of Bulgaria's efforts to further develop concepts of information operations and, more importantly, capabilities to participate in such operations. Nevertheless, during the past decade the Bulgarian defense establishment reached a certain level of conceptual and doctrinal maturity, assigning main IO responsibilities to military organizations, launching an ambitious program for the introduction of advanced communications and information technologies and, most importantly, gaining operational experience.

The main challenge at this stage is to promote information operations

requirements among all competing requirements, and to elaborate realistic IO policies and an efficient capability development plan. These must also account for NATO and EU policies and burden sharing arrangements, as well as for developments in the national security sector. It is fairly safe to make several predictions in that respect:

First, the development of unique IO concepts as a result of original thinking, and in particular the implementation of such concepts, would hardly be encouraged. Instead, the Bulgarian military will adhere to the NATO military policy on information operations and information operations doctrine, as well as the EU concept for military IO. Nevertheless, it is important to underline that Bulgaria has the potential and willingness to contribute to NATO and EU IO-related research efforts, concept development and experimentation, or innovative developments in other bilateral or multinational forums.


Second, when it comes to the contribution to allied or coalition operations, one should not expect Bulgaria will develop and provide a broad spectrum of IO capabilities. Possibly the country will select a subset of capabilities, and will specialize in their development and utilization. In this respect, define generic units that are relatively self-sustained and can bring useful capabilities into a multinational operation is a topic of particular research interest.

Third, the IO attack aspect will most probably be subordinated to the evolving effects-based approach to operations (EBAO). Bulgaria will contribute to the development of this concept in the framework of NATO.

Finally, while protection of one's own command and control is part of defensive information operations, other elements of the information infrastructure may also be of considerable importance for the security of the state and society. As mentioned above, Bulgaria adheres to the EU policy on critical infrastructure protection and the major efforts will be on its implementation. At this stage the EU policy covers the Internet, but does not explicitly include defense or law enforcement infrastructure. It is still to be seen whether and how the military will cooperate with other governmental organizations and private actors in protecting critical national information infrastructure.

Conclusion

From 1995 till 2002, Bulgaria's interest in information operations was on the rise, but it has not been so prominent in the last five years. The decline in IO

effort is relative—proponents find it very difficult to receive adequate financing among all competing requirements. The country still struggles to define areas of specialization within NATO and the EU in which Bulgaria wants to be competitive, and provide useful and efficient contributions. Nevertheless, it is possible to predict that Bulgaria will develop selective capabilities for conducting information operations as its contribution to the EBAO. The participation of the Bulgarian military in critical information infrastructure protection (CIIP) is less clear at this stage. The CIIP policy will reflect the policy of the European Union, with civilian organizations and the private sector in the lead. Whatever the decision, Bulgaria still needs a more realistic policy, and efficient capability management accounting, to meet developments in NATO, the European Union, and the national security sector. 



Todor Tagarev is Chair of the Defense and Force Management Department of "G.S. Rakovski" Defense and Staff College, Sofia, Bulgaria. He was the first Director of the Defense Planning Directorate in the Bulgarian Ministry of Defense since its establishment in early 1999. From May until October 2001, he served as Director for Armaments Policy. He is a 1982 Graduate of the Bulgarian Air Force Academy; received a PhD degree in systems and control from the N.E. Zhukovsky Air Force Engineering Academy, Moscow in 1989; and is a 1994 Distinguished Graduate of the US Air Command and Staff College at Maxwell Air Force Base, Alabama. Dr. Tagarev has authored or co-authored six books, including *Information Aspects of Security*, and more than 40 papers published in refereed journals. Since the early 1990s he is conducting research on chaos theory and complex systems as related to military issues, with a focus on information technology developments and their impact. His current research is concentrated on defense and force planning and on novel operational concepts. Dr. Tagarev is a member of the NATO Research and Technology Board and is a national representative on the RTO System Analysis and Studies panel. He is Managing Editor of *Information & Security: An International Journal*, <<http://infosec.procon.bg>>, and a member of the Editorial Board of *Connections: The Quarterly Journal*, <www.pfpconsortium.org>. -mail: tagarev@bas.bg.

Ukraine: Information Operations In Countries of the Former Soviet Union

By Dr. Georgii Pocheptsov

Editorial Abstract: Dr. Pocheptsov offers a very different definition of IO than the other contributors. He notes information operations are the achievement of non-information goals (social, economic, military, political) using information technologies. He offers some mass communication means for changing public opinion, and recommends altering channels of mass communications and mass meaning if one desires to change a target group's conscience. For fighting extremists, he recommends finding ways to disagree with reality in more "soft" ways; and work toward new ways of "interpreting events," instead of only working toward targeting the "user-website" relationship.

The Development of Information Operations in Ukraine

Ukraine, as well as other former Soviet Republics, has limited experience in using public communications to influence the mass consciousness. The process for creating one's own identity is slowed primarily due to a lack of experience as an independent mass culture. At the same time, however, Russia was able to "turn on" its mass culture, which created the necessary prerequisites to produce, for example, TV shows and soap operas on a variety of themes from romantic to patriotic.

Such a primary flow of information allows for the crystallization of the required configurations of virtual objects. Mass consciousness can only be altered using the channels of mass communications and mass meaning (for example, a bestselling novel or soap opera). The latter allows for creation of a parallel virtual world, where the configuration of the content is presented "as is," in the case of religion for example.

Information operations can be defined as the achievement of non-information goals (social, economic, military, political) using information technologies. Among information technologies we are currently seeing an increasing role for non-mass produced messages, such as rumors and direct contacts. This shift is driven by the inherent higher level of trust in direct contact communication as compared to mass communication.

As such we can emphasize two important characteristics of information technologies:

- They are directed towards the successful transition from information to another level (social, economic, military, political)

- They mimic natural communication flows. The opposite case would be the use of political advertising, or any type of advertisement, where the artificial nature of such communication flow is clear.

Information operations can also be divided into defensive and offensive,



*Republic of the Ukraine Coat of Arms.
(Wikimedia)*

although recent research underlines the connectedness of these processes. If we talk about offense versus defense in the former Soviet block countries (with the exception of Russia), they have only defensive information operations experience. For example, government institutions of the Ukraine gained experience in defensive IO in the following situations:

- A scandal involving tapes of the former guard of the President, that had an effect on both the local and international levels;

- Western accusations of the trade of the Ukrainian "Kolchugi" radar system

to Iraq, which produced pressure on both the information and political levels;

- The natural gas conflict between Ukraine and Russia; a conflict over meat and milk products trade; as well as other similar trade-related conflicts;

- Local conflicts of smaller intensity and duration (between Ukraine and Romania, Ukraine and Poland, Ukraine and Bulgaria);

- The Orange Revolution of 2004;

- The emergence of totalitarian religious cults, such as "White Brotherhood."

The press-secretary of the Ukrainian President at the time of the 'tape scandal' noted: "I was long affected by the tape scandal. It was the hardest time for President Kuchma, no other President was in a worse situation. I remember we had consultants who worked with President Clinton during his troubles. God, I thought, I wish I was faced with their problems instead of this!"

The gas conflict between Ukraine and Russia, which emerged around the particulars of the gas trade treaty, was interesting as both Russian and Ukrainian media attempted to create parallel interpretations of the same events for the Ukrainian audience. A consensus among experts was that Ukraine lost that battle.

We can also view the Orange Revolution of 2004 as a war of interpretation—one also lost by the government—despite the fact a large proportion of the media outlets were under government control. At the time, the opposition created a more compelling narrative, which engaged key audiences. The government was seen as slowing down the country's progress, and it

could not get rid of such an image. It is well known in the history of religion that faiths under pressure become more creative. Similarly, the opposition during the Orange Revolution was more creative than the government.

During the war of re-interpretations, especially during “colorful” revolutions, the same events achieve different meanings. Such wars display the following patterns:

- The more successful the narrative, the more favorable the interpretation of new events in accordance with this narrative;
- Good narrative submerges ambivalent facts;
- “Mobilizing narrative” is written from the citizens’ perspective, which makes it that much harder for the government to create a similar narrative.

Ukraine also witnessed new developmental means among totalitarian religious cults, such as “White Brotherhood,” which successfully took over a church building and made a call for the mass suicide of its members. No other former Soviet country experienced this. Investigations into the cult left unanswered questions:

- An organization of such magnitude could not have survived only through donations from its followers;
- The leader of the sect did not use hypnosis to influence followers, yet a large number of followers had some sort of psychological deficiency;
- It was difficult to define the nature of these psychological deficiencies, as well as the large number of followers and their geographical spread;
- One of the leaders of the cult was rumored to work for a special agency (KGB) [former Soviet intelligence].

The Ukraine was also used as a test-tube for several large-scale information operations that affected the whole population of the country. Local specialists in the Ukraine participated in political technologies and spin-doctoring. During the last decade, the practice of discrediting was always ahead of the practice of refuting negative information, which allowed some organizations to



Ukrainian officer demonstrates IT monitoring to NATO colleagues. (Defense Link)

“build up muscle” in this area. This offensively-oriented information sphere is characterized by:

- What is seen as information fact by one side, is seen as disinformation by another;
- Information conflicts are an extension of economical ones;
- A more powerful economical or political player is also a more powerful information player, as he has the necessary resources.

All Ukraine citizens have experienced a drastic environmental change—one that led to a life in a different civilization (from a Soviet to a post-Soviet one).. Both “Perestroika” and the Orange Revolution have similar characteristics, mainly a rapid change in ‘who is the enemy.’ The enemy played an important role in the Soviet model, as it defined everything. “Perestroika” followed this model:

- First Stage: **The Change**: an outside enemy is substituted by an inside one: a governmental system;
- Second Stage: **Use Of An Internal Resource**: all types of propaganda mechanisms are used in the internal attack;
- Third Stage: **Delegitimization**: the population refuses the power’s right to rule.

The Orange Revolution was also crafted by creating an enemy inside the government, not post factum as in previous examples, but during the process of its formation.

Overall the population of the former Soviet block countries have more experience with information operations than any other country in the world. During the Soviet era people learned to read between the lines of mass produced messages, thus intuitively stumbling upon the opposite meaning.

In order to speak about IO theory, we have to separate the players with theoretical and practical experience. They rarely intersect, which complicates the transition of the experience between the two. The practitioners fill the lack of theoretical knowledge with creative approaches, teamwork to generate ideas, and actual execution.

Ukrainian experience in the theory of information technologies is significantly slowed, since theorists do not participate in practice and practitioners do not write theory. Where common sense predominates, both substitute this for their lack of theory or practice.

The Ukrainian military position, at least that published in the mass media, has two characteristics: first, the level of novelty of ideas lies only in the very detailed aspects of the offense; second, there is a transition to a psychological sphere, which is where the terminology “informational—psychological influence” originates.

Academic research (such as doctoral dissertations) is an active area of the information sphere, as are information policy, and Ukraine’s international image. O. V. Litvinenko proposed what

can be called a 'culture-oriented model of IO,' in which the narrative introduced is taken from some local mythological structure. Additionally, Ya. Varyvoda analyzed Russian financial groups' information activities in the Caucasus region, focusing on those connected with economical and political interests. This author is creating what can be called a 'semiotic model of IO,' in which mass culture plays a crucial role.

As to Ukraine's international image, a powerful political player such as Russia looks at Ukraine as an object, and not as a player in information wars. The Ukraine is seen either at the intersection of the interests of Russia and US, or the US and Europe.

There are several agencies in Ukraine specializing in information warfare within the economic sphere. In 2006 these agencies held corresponding training to attract attention to their work, under the title "Ukraine: The Art of Future Information Warfare."

Conflicts in post-Soviet block territory frequently have underlying economic tension, although they are also frequently tied to political tensions. Apart from Russia, most countries have very limited access to TV broadcasting outside their own territory. Thus they frequently become the source of Russian attacks, as in recent actions against Lithuania, Ukraine, Georgia, Estonia, and Latvia. Just looking at this list, it is clear that the political component is present in these actions. However, it is possible that an economic war (using information warfare as a tool) also took place, due to two factors:

- There are fewer political restrictions over actions;
- There is a need to cut off economical ties due to political or military concerns.

More generally, information conflict usually develops through the following stages:

- Stage one: A point of conflict suddenly appears;
- Stage two: Public attention is brought and kept at the point of conflict;

- Stage three: The conflict fades (public attention is turned away from the conflict).

The conflict fading stage is usually long-lasting: in the case of Russian-Georgian relations, it lasted a full year. This was driven by the vivid events in the first two stages, not easily forgotten by the public. Even when the government wants the conflict to be over, it continues to linger.

For controlled conflicts—and all the conflicts on the post-Soviet territory are like this—the fading stage signals the end of the conflict. After event X happens, which was the sole purpose of the conflict, the controllers no longer invest resources, thus the conflict fades out.



Republic of Ukraine. (Univ. of Texas)

Russia has vast experience in conducting information operations targetting outside parties. Let's recall, for example, the "Romancing the Stone" situation, when the British Special Forces were caught in Moscow with a 'stone' used to read information from agents at a distance. As a result, Moscow's government passed a law restricting nongovernmental organizations, since one of the members of the British group was also responsible for distributing nongovernmental grants inside Russia. In 2007 a similar information conflict was observed around the poisoning of Alexander Litvinenko in London.

All major international players have dealt with some issue aimed at uniting the public: for the US it was recovering from the Great Depression; and for the USSR it was the propaganda during the foundation of the Soviet Union. The major players built the new picture of the world through traditional media environments: movies in earlier times, and TV now. Ukraine, with its problem of a political split along geographical lines, requires projects of the same magnitude to unite the country.

Information Warfare Strategies on the Internet: Fighting the Extremists

We can define the following characteristics of the Internet that do not easily coexist with items associated with visual culture:

- A more dispersed environment, where the objects are hardly connected to each other;
- A multitude of events that becomes less important due to their sheer number. As a result it is hard to respond to them with individual interpretations, which requires more general interpretation systems;
- Increased dependence on the source of the interpretations;
- The knowledge of the details comes before the understanding of the whole structure;
- An Internet environment is formed by interaction with its consumers.

The Internet environment is frequently analogous to a social network, since the consumer visits its "own" websites. The consumer trusts the information presented there more than other sources. The website and the consumer have a friendly relationship, as compared to the simpler 'consumption' relationship of newspapers or TV. Modeling such a "friendly" environment should incorporate the fact that models work with objects which do not interact physically with consumers. All objects lie in the information environment.

Several historical examples show a similar disconnect between the physical environment and the receiver's understanding of the environment:

• The WWII propaganda campaign with Japan, where in addition to nine messages a soldier could verify through direct physical contact, there was one message with informational evidence.

• A maxim was formulated during the election of former US President Richard Nixon: since there was no direct contact with the candidate, one should not change the candidate, but rather his image.

Another way to change the environment is to change the voter rather than the candidate. Therefore, there are several ways to change the elements of the communication chain:

• Keep the speaker and the listener constant, but change the message. This is the most standard way of creating communication;

• Change the speaker (or the content) keeping the listener constant;

• Change the listener, but keep the speaker constant;

• Change the context. For example, to diminish the negative interpretation of disasters, the Russian Ministry of Emergency Situations started a weekly TV program about disasters in the rest of the world.

The modification of certain “off limits” subjects can be painful for the audience, and usually should be avoided. For example, a figure of the Japanese Emperor was one such object; he remained unchanged even after Japan’s capitulation. Hence, certain political as well as religiously sensitive objects remain constant for the audience, thus making it harder to modify them.

However, there exists a distribution of genuineness within the social network: the more direct contact we have with our sources, the more we trust them. Yet as we move upward in any hierarchy, there are more possibilities to loose trust, as direct contact is less likely.

Speaking from [author] Marshall McLuhan’s view, the Internet environment is more similar to the acoustic than the visual environment. Let’s examine the following characteristics of such an environment:

• An audio environment does not have a definite distinction between the author and the listener, since everyone

can be both; Internet blogs provide this opportunity. A visual environment creates authorship and corresponding hierarchy;

• An audio environment moves away from individual to collective. Collective opinion, collective structures dominate here;

• Authority and authenticity are built through institutions, and not through people. Therefore there is a high level of stability, similar to those in Muslim society which are maintained through a religiously-oriented educational system.

We can use precisely these characteristics as counterstrategies:

• If everyone is equal in the acoustic environment, this makes it easier for your people or ideas to advance;

• The audio environment is more likely to be affected by a swarming attack, a la [author John] Arquilla, and not a standard centralized attack;

• The model of a “magnet” attracting attention, which can be realized through marginal changes that introduce doubt into the main version of events, without openly denying them;

• Major changes in this environment can only occur through extraordinary events (for example, news of Arafat’s death from AIDS can change the attitude towards his movement as a whole). Audio environments can act irrationally by shifting attention to the most vivid event, rather than the most important one.

General tendencies in the development of any environment follow the same principle: human systems try to expand, and thus subordinate any unclaimed environment. Physical, informational, and virtual environments all are constantly under attack by other physical, informational, and virtual environments trying to force the former to live under its rules.

The following goals highlight any attempt to modify the points of a conflict:

• A change of heroes, enemies, and victims;

• A change of the objects of attention;

• A change in the underlying motivation of actions;

• A shift of attention to the historical period and the symbols of that time.

The goal is to create a new virtual reality that would fit the interests of the communicator. This new virtual reality must not change completely: as a first step it can only question the validity of the previous reality. For example, we can keep the heroic event, but find a different motivation for it, such as struggle for power, cowardice, or other similar negative aspect. So the structure: “positive act—positive motivation” is transformed into a “positive act—negative motivation.” Let’s call this example *Negation Through The Change Of Motivation*.

During the destruction of the image of [Vladimir] Lenin, his story went through a ‘broadening’ of his personal characteristics, and as a result it was no longer a taboo or “off limits” subject. It was okay to move away from a canonical image. The stage of Lenin with a “human face” was followed by the stage of Lenin with an “inhuman face.” Thus even though this broadening of image was done with noble goals in mind, it was followed at the next step by a more negative characterization. Let’s call this device a *Negation Through The Broadening Of The Canon*.

Another device is to change the nature of the communications: a shift from storytelling from one point of view to another. Let’s take for example possible ways of telling the story of “Little Red Riding Hood.” The traditional version is told from the point of view of a little girl. But it is also possible to tell this story from the perspective of the mother, grandmother, or even the wolf. Let’s call this device *Negation Through The Change Of The Storyteller*. We can use this device frequently, as many events can be described from the point of view of different witnesses, allowing new information to be introduced.

The Internet environment has less inertia; therefore it is frequently used in situations when the environment of traditional media is blocked, for example, by authorities. A campaign in the Internet environment can employ different types of messages unusable in an official environment. It could be a

campaign similar to dissemination of rumors, which takes on a second-life through repetition.

The environment which serves as a source for extremist/terrorism-friendly feelings is very ritualized and closed. The main goal of an Internet counter-propaganda war, which has very well defined rules about both allowable and banned actions and messages, should be to increase the number of possible future life directions of an individual. Specific results of such work are:

- A deceleration of the processes of moving towards a goal predetermined by the creators of the environment;
- An introduction of the possible “crossroads” that can shift the attention or action away towards more secondary tasks;
- An introduction of new models of individual development.

The destruction of the pre-programmed nature of terrorist behavior can be done by increasing the number of options for development, where one can transition from one state to another. For example:

- Breach of the interpretation of real events;
- Breach of the understanding of virtual objects;
- Breach of the motivations and goals of terrorism by showing that they can be achieved using other means.

The destruction of the interpretive model of the object is done by introducing a new opposite characteristic: adding a negative feature to a positive object or adding a positive feature to a negative object. For example, when the US was bombing Afghanistan (a negative object), the addition of dropping food supplies and not bombing on religious holidays added a positive feature to the object, which slowed down the creation of the solitary negative view.

In another example, the Orange Revolution in Ukraine destroyed the legitimacy of power, by introducing new connections: not just power, but “criminal power.” According to scholar George Lakoff, trying to dispute a particular framing of an issue does not destroy it, but rather strengthens it. We should refocus away from disputing

someone else’s framing of an issue, and towards creating and maintaining a new one. A more global goal in this case is to conceptually change and modify the virtual environment by:

- Change of heroes;
- Change of enemies;
- Change of sacred texts which make a coordinated system of heroes, enemies, and victims.

Such principal change is hard to achieve. Therefore we talk more about a correction of the meaning of heroes, enemies, and sacred text. This triad is interconnected: by changing enemies, we change the heroes, and vice versa.

New meanings serve as goals in information warfare. These should not repeat existing and conflicting themes, which would ease their acceptance into the mass consciousness. The generation of new meanings can be seen as a separate research task. Using another historical example, when the Apostle Paul introduced communion with bread and wine, where the latter is seen as blood, introduced something that goes against Judaism, which does not allow the use of blood. But, this practice was close to pagan religions, where the use of blood was accepted. The main obstacle to development of new meanings is that they are hard to come by in a world flooded with old meanings. If the technical aspect of human civilization has developed rapidly, the social aspect is, paradoxically, advancing slowly.

The Internet-environment can fulfill three tasks:

- Compensating for the lack of something in reality (for example, film and comic book superheroes appeared as a reaction to the Great Depression);
- Reinforcing reality (for example, extremism reinforces the existing confrontation between the East and the West);
- Transforming reality (for example, the US war for Muslim hearts and minds is designed to negate the negativity directed towards the West).

Perestroika, the Orange Revolution, and the war for the hearts and minds of Muslims are fought in a highly controlled (by ideology or religion) environment. In this case it is only possible to create a new

virtual reality using more “soft” tools, without engaging in direct conflict.

Yet another counter strategy is creation of an alternative virtual reality:

- Stage One: Expansion - broadening canonical frames of the description, which allows addition of negative features into the positive objects, and positive to negative;

- Stage Two: Negativity - addition of negative features into the positive objects, and positive to negative;

- Stage Three: Change of enemies into friends - this is a final stage of changing the virtual reality model.

Political leaders go through the same stages when they go from admiration to condemnation. Mikhail Gorbachev, for example, went through this process as did most major figures from his administration. Ukraine’s Orange Revolution went through a stage of controlled chaos, which made it easier to change the model of the world of the mass consciousness. For that purpose Perestroika used empty store shelves, mass protests, and the fight against alcoholism, which resulted only in longer lines in the stores. The Orange Revolution openly expressed insubordination to the government, used the main square of Kiev as a stage for protests, and used the previously-noted presidential tape recording scandal to replace the serving president.

In many ways the West did not win the Cold War on the level of ideologies, where there were no deviations, but rather on the level of reality—everyday existence. Ballpoint pens, bluejeans, etc. turned out to be more powerful “weapons” than real ones. This happens because each element of everyday life carries inside it the element of virtual reality—new meanings that can disagree with accepted reality in more “soft” ways. Russia faced the problem of confronting foreign influence much earlier than the time of [Emperor] Peter I. This was a problem during the governance of his father, Tsar Alexej Mikhailovich. A. S. Orlov sees the emergence of this conflict even earlier during the times of Ivan the Terrible.

The opinions of that earlier time are very similar to what Muslim society now experiences. Both then and now, religion remains the main component of this society, subordinating everything else. From here, we can see a way to influence Muslim society: through building secular organizations, which have the potential for change. The same experience easily translates to the Internet environment: our goal is to build a new representation of reality in the new virtual world.

It is possible to borrow experience from other related disciplines. For example, social marketing suggests different types of interventions depend on the target audiences' motivations, abilities, and possibilities to act. We must incorporate all of these factors into an Internet-based information war.

For example, some suggest nongovernmental organizations become highly visible when their activities resonate with international nongovernmental organizations. The counteraction strategy in this case can be fighting against the interpretation of a fight for power or property in the light of the fight for human rights and democracy, when such interpretation is

provided by the local NGOs. In this way, such interpretation loses resonance.

However, information reality turns out to be more complex than one can assume from such analyses. In the case of the Internet, we can observe the following characteristics:

- Multitude of websites: blocking them is no longer effective;
- Websites change rapidly: it is hard to apply the same methods of influence on them;
- Decentralization: it is harder to attack the hierarchy;
- Reliance on local websites: this is the source of information in Arab countries.


It is also necessary to be closely connected to Arab culture as the only way to establish trust. Counterpropaganda requires even more complex constructs than propaganda, yet at the same time the consequences of such actions are harder to plan. Counterstrategy can be realized through counter-narratives, which can stand against the narratives of the terrorists.

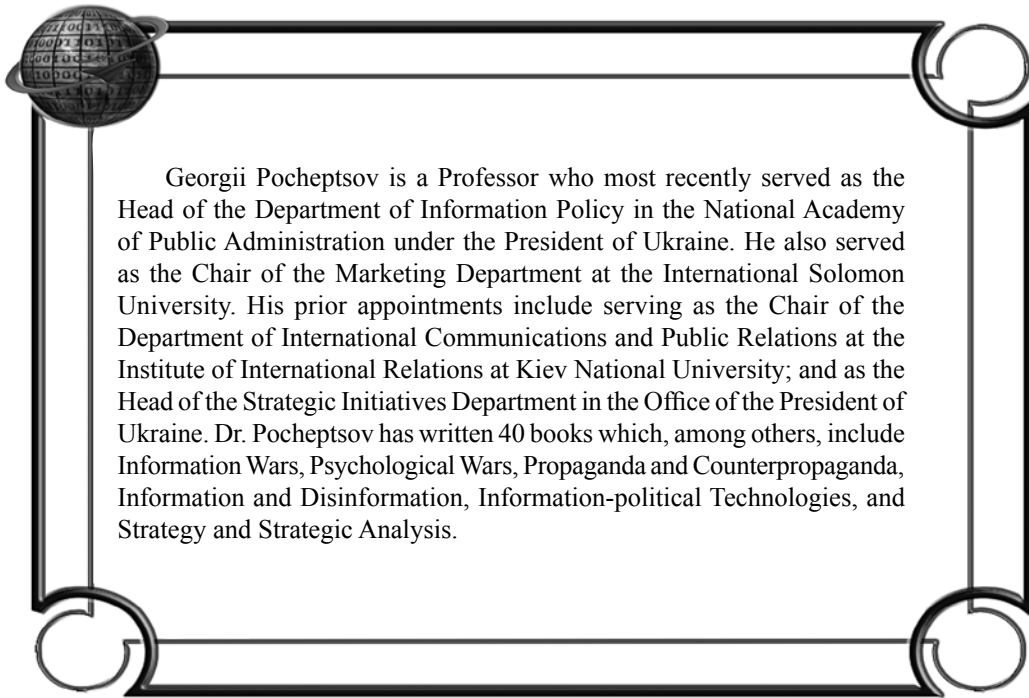
The most effective counter-narratives are the internal sources of influence. For example, the UK's Information Research

Department (part of the Foreign Office and MI6), has worked from inside the foreign field. As a result its articles and books did not refer to the true sources or true authorship. Therefore, the level of trust to such information was rather high.

Conclusion

The Internet is so flexible it allows us to use of a wider set of possibilities than traditional media. But the consumer wants to receive the information flow he is looking for. The conflict or fight should not be targeted towards the "user-website" relationship, as such would not be productive, but towards "event-ways of interpreting" relationship. It is important that this, or any such type of interpretation, should be acceptable to the consumer.

The Internet can foster the generation of new needs, which can also be an effective technique of information warfare. If the old needs stem from religious or political roots, the news ones do not have this connection and become a way of creating new meanings. New needs can be met: by new people, with new types of virtual objects. 



Georgii Pocheptsov is a Professor who most recently served as the Head of the Department of Information Policy in the National Academy of Public Administration under the President of Ukraine. He also served as the Chair of the Marketing Department at the International Solomon University. His prior appointments include serving as the Chair of the Department of International Communications and Public Relations at the Institute of International Relations at Kiev National University; and as the Head of the Strategic Initiatives Department in the Office of the President of Ukraine. Dr. Pocheptsov has written 40 books which, among others, include *Information Wars*, *Psychological Wars*, *Propaganda and Counterpropaganda*, *Information and Disinformation*, *Information-political Technologies*, and *Strategy and Strategic Analysis*.

Australia: Current Developments In Australian Army Information Operations

By James Nicholas, Major, Australian Army

Editorial Abstract: Major Nicolas notes Australia's armed forces are considering doing away with the term "information operations" and substituting the term "information actions" in its place. IO appears to be too much of a specialist's stove pipe, as influence emanates from all military activities. This change may better reflect the relative weighting Australia places on specific aspects of information-related issues, such as the terms "decision superiority" and "influence."

Introduction

Over a decade ago, the concept of "command and control warfare" was incorporated into US doctrine. It focused on enabling US commanders to complete their decision-making cycles more quickly and more effectively than their adversaries. Subsequently, the concept was refined and renamed "information warfare," and later replaced by the concept of information operations which has been incorporated in Australian and allied joint doctrine.

The developing concept of information operations is broader than its predecessors. While continuing to focus on the need to move through decision-making cycles more quickly and effectively than the adversary, IO also recognizes the need to influence and win support to enable friendly force military actions. This support primarily emanates from the local population in an area of operations, as well as from broader regional and international audiences.

Currently, the Australian Army is developing processes to enable conduct of information operations at the tactical level. While the Australian Defense Force (ADF) joint information operations doctrine allows the strategic whole of government to focus on operational planning, such doctrine does not provide commanders an adequate approach to conduct tactical level IO. Accordingly, many believe a gap exists in tactical Australian Army information operations.

Issues addressed here include: status of Australian joint and ABCA armies' doctrine; coalition experience; information operations versus use of the term information actions (IA); core elements of information actions; and information actions and intelligence preparation of the battlespace.

Status of Australian Joint and ABCA Armies' Doctrine

Australia published its first joint doctrine on information operations in 2002. Until early 2006 there was no change in Australian joint doctrine, and little change in the Australian/British/Canadian/American (ABCA countries') joint and armies' doctrine. In early 2006 the US issued a new US joint information operations publication. Some IO professionals envisaged that this publication, together with recent operational experience, may force change in the doctrine of ABCA armies.

Prior to 2007, the ADF produced joint information operations doctrine suited to the conduct of strategic and operational IO, but no lower order doctrine existed. The decision

to develop Australian Army land warfare doctrine (LWD) arose from the requirement to develop an Army information operations capability to address tactical requirements, for operations at brigade and below.

The 2002 doctrine provided an Australian perspective on information operations, based primarily on US doctrine of the time. Since then there have been shifts in joint US information operations doctrine, and although not fundamental, the changes are significant. In late 2006, the Australian Army finally began writing its own information operations doctrine.

Coalition Experience

Recent operational experience has generated considerable criticism of Coalition information operations. First, these criticisms include being unwieldy and difficult to apply; secondly, as being inadequate in relation to the practical aspects of gaining influence and support. This is especially significant in what may largely be an unfriendly operating environment, with an instinctively distrustful civilian population. Additionally, aspects such as training, inadequate allocation of appropriate resources, untrained staff, and inadequate intelligence support to IO, have all drawn close examination. A US commander recently wrote:

I am absolutely convinced that we must approach IO in a different way and turn it from a passive war fighting discipline to a very active one. We must learn to employ aggressive IO. We cannot leave this domain for the enemy; we must fight him on this battlefield and defeat him there just as we've proven we can on conventional battlefields.

Complicating our efforts in the information domain is the fact that we are facing an adaptive, relentless, and technologically savvy foe. Our adversary recognizes the global information network is his most effective tool for attacking what he perceives to be our center of gravity: public opinion—both domestic and international. And the truth of the matter is that our enemy is better at integrating information-based operations, primarily through mass media, than we are. In some respects we seem tied to our legacy doctrine, and less than completely resolved to cope with the benefits and challenges of information globalization.

Such feedback may have been the basis for the decision at the recent ABCA Information Operations Project Team meeting to recommend the abandonment of the concept of IO, at least in its current form. The team recommends the term 'information operations' be discarded, but that the core activity

of *influence* be retained. British Forces are also conducting a detailed analysis of the influence component of information operations.

The ABCA report recommendations were an effort to ensure a less cumbersome application of various capabilities, and to meet situations where influence and support achieve a much greater weighting than at present. Thus the Australian Army views retention of the term ‘information operations’ as non-critical; however, retention of the underlying concept of ‘influence’ is seen as paramount.

Another critical need is to remove information operations from a specialist stove-pipe, and recognize that influence emanates from all military activities: either as a planned (list order) effect, or as an unintended (second or third order) effect.

Information Operations Versus Information Actions

Apart from the ABCA Project Team’s recommendation not to retain the term information operations (yet to be formally endorsed by ABCA), further examination of how NATO sees the IO construct led the Australian Army to examine alternative terms to describe tactical level information-related actions.

One issue with the term information operations is the current variety of definitions in use. The Australian joint doctrine definition is significantly different from US joint doctrine, and those of the other ABCA services.

The varying definitions reflect the relative weighting placed by different countries or organizations on the decision superiority and influence aspects of information operations. The current US joint and Army definitions focus on achievement of decision superiority, with somewhat less emphasis on influence. The current Australian joint definition addresses both aspects. The current NATO definition reflects the need for information operations to focus on influencing target audiences. The current US, NATO and Australian Joint formal definitions are:

(US Joint) *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.*

(NATO) *Coordinated actions to create desired effects on the will, understanding, and capability of adversaries, potential adversaries, and other approved parties in support of overall objectives by affecting their information, information-based processes, and systems while exploiting and protecting one’s own.*

(Australian Joint) *The coordination of information effects to influence the decision making and actions of a target audience and to protect and enhance our decision making and actions in support of national interests’.*

A second issue with the term information operations is that it is somewhat at odds with other Australian Army doctrinal guidance and recommended ABCA standards. At present,

the term “operation” is used openly, with a wide range of Actions described as operations. Examples are “bridging operations,” and “transport operations.” The reference aims to establish tighter usage and more precise meaning within a defined spectrum. For example, the Australian Government’s commitment to stability in the Solomon Islands, Operation Anode, conducts four types of activities: offensive, defensive, stability, and enabling. Enabling activities can be described as tactical actions that link, support, or create the conditions for offensive, defensive, and stability activities.

Offensive activities in turn have a number of associated actions, such as: attack, advance, and pursuit. Within an offensive activity (including defensive, stability, and enabling activities), information actions would be intrinsically organic to the conduct of that activity, and may be represented in one or more (simultaneous or separate) information actions. We can use a number of tools to best effect implementation of the information action (Figure 1).

The Australian Army is therefore considering replacing the term information operations with *information actions*. An emerging Australian Army definition under consideration is:

Actions conducted to influence target audiences in order to achieve understanding, acceptance, and support of our actions and aims, and to diminish the quality and speed of the adversary’s decision making, while maintaining our own, to achieve decision superiority.

Battlespace Operating System

In the Australian Army tactical lexicon, information operations is also referred to as a battlespace operating system (BOS). This is a framework within which a force synchronizes actions across the battlespace. The Army further envisions moving away from the title of ‘IO BOS.’ Accordingly, they are considering a number of titles, including ‘information dominance and influence’ (IDI) BOS. This reflects an Australian Army view that the previously-titled BOS needs to reflect information dominance in terms of effective electromagnetic environment management—resulting in domination of adversary or neutral information and protection of one’s own. Additionally, core influence activities are incorporated into the BOS, extending not only across the information environment, but also the cognitive environment of any target audience.

Core Components of IA

At present, information actions are the integrated employment of a number of core capabilities: deception, psychological operations (PSYOP), electronic warfare (EW), operations security (OPSEC), and computer network operations (CNO). Additionally, IA has a number of supporting capabilities, including physical attack, information security, and some related capabilities—public information and civil-military cooperation (CIMIC). These various capabilities can be employed across three core information actions that align to the broad ABCA working group’s recommendations. The core actions are:

Title	Activity		Actions	Info Actions	Capabilities/Tools
A Military Operation, eg OPERATION ANODE	Offensive	Information Actions	Attack, Advance, Pursue, etc.	1) Influence 2) Counter Command, 3) Command & Info Protection	PSYOP, MILDEC, EW, CNO, CIMIC, PI, MPA, PPP, OPSEC, HUMINT, Targeting, (Example list)
	Defensive		Static, Delaying, Mobile	As above	As above
	Stability		etc.	As above	As above
	Enabling		etc.	As above	As Above

Figure 1. Link between an Operation, Activity, Action, and Capability in Describing Information Actions.

1. Influence: aimed at changing the perceptions and will of target audiences.

2. Counter Command: focused on diminishing the adversary's command and control systems and associated decision making.

3. Information and Command Protection: focused on protecting our own information and command and control and information systems.

Influence actions include employing the supporting capabilities of Military Public Information, PSYOP, deception, CIMIC, plus presence, posture, and profile tasks. However, depending on the results of ongoing analysis, this list may eventually include other tactical capabilities.

Counter command actions include employment of a range of capabilities or tools. OPSEC, EW (specifically electronic attack), and CNO (computer network operations, including attack) are predominantly focused on the physical dimension of information terrain (information systems). Deception and PSYOP focus on the cognitive dimension (decision makers' brains). Yet we may also employ other capabilities enabling physical destruction of enemy commanders, their staffs, and systems. Coalition staffs would draw on the assistance and advice of specialist staff areas such as EW, PSYOP, and kinetic targeting as appropriate. The Australian Army is still analyzing which staff function should have responsibility for Counter Command Activity.

Information and command protection actions include employment of a range of capabilities including information security, EW (via electronic protection), CNO (primarily, computer network defense), OPSEC, counter deception, and counter PSYOP/counter propaganda. While information and command protection actions would most likely draw heavily on the assistance and advice of specialist staffs, indications are that "operations" or the "3" may be the most appropriate responsible staff area. Notably, the ABCA Armies' draft report refers to this activity solely as information protection, though the Australian Army is still examining inclusion of command protection. There is an obvious need to address protection of our own commanders, staffs, and command and control systems against the adversaries' counter command activity.

Furthermore, commanders are increasingly likely to encounter a range of actions intended to impair or diminish the quality of their decision making, and their ability to command effectively. With our increasing IT reliance, modern armies

and commanders will undoubtedly face hostile activity directed towards destroying or impairing automated command and control and information systems.

Defense against such measures is the core information and command protection activity. Physically, commanders, their headquarters, and staffs could be subject to destruction by a range of weapon systems or attacks. Defense against such hostile actions is the realm of OPSEC, as well as defensive force protection and other security measures. Commanders may be the target of deception measures, or PSYOP intended to impair the quality of their decisionmaking. Defense against such measures is achieved through effective intelligence, surveillance, target acquisition, and reconnaissance (ISTAR), enabling accurate situational awareness, understanding, and counter deception measures.

The potential for all service members to be subject to an evolving class of incapacitating or debilitating weapons is also increasing. The following quote advocates the need to "firewall" the minds of commanders, staffs, and systems operators:

We are on the threshold of an era in which these data processors of the human body may be manipulated or debilitated. An entirely new arsenal of weapons, based on devices designed to introduce subliminal messages or to alter the body's psychological or data processing capabilities, might be used to incapacitate individuals.

We are potentially the biggest victims of information warfare, because we have neglected to protect ourselves.

Our obsession with a 'system of systems' is most likely a leading cause of why we neglect the human factor in our information warfare theories. It is time to change our terminology and our conceptual paradigm. Our terminology confuses us, sending us in directions dealing primarily with hardware, software, and communications components. We need to spend more time researching how to protect the *humans* in our data management structures. We cannot sustain anything within those structures if we're debilitated by our adversaries. Right now someone may be designing the means to disrupt the human component of our carefully constructed notion of a system of systems.

There has been significant development in the evolution of mind- altering weapons since the preceding quotes were written. While much more than a doctrinal issue, there is obvious value in placing greater emphasis on protection of

commanders, their staffs, and systems operators. Hence, the Australian Army is considering inclusion of “command” into the core activity of information and command protection.

Information Actions and Intelligence Preparation of the Battlespace

Australian Army planning doctrine includes a chapter on Intelligence Preparation of the Battlespace (IPB). The description places more emphasis on factors that have far wider scope than the traditional domains such as physical terrain, weather, conventional or adversary weapon capabilities, and tactics, techniques, and procedures. These factors include: the electromagnetic spectrum, societal, political, cultural, religious, and economic aspects, with this list not being exhaustive. Past Australian Army doctrine gives limited consideration of information terrain and human terrain; future doctrine will address these areas in more depth.

The information terrain is an increasingly important component of the battlespace. It includes the individuals, organizations, and systems of both friendly and adversary forces that collect, process, or disseminate information—as well as the information itself. It also includes the civilian population and governmental agencies that coordinate international efforts, non-governmental organizations, and the news media. Accordingly, the information terrain and human terrain are interconnected.

Australian Army doctrine regarding information actions needs to address intelligence support, through the IPB, to all core areas of information actions. Given recent operational feedback and associated criticisms of current doctrine, we should place more emphasis on intelligence support to influence, particularly in respect to peace support and counterinsurgency operations. Much greater emphasis could be placed on defining, describing, and understanding the diverse groups and micro populations that may exist in an area of operations and areas of interest. For each segment of the population, as well as the overall population, this would include aspects such as aspirations, motivations, goals, religions, leaders, leadership rivalries and associated factions, alliances, loyalties, obligations, hatreds, daily rituals, historical dates and cultural norms.

Likewise, the Australian Army is considering information actions, its roles, and relationships across the five lines of operation considered within adaptive campaigning:

1. Joint Land Combat - Involves actions to secure the environment, remove organized resistance, and set conditions for the other lines of operation;
2. Population Protection - Provides protection and security to threatened populations in order to set the conditions for the re-establishment of law and order;
3. Public Information - Informs and shapes the perceptions, attitudes, behavior, and understanding of target population groups;
4. Population Support - Establishes/restores or temporarily replaces the necessary essential services in effected communities;



*Commonwealth of Australia
(Univ. of Texas)*

5. Indigenous Capacity Building - Nurtures establishment of civilian governance (local and central), security, police, legal, financial, and administrative systems.

Based on contemporary operational experience, there appears to be a growing recognition that Australia should adopt a broader, more comprehensive, yet more systematic approach to information-related actions. The answer to current difficulties in applying information actions to operations is not to abandon the concept, but to “think outside the box” and improve on it.

In order for this to occur, the Australian Army is currently developing doctrine to meet the needs of the tactical commander. This will further develop concepts discussed in this article, to ensure that information actions broadly align to the Australian joint IO approach, and help the Army implement its components of any or strategic shaping and influencing plan. Additionally, the Australian Army is cognizant of the ABCA Program’s works, and of the need for doctrinal interoperability with other nations.

Development of Australian Army doctrine will enable refinement of information actions and capabilities, by providing guidance to commanders and their staffs on the most effective employment of IA-related capabilities across the IDI BOS. Underpinning this development is that information actions are intrinsically one of the four types of activities: offensive, defensive, stability, and enabling. Accordingly, we must plan information actions in conjunction with all aspects of a military operation, to ensure success and relevance in the future complex operating environment —across all lines of operation.

Defeat or Neutralize Extremists’ Use of the Internet?

How Australia plans to defeat or neutralize extremist use of the Internet raises a number of issues. First and foremost are those actions undertaken by a ‘Whole of Government’

approach: employing strategic, operational, and tactical capabilities that revolve around management and domination of the electromagnetic spectrum. Yet we must examine other issues relating to extremist Internet use: spectrum of interest; scenario generation; countering extremist Internet-based influence actions; risk mitigation; and national policy considerations.

Spectrum of Interest

First, it is important to look further afield than just the extremist group. We must also acknowledge that an extremist group attempts to influence an audience. This may range from a domestic population (with its various sub-groups), where military or stabilization operations are being conducted; to the domestic audience (including political) of the contributing coalition nations. More broadly, we must consider a world audience who may or may not be sympathetic (depending on country, background, and/or culture) to the extremists' cause. The latter audiences will hold ongoing interest in both what is occurring, and what is being released via Internet and other media. This may be due to personal connections to the events as they unfold, a cultural or socio-economic link, or a base level interest centered simply on curiosity.

While adversary use of the Internet will continue and expand, it is how coalition nations discredit adversary themes and messages across the majority of audiences described, that make adversarial Web influence actions redundant. Thus, the remainder of this article examines how adversaries seek to gain influence, versus dominate the electromagnetic spectrum from a technical perspective.

Adversaries look to exploit the broad fringe populations within the spectrum of interest. In simple terms the adversary seeks to: separate and splinter local populations against occupying forces or agencies, or for those groups that are neutral to the adversary and the coalition; or subvert them to provide full support by joining in adversary activities. Subversion could be achieved via the provision of finance, weapons, safe houses, or more simply just not providing information to an occupying force on known or intended adversary activities. Additionally, extremists will target contributing coalition nations' troops and commanders, in an attempt to affect morale and the overall success of the military operation.

Noting the extremists' spectrum of relative interests, it is likely the same spectrum would apply to any coalition conducting IO (Figure 2). In this author's opinion, what makes coalition IO slow to counter extremist Internet use is not an issue of technological superiority, nor lack of ability to respond—but inflexible command structures that do not enable quick and effective counter-computer network ops. This is especially pertinent for audiences in the “friendly but uncommitted,” “neutral,” or “inactive hostile” range of influence.

Scenario Generation

An example of how extremists use information is reflected in the following scenario:

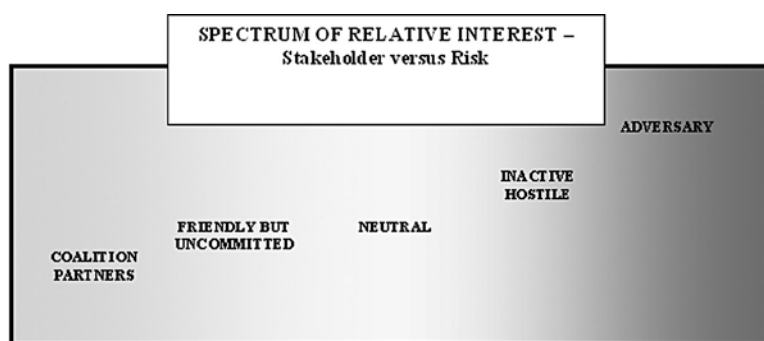


Figure 2. Spectrum of Interest.

- Extremists react to the outcomes of a coalition tactical action by posting either staged, incomplete, or deliberately incorrect website transmissions, to gain maximum effect on one or more groups outlined in the spectrum of interest;
- Coalition reaction (based on the ability to effectively upload accurate combat camera images or other imagery), devises a response at the tactical IO level in the area of operations;
- A coalition response would require operational level approval, from those who vet—and if required—recommend changes to any proposal. Additionally, forces may request further guidance from experts at the military-strategic decision-making level, with the possibility of input from non-military strategic decision-makers and bureaucrats;
- Concurrently (and noting the known delays imposed by command and control), extremists are planning to launch the next information Web activity aimed at influencing those populations within the spectrum of interest. One could interpret that extremists' second and third order Internet influence activities (possibly without a friendly counter-influence activity targeting the first extremist Internet action) are inside the response cycle of a coalition or a single nation;
- Accordingly, extremists can and will continue to force coalition reactions to their Internet activity. In this scenario, extremists identify and target the coalition's critical vulnerability of being unable to implement rapid response to Web-based information actions.

Countering Extremist Internet Based Influence Actions

To counter extremist dominance, in terms of uploading their IO messages and disseminating a message quickly to achieve influence, coalition individuals/groups who conduct tactical level IO need to be empowered. Leaders at brigade level and below must be able to make command decisions about the responses they devise, and to launch rapid counter network-based influence actions.

This in conjunction with robust implementation of a Military Public Information plan that supports and highlights coalition strengths, sending messages to the world's media and domestic populations that compliment coalition Internet actions. Concurrently, PSYOP and CIMIC would look to build on the influence that “neutral” or “inactive hostile” audiences are exposed to via coalition Internet actions.

Risk Mitigation

An associated risk of empowering the tactical IO commander is that the tactical IO message may not exactly mirror the military-strategic IO message. We can mitigate this risk by effective and direct communication between the IO command levels, enabling a detailed understanding of the strategic shaping and influencing (S&I) plan established by a “Whole of Government” approach. Thorough understanding of the S&I plan, in addition to robust comprehension of the operational and tactical IO themes and messages, will assist in risk mitigation and ensure timely and appropriate responses.

While the outcome of the proposed solution enables a quick response, some could still probably view it as reactive. However, it does have a second order effect of making the coalition operational/tactical IO staff less encumbered by time intensive staffing issues—and more empowered by proactive information Internet actions. Once implemented, such actions would force an extremist group to consider an influence response. Accordingly, the extremists’ ability of to get inside the coalition’s Web-based influence decision response cycle starts to erode, forcing the extremists to respond to out influence activities.

While an extremist group may choose not to respond with counter Web-based influence activities, it is at this stage (acknowledging that technical attacks are a separate critical target for extremists), that a coalition starts to achieve Web-based decision superiority. While this approach may not completely negate extremist use of the Internet, combined with technological domination of the electromagnetic spectrum, it will make extremists’ Web-based influence actions more difficult.

National Policy Considerations

Achieving influence “action-decision” superiority across the spectrum of influence enables a coalition to consider implementing more aggressive targeting of extremists. Web-based information deception is but one example. To enable effective information deception, national governments must consider Internet-based rules of engagement that empower the tactical commander to launch information deception against Web-based extremists. While this delicate legal and ethical subject, in terms of how different nations empower their forces, we must acknowledge that extremists operate under no such restraints. They are essentially free to conduct Internet-based influence actions as they desire.

Extremists retain the ability to utilize the Internet for influence activity, knowing that a coalition is only able to conduct counter-actions that adhere to restrictive rules of engagement. Future examination of national policies and procedures (at a military-strategic and political-

strategic level), are needed in order for coalition Web-based influence actions to encounter less operational hindrance. We could continue to hear comments such as “we are failing to win influence and are being defeated by technologically competent extremists in the area of influencing perceptions,” unless there is a unified will to empower coalitions to conduct influence operations free of encumbrances. Such freedom of action still needs to maintain the moral and ethical high ground, and be appropriately balanced. Yet it demands a tactical and operational freedom of action which allows degradation of extremist influence operations on the Internet. Accordingly, national governments need to empower the highest-level military-strategic decision-makers and strategic and operational commanders to authorize responsive, appropriate tactical-level actions.

From a non-technical perspective, preemptive or pro-active dislocation of extremist Internet presence is best achieved by implementing an aggressive IO campaign which saturates the Internet with favorable messages. This should create a situation where extremists, in order to pursue their own IO Internet agenda, are forced to react to an overwhelming coalition Internet influence campaign. Otherwise, extremists have an open time frame within which they can initiate unhindered support for their influence campaign.

Combined with technological domination of the electromagnetic spectrum, reflections presented here are just some of what we need to further explore. In order to combat extremist use of the Internet, we must degrade their ability to dominate influence activities. We must keep them from reaching audiences within the spectrum of interest. ☞



Major James Nicholas, Australian Army, serves as Staff Officer Grade Two Intelligence, Surveillance and Reconnaissance, and IO at the Land Warfare Development Center. Other postings include Platoon Commander, General Engineering Platoon, Logistic Support Force Army College of Technical and Further Education instructor, Faculty Adviser for Logistics Training, and Training Development Officer at the Defense Intelligence Training Center. His Intelligence Corps postings include the Defense Intelligence Organization as Global Security Section Analyst and OIC 35 Security Section, 1st Intelligence Bn. Major Nicholas deployed to the Solomon Islands in 2005. He holds a Masters in Education & Training Development, a BA, and Diplomas in Teaching, Vocational Education, and Training Development.

Canada: Information Operations

By Commander Derek Moss, Canadian Navy

Editorial Abstract: Commander Moss notes that information is as important as forces, space, and time on the operational level. Canada's IO definition has taken out references to "influence an adversary's decision makers" implying that Canada can now message target audiences that are not adversaries. He references Canadian Marshall McLuhan, who famously wrote "the medium is the message." Finally, CDR Moss notes that Canada has developed a increasingly accurate "measures of effectiveness" (MOE) paradigm.

Introduction

Information Operations is often talked about in tones that suggest it is a panacea, created as an alternative to kinetic action. It is often performed by a group of staff officers who are, physically and by job description, removed from operators. Many talk about it, but few understand it. Although not entirely PSYOP or Public Affairs, it coordinates and advises on both topics, and many more. This article defines Canadian IO concepts and direction, and offers recommendations for fighting extremists' use of the Internet.

Definition of Information Operations

Until recently, Canada defined information operations as "actions taken in support of national objectives that influence an adversary's decision-makers by affecting other's information and information systems while exploiting and protecting one's own information and information systems and those of our friends and allies." An information operation is a "military advisory and coordinating function that targets and affects information and information systems, human or technical, of approved parties in order to achieve desired effects, while protecting our own and those of our allies."

Canada has now removed "influence an adversary's decision-makers" from the definition of information operations. While perhaps only a difference in semantics, the implication of this change may be that we can message target audiences that are not our adversaries. The people of Afghanistan spring to mind. An interesting question would be, "does this target audience include the Canadian public?" From my personal perspective the answer would be yes,

even though not formalized in Canadian doctrine. If national opinion is a strategic center of gravity, information operations practitioners had best form relations with the Public Affairs section. Of course this brings to mind the question of whether we are embarking on a slippery slope—though not if all your information is correct, and the Public Affairs Office (PAO) is out front with the message.

With respect to operational art, our opinion is that information now ranks on an equal level with forces, time, and space as the fourth operational factor. It is peculiar because the effects it delivers happen in both the physical and cognitive realms. That particularity has two corollaries: First, only proper targeting and measurement of the effects will allow for a reliable assessment of information activities; Second, the wide range of effects allow for the use of information operations along the full continuum of conflict for both domestic and international operations.

Successful planning, conduct, and execution of operations require that all military and government agencies and organizations involved must cooperate and their activities coordinated. Although the term information operations is defined as a military function, it must be coordinated with other government departments (OGD), or at least be de-conflicted, in order to be successful. Further, information operations "Encompass political, economic, and diplomatic efforts as well as defense and military measures. Coordination among all government departments, under the guidance and direction of the central agencies, is crucial." IO involves the three "Ds" as follows:

Elements of IO

Canada's current IO doctrine is based on original input from 1998,



Three D's of IO. (Author)

revised in 2004. Now Canada is working closely with NATO to update the latter's doctrine and also with the North American Aerospace Defense Command (NORAD) and US Northern Command (NORTHCOM) IO Staffs. A comparison of US and Canadian IO doctrine as it has developed from 1998 through February 2006 (Figure 1), reveals the following:

Canada believes that offensive information operations include actions taken to influence an adversary's decision-makers; and these operations may be done by affecting kinetically or non-kinetically an adversary's use of or access to information and information systems. Defensive information operations, from Canada's perspective, include actions taken to protect one's own information and that of one's friends and allies. Defensive IO ensures friendly decision-makers have timely access to necessary, relevant, and accurate information; and ensures that the friendly decision-making process is protected from all adverse effects, deliberate or accidental.

Electronic Warfare (EW) is defined as actions taken to exploit the electromagnetic (EM) spectrum which encompasses the interception and identification of EM emissions. It includes the employment of EM energy, including directed energy, to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by friendly forces.

Computer network operations include defensive, offensive, and exploitation activities. Computer network attack (CNA) involves actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Computer network defense (CND) involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks. Computer network exploitation (CNE) enables operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Operations Security is the process which gives a military operation appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities, and intentions of friendly forces.

Deception is measures designed to mislead the enemy by manipulation, distortion, or falsification of information, to induce them to react in a manner prejudicial to his interests.

Psychological Operations are planned activities designed to influence attitudes and behaviors, affecting the achievement of political and military objectives.

Civil-Military Cooperation is a military function that supports the commander's mission by establishing and maintaining coordination and cooperation between the military force and civilian actors in the commander's Area of Operations.

Public Affairs is a distinctive function within DND/CF that helps establish and maintain mutual lines of communications, understanding, acceptance, and cooperation between an organization and its audiences.

IO targets include decision-makers, perceptions, information systems, the C4ISR communication infrastructure, software, and data.

Terrorism – the Canadian Context

Canada is facing several terrorist threat elements: religious extremism, with various Sunni Islamic groups being the most serious threat at present; state-sponsored terrorism; secessionist violence, which encompasses Sikh extremism, and separatist movements in Sri Lanka, Turkey, Ireland and the Middle East; and domestic extremism, including some anti-abortion, animal rights, anti-globalization, and environmental groups. Plus there exists a small but receptive audience for militia messages emanating from the United States, white supremacists, and elsewhere.

With the possible exception of the United States, there are more

- Fund-raising and lobbying through front organizations;
- Providing support for terrorist operations in Canada or abroad;
- Procuring weapons and materiel, coercing and manipulating immigrant communities, facilitating transit to and from the United States and other countries, and other illegal activities.

All of these functions are facilitated by the use of the Internet, and remain among the core components of cyber-terrorism.

One of the sponsoring registrars for Hizballah is Register.com located in New York (but with offices in many places). The municipality and province provided hundreds of thousands of dollars in perks to convince it to locate operations in Yarmouth, (southeastern) Canada. And, it has a very specific policy for dealing with cases where someone reports a domain being used for illegal purposes.

"This policy includes reviewing the content to determine the validity of the report and, if applicable, disabling the domain and notifying the customer of the reason for this action," says Wendy Kennedy, the firm's manager of public relations and customer marketing. "At times, Register.com has also reached out to law enforcement to report suspicious activity."

But the servers in Yarmouth are by no means the only ones in Canada where terrorist-related content may be residing. Until a few weeks ago, the website for Al Qaeda in the Islamic Maghreb, one of the most extensive and regularly updated of its kind, was registered to a building near downtown Toronto. The address belongs to Contactprivacy, the anonymous-registration arm of Canadian domain-name provider Tucows Inc. After its Web-hosting service in Germany was alerted to the Maghreb site and pulled the plug earlier this year, Tucows followed suit. But in an environment where similar sites are popping up daily, it was a small victory.

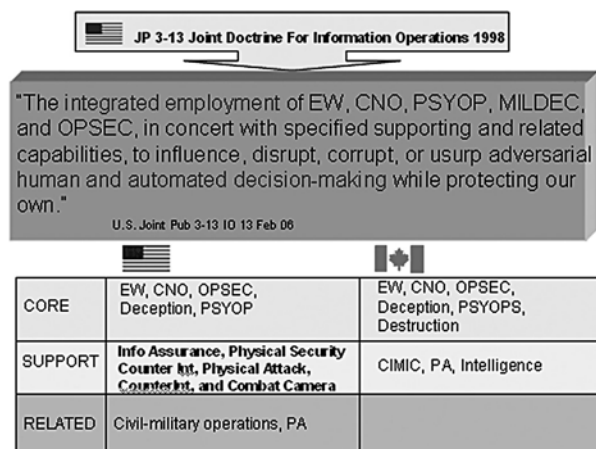


Figure 1. CA & US doctrines compared. (Author)

international terrorist organizations active in Canada than anywhere in the world. This situation can be attributed to Canada's proximity to the United States which currently is the principal target of terrorist groups operating internationally; and to the fact that Canada, a country built upon immigration, represents a microcosm of the world. It is therefore not surprising that the world's extremist elements are represented here, along with peace-loving citizens, as part of Diaspora communities.

Most terrorist activities in Canada are in support of actions elsewhere. In recent years, terrorists from different international terrorist organizations have come to Canada posing as refugees. Other activities include:

Porn versus Terror

Years ago, authorities noticed that child pornography websites, though often operated from outside North America, made use of North American anonymous-registration services. In response, a large number of watchdog groups began hunting down such sites to force the registration firms to shut them down. Wade Deisman, Director of the National Security Working Group near the University of Ottawa, noted in August 2007 that “There’s nothing near that level [of public monitoring] with terrorist websites” and “I haven’t seen anything that comes even close to addressing this issue.” If you shut down a terrorist site, you still can’t arrest its originator. If you keep it going, you can at least monitor the site.

Countering Terrorist Use of the Internet

Terrorist use of the Internet can be countered when a terrorist attack is computer based; is orchestrated by a foreign government, terrorist group, or politically motivated extremists; or is done for purposes of espionage, sabotage, foreign influence, or politically motivated violence. Ward Elcock, Canadian Security Intelligence Service (CSIS) Director to the National Joint Committee of Senior Criminal Justice Officials, noted on 22 November 2001 that “Our role is to determine what is out there so as to provide adequate warning to government and, where appropriate, to law enforcement agencies about threats to the security of Canada, in particular from terrorism. If we lose our ability to do so, then Canadians and our allies will have been ill served.” The threat of attacks on critical information systems and the infrastructures that depend on them will, in the foreseeable future, be almost impossible to eliminate entirely, owing to the fact that attack tools, networks, and network control systems are constantly evolving. As new technologies develop, so too will new attack tools along with the sophistication of the perpetrators who use them.

The Canadian Cyber Incident Response Center (CCIRC) is the national focal point for addressing cyber security issues. A component of the government operations center, it is located under the national emergency response system. CCIRC is the focal point for reporting real or imminent threats and incidents. It includes a threats and vulnerability identification and analysis, early warning dissemination, and incident strategic response and coordination elements.

Protecting Canada’s telecommunications networks is a job too big and too important for any one company or government. Therefore:

- A partnership approach to cyber

security stakeholders such as the telecommunications, financial, energy, and vendor communities and other government departments;

- Collaboration has been established with domestic and international partners such as the Canadian Cyber Incident Response Center (CCIRC), as well as the US and UK Network Security Information Exchanges.

Short-term Solutions

Two agencies, the Royal Canadian Mounted Police (RCMP) and CSIS, are lead counterterrorism elements in Canada. They have access to a wide range of investigative tools and powers

—including physical surveillance, interception of communications (telephone, computer, pager, etc.), and recruitment of human sources or agents who can report on suspects’ activities and intentions. Legislation, ministerial directions, and policy define what can be investigated and which tools can be used under what circumstances. Many powers require prior ministerial and judicial authorization. In addition, both agencies are subject to independent review.

Just because an investigative capability is lawful and available does not mean it will be used automatically. Canadian

intelligence and law enforcement agencies do not have the human and technological resources to target all potential targets all the time. For the most part, they focus on two categories—first, leaders and principal organizers and second, those who represent a serious threat in that they are known to have engaged in terrorist activity in the past or are believed to be planning future terrorist action in Canada or abroad.

Investigations involving targets residing, working, or hiding in Diaspora communities may present serious challenges. Police and intelligence agencies may not possess the requisite linguistic skills, or may be unable to penetrate closely-knit groups using human sources or agents. They may



Dominion of Canada (Wikimedia)

security provides the momentum, speed, and flexibility required to address emergencies and the challenges presented by emerging technologies;

- Industry Canada, as the lead government department for telecommunications, has established the Canadian Telecommunications Cyber Protection Working Group (CTCP) to promote industry-to-industry, government-to-industry, and industry-to-government cooperation in protecting Canadian networks;

- Industry Canada and the CTCP Working Group have established the Canadian Network for Security Information Exchange (CNSIE) to promote collaboration among larger communities of cyber

face resistance to requests for community cooperation, may fail in attempts to recruit new officers from within the community, and may even be unable to find individuals prepared to work as translators. They may be forced to take extraordinary measures to protect the identity of agents or employees who fear for their safety in closely-knit Diaspora communities. Such measures may include:

- Joint investigations involving Canadian and foreign police or intelligence agencies. Terrorist global connections and movements call for global cooperation to track them and prevent them from taking violent actions. CSIS has reported that it has cooperation arrangements with about 230 agencies in about 130 countries, while many foreign police and security agencies have permanent liaison staff in Canada.

- Designation of individuals or entities associated with terrorist activity. Canada did adopt a designation process for terrorists, terrorist groups, or state sponsors of terrorism after 11 September. By October 2003, the Canadian list included 31 organizations—10 each based in the Middle East and Asia, four based in South America, three in Africa, and one in Europe.

- Security screening of applications for refugee or permanent resident status or for Canadian citizenship. If terrorism links surface during background checks, the government may commence deportation action. Additionally, the Canadian Government can expel suspected terrorists under special security provisions of the Immigration Act, and has done so more than a dozen times.

- Screening of people and goods at ports of entry. Transport Canada, Immigration and Citizenship Canada, the Canada Customs and Revenue Agency, and other organizations have enhanced their screening for terrorist connections since 11 September. A new agency, the Canadian Air Transport Security Agency, performs this role at Canadian airports.

Long-term Solution

Canadian security and intelligence agencies seek to build positive counter-

terrorism relationships with some Diaspora leaders and groups in the following ways:

- Consultations and briefings on policy or legislative proposals (for example, those affecting changes in immigration/refugee criteria or charity regulations);

- Membership on advisory boards (the RCMP Commissioner's Multicultural Advisory Committee, for example);

- Community liaison with police officers assigned to specific Diaspora communities to raise awareness, increase confidence, and promote open cooperation with Canadian authorities;

- Direct requests for help and cooperation, usually through community leaders or associations (such as the Canadian Arab Federation) and in connection with specific events (for example, visits to Canada by controversial foreign leaders) or in relation to specific investigations.

Change: Information Operations in Operations

It wouldn't be a Canadian article without a shameless reference to a famous native son. (William Shatner, Mike Myers, John Candy, or any other Hollywood hack will not be quoted.) Instead, the reference here is to Marshall McLuhan (see book jacket), a name endured by many Canadians during painful undergrad classes.

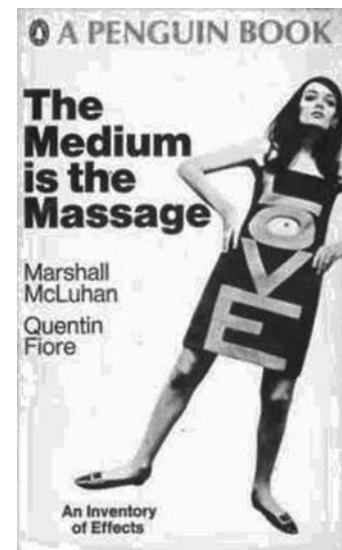
One of McLuhan's lesser known books (pictured), is strangely prescient. Although not prescriptive, the book's thesis, broadly speaking, is that historical changes in communications and craft media change human consciousness, and that modern electronics are bringing humanity full circle to an industrial analogue of tribal mentality, what he termed "the global village." By erasing borders and dissolving information boundaries, electronic telecommunications are fated to render traditional social structures like the nation state and the university irrelevant.

McLuhan's book was written in 1967 yet it has a lasting premise. Shortly we'll discuss how we apply it today. But

first we need to explore an earlier work, *Understanding Media: The Extensions of Man*, source of McLuhan's most famous quote:

In a culture like ours, long accustomed to splitting and dividing all things as a means of control, it is sometimes a bit of a shock to be reminded that, in operational and practical fact, the medium is the message. This is merely to say that the personal and social consequences of any medium—that is, of any extension of ourselves—result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology.

Two examples highlight changes introduced by technology. First, *Rana FM* is a Canadian Forces radio station broadcasting in Afghanistan but located



in Kingston, Ontario (two hours outside of Toronto). The broadcast is recorded on-site and digitally transmitted via satellite. *Rana FM* uses an effective listener feedback capability, the only one in the area of operations. Callers to the station, whether by phone or text message, call a local Afghanistan number and have their message recorded to an in-theatre digital repository. This message is stored and quickly forwarded to Kingston and put on the air, with only a 0.6 second delay. *Rana* has demonstrated its potential to be a giant campaign-winning enabler with its interactive nature since Operation Athena on 6 January 2007. *Rana* can be

heard in Kandahar City, the Kandahar Airfield region, in Sperwan Ghar and, shortly, in Spin Boldak (but spare parts are scarce).

Second, *My Thum* is a cell phone aggregator that also develops applications for automated responses (SMS, voice, or the Internet) to cell calls or Internet contacts. *My Thum* services the radio industry in the Toronto area. It works by accessing all of the local cell phone carriers, and setting up a system that aggregates these carriers with one number (an SMS “short code” which is simply an easily remembered six digit number that callers can recall and dial from any cell system). The short code automatically brings any cell carrier user/customer to an automated response that is either voice or SMS in the case of cell phones (or the Internet if so desired). The caller is guaranteed a response.

Commercially, *My Thum* is used mainly for contests and have great utility for “polling the audience” safely and inexpensively. The automated response can and usually is set to automatically answer and offer an ‘invitation’ to join the station’s ‘club’ to receive early advisories on programs, contests, etc. Because the law in Canada requires users to agree to receive SMS from ‘businesses,’ this automated system invites them to join, thus agreeing to receive whatever messages are sent to them.


Measures of Effectiveness (MOE)

MOE are developed as part of the planning process to determine the effects of IO activities. MOE must link our IO coordinated activities (cause) to the response generated by adversarial capabilities and decision makers.

The initial objectives set the course, but MOE act as the rudder in order to maintain that course.

MOE feedback allows IO planners the ability to revise, create, and delete IO objectives and themes as required, in order to support the commander’s mission. Regardless of its importance, the conduct of a MOE has been largely overlooked. Within Canada, we have developed such a system and have used it successfully in two missions (Operations Halo and Athena). J3 Information Operations leads the MOE effort by developing a combination of quantitative or objective questions and qualitative or subjective questions that are felt to accurately reflect the information needed to establish whether an objective is being met. These questions are then distributed to appropriate stakeholders such as Canada’s Assistant Deputy Minister for Policy, PA, intelligence and those in theatre. Once the answers are received they are compiled by the J3 Information Operations staff and are then assigned a value of “met, partially met, or not met” to each objective. The final product is sent back to the contributing stakeholders to seek agreement on the assessment.

Conclusions

Overall, Canada has a very robust telecommunications industry which, through close collaboration with the government, is able to mitigate many cyber attacks against communication networks. As an example, the recent attacks against Estonia, which caused a significant stir and amounted to not much more than a national five-day inconvenience, would have caused a five minute disruption in Canada. This has nothing to do with advanced technology. In fact, Estonia is one of the most communications-advanced countries in the world. Canadian successes are the result of a vested interest in the telecommunications industry in maintaining a robust system based on redundant technologies and no single points-of-failure. Short-term technological solutions will be an ongoing, iterative process until longer-term social solutions are found. Long-term solutions will not eliminate the problem, but they will make it more manageable. 



Commander Derek Moss underwent indoctrination training at the Naval Officer Training Center in Esquimalt, British Columbia and was subsequently posted to HMCS Terra Nova in Halifax, Nova Scotia. Terra Nova was tasked with several exercises in Europe, goodwill visits in the Great Lakes, and multiple operations off the coast of Haiti. In 1998 he served as Deck Officer on the HMCS Toronto where, as the east coast flagship, he took part in exercises off the coast of Canada, the United States, and the Caribbean. In 2001 Cdr Moss joined HMCS St. John’s, deploying to the North Arabian Sea and Arabian Gulf as Combat Officer and, eventually, Plans Officer for Commander Task Group 54.1. He went ashore to the Canadian Forces Maritime Warfare Center, where he held subsequent appointments as Electronic Warfare and Anti-Air Warfare Tactical Development Officer. Following a very rewarding Executive Officer tour aboard HMCS Winnipeg, CDR Moss was appointed Information Operations section head at Canadian Forces Expeditionary Forces Command Headquarters, in Ottawa. He holds an undergraduate degree in Media Communications from the University of Ottawa, and a Masters in Defense Studies through the Royal Military College of Canada.

Israel: Information Operations Threats And Countermeasures

By Tomer Ben-Ari

Editorial Abstract: Mr. Ben-Ari calls for a more proactive response to cyber threats, in order to win on the new “cyber front.” Proactive steps include controlling the number of terrorist websites and their content, creating a search and download detection engine for suspected terrorist activity, surveilling Internet communications devices, identifying insider help, and concluding international conventions and local legislation. Ben-Ari sees Israel’s vulnerabilities as spam/phishing attacks and terrorist use of webcams. He also explores extremists perceptions of a hundred year war.

Introduction

The use of information operations (IO) by terrorist organizations is here to stay. Conflicts with terror organizations such as Hizballah and Hamas show that with the use of IO, even attacking the civilian population can be achieved easily. As a result, Israel has changed its approach to IO within the last decade. The country’s leadership realizes IO is a real threat that can easily create massive physical and cognitive damage, to civilians and military personnel alike. Several measures have been taken in order to protect critical infrastructure, to include countermeasures. Yet a defensive approach is not enough—we need a proactive approach in order to win a cyber war. The software solutions offered here focus on active counter-methods. Two vulnerabilities serve as immediate threats for Israel to confront: spam and phishing attacks; and the explosion of webcams as a concrete threat.

IO Roadmap of Terror Organizations

Dr. Boaz Ganor, a well-known counterterrorism researcher, defines the potential of terror as the sum of the motivation and operational capability of terror groups. The use of IO directly increases both capabilities and motivation in a significant way, plus at a relatively low cost and minimal risk. The increasing use of IO warfare tools will surely increase the spread and magnitude of terror worldwide, as well as its sophistication and ability to avoid interception. The facts clearly indicate that the use of IO will become more popular in the years to come, due to Western societies’ (followed by developing countries) increasing dependence on computer systems for all operations—in almost every aspect of life. Dr. Ganor claims that Al Qaeda’s global terrorist warfare is one of the most dangerous threats ever mounted against mankind; furthermore, it is more lethal than the threat posed by the Cold War’s nuclear confrontation between America and the Soviet Union. Dr. Ganor points out several characteristics of contemporary terrorism:

- The first characteristic is that Al Qaeda and its affiliates are not bound by any geographical or national restraints. Today al Qaeda and its affiliates are dispersed in many lands, especially

in lawless regions, but also have cells in Western countries. The cyber world has no law, limits, or constraints. Computer systems and networks are interconnected and accessible from anywhere, thus there is no need to physically be present in some geographic area to exploit them. Additionally, there are many security flaws in current systems. It takes a long time to fix them, leaving them vulnerable for some time. Moreover, we don’t know every vulnerability—there are lots of viruses and vulnerabilities found daily. As terrorists use the Web to organize, recruit, and gather intelligence (and exploit information) it will be much more difficult to fight terror groups, find them, or trace their operations. They are able to hide just about anywhere, do all communications over the Web, exploit vulnerabilities, and cause real damage.

- Second, Al Qaeda and its affiliates are interested in employing weapons of mass destruction represents a transition from conventional to non-conventional terrorism. There are cookbooks available on the Web offering “step by step” instructions on how to make bombs and other lethal weapons. By using Web communications it will be easier to interact with researchers that are trying to develop chemical, biological, and nuclear weapons, and are willing to sell their knowledge for extra income. It is relatively easy to influence people anywhere to develop these weapons, and to use them to serve mutual goals of both terror organizations and their collaborators.

- Third, Al Qaeda and its affiliates believe they are waging a “100 years” war, in which they will ultimately prevail, no matter how many years it will take to achieve their objectives. This is a non-rational perception of time. World leaders have a tough time convincing their civilian populations to fight such long wars, yet civilians demand immediate security. This perception of time by terrorists, the strength of terror movements, is opposite and irrational for nation states. Most believe current IO threats such as Distributed Denial of Service (DDOS) attacks, partial damage to government services, communication between service cells, and information gathering are still far less damaging than a 9/11 attack. Nevertheless, terrorist organizations believe that as the Web and computerized solutions develop in the forthcoming years, our lives will become captive to a handful of computers. This will enable them to find weak points in the civil and governmental systems,



Israeli Defense Forces insignia.
(Wikimedia)

and cause massive damage in the long run. Due to the fact that they only need to succeed a few times out of many attempts, it's only a question of time before they will be able to cause significant damage on an ongoing basis.

- Fourth, Al Qaeda's pre-9/11 organizational structure has changed from a structured, hierarchical organization with a decision making process based on command and control principles, into its current flat and cellular organizational structure. After losing much of its infrastructure in Afghanistan as well as the ability to move freely, Al Qaeda began using other Islamic terrorist organizations as proxies to carry out their operations. Spreading the message and recruiting over the Web can prove to be a tremendous unexpected proxy. By using simple cyber recruitment tactics, organizations like Al Qaeda's can easily outsource their operational attacks—even to individuals.

All of these factors indicate that information operations are here to stay. Countries must encourage research and the development of tools to resolve these and future IO threats, to avoid being surprised at the end of the day.

IO in Israel

Cyber threats have been in decision-maker and intelligence forces' crosshairs since computers started playing a major role in our defense forces and day-to-day lives. At first governments didn't see cyber threats as another war zone, but as a way of gathering critical intelligence information on forces, strategies, and facilities. In the past 10-12 years Israel has changed this thought process. Today Israel understands that cyber threats are actually another war front. Cyber attacks will not be directed only at defense forces, but will mainly attempt to interrupt and affect the civilian population. This occurred during the Second Lebanese War [2006], when Israel's adversaries attempted to demoralize the civilian population by aiming thousands of missiles at them. Through their massive exposure to computerized services, civilians will serve as a main front in a future cyber war. Damage to banking systems, traffic control systems, or major news websites (to include taking them hostage) can cause chaos, damage, and fear. In the past 10 years more and more government offices began providing Web services, making these more essential and more common in the public sector. Government and civil sector services are the main factors in our day-to-day lives. Continuing disruptions of critical infrastructure might raise the question "Can this government really defend and secure us?" Governments recognize that disruptions of websites, even if not causing an immediate security crisis, can motivate more and more people to try to hack and cause further problems.

Israel is facing increasing attacks on its computer infrastructure, averaging approximately 20-40 thousand attempted attacks every day, mainly against government websites and services. There is a real fear these may expand to more serious attacks: such as data corruption; data gathering and spying operations; traffic disruption; and the spread of disinformation thru media sites.

During the Second Lebanese War, Hizballah opened a website hosted in Iran. Launched in English, Arabic, and Farsi (and after the war in Hebrew), the site offered reports on the Israeli Defense Force (IDF) and the political situation in Israel. This Web effort was a well planned attempt to influence Israeli public opinion. It also turned out that Israel suffered from critical information leaks. Anyone could easily find movies, pictures, and operational charts that included frequency network channels, soldiers' equipment, and tactical memos.

Classified information from the "Binat Jabel Fight" was also available. Binat Jabel is a village in southern Lebanon which is considered as Hizballah's main area. The Second Lebanese War saw intense fighting there, though the IDF eventually managed to take control of the town—a major turning point in that war. On the other hand, Hizballah had modern equipment on the battlefield including cameras. Photos and movies didn't find their way to the Web in an uncontrolled way. It is believed that rocket strike locations were reported to Hizballah in real-time via the Web, which helped them improve their aim. Further, a huge number of websites were defaced as protests against Israel, to include NASA, Microsoft, University of California at Berkeley, and US Government pages. The hackers used Structured Query Language (SQL) injection techniques to extract



Republic of Israel (Univ. of Texas)

users' names and passwords, then used this access to change website content. In order to motivate supporters, especially the younger generation, Hizballah recently launched a computer game named "Special Forces 2." The game imitates events that actually happened, such as kidnapping soldiers, firing rockets on Israeli towns, and participating in guerrilla battles. Based on recent experiences, Israel changed its attitude toward the IO threat, and established units that will deal with this problem on a daily basis. These new organizations will provide preventive instructions, consulting options, and tools.

Defensive Operations

Israel's definition of IO is similar to Ivan Goldenberg's definition, who claims that information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy an adversary's information,

information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military, political, or business adversaries. This definition is sometimes minimized to the following: "Taking the offensive on the computer services of the enemy while defending one's own computerized services: defending and securing the secrecy of the service while maintaining its availability."

Israel has established the National Data Protection Authority (NPDA) to lead the way in information warfare measures. This authority is responsible for securing government offices and services from possible offensive operations. NPDA leads the research and countermeasures effort against any information warfare danger. The authority is under Israeli Shabak (Israel's internal security service, the equivalent of the US Federal Bureau of Investigation) supervision. In order to better deal with information warfare dangers, the prime minister's office has adapted a data protection doctrine to be applied to all government infrastructures defined as critical. Fundamentals of Israeli protection doctrine are:

- **Information Mapping:** Each office and critical institute would examine and categorize data as sensitive or non-sensitive information, according to two main parameters: classified information and vital information. The latter means information which needs to be kept available and reliable at all times. Each entity receives a risk analysis based on information exposure and use. This includes possible threats, current vulnerabilities, increasing risks, and countermeasures taken;

- **The Human Factor:** Offices must minimize human errors, theft, fraud, or misuse of information. Therefore, each employee should be questioned and checked thoroughly. Connections with outsourcing companies should be reduced to a minimum. Employee training is provided on how to identify and track a social engineering attack;

- **Logic Protection:** Each office will define a management policy for all the computer data systems. Each user will be able to access only the resources that were authorized to him. Password usage is a must. Biometric devices will be combined on some of the systems. Logical monitoring will look for suspicious acts within the system's log;

- **Physical Protection:** Employees must reduce the number of printed documents, limit access to printing rights, and prevent the exposure of classified information to optical or magnetic devices. Secure data transfer between different entities is required. Employees ensure only unclassified data is put on personal computers.

- **Disaster Recovery Planning (DRP):** Preventing disruptions and sabotage to an entity's ongoing work processes, and protecting critical processes from deliberate damage or unexpected failure are absolute necessities. This process will

enable the quick restoration of the system to its former status before a collapse starts. Organizations must maintain status of their systems at all times.

- **Network and Internet Security:** Access to internal data should be limited based on management roles. There will be no direct connection between office data and websites. Office websites will have a secure zone for their computers. Establishing firewalls on all networks, plus consistently checking for Trojan horses, viruses, and other malicious software is required.

Countering Cyber Terror Methods and Recommendations

In order to win on the cyber front, we require proactive steps. In order to prevail in cyberspace, protection of valuable resources is not enough—we need offensive action in order to reduce a terrorist organization's impact.

- The first action to take is to control the number of terrorist websites and terrorist content on the Web. Here, one person can look like a whole army. It is very easy to appear to be a powerful and large organization by opening many websites, then generating content and traffic. Moreover, unlike real life, on the Web people do not die: their message can stay forever.

A combination of DDOS attacks against terrorist websites, plus legislation that prohibits terrorist propaganda on the Web will significantly reduce the amount of terrorist content. We should also consider deliberate actions make some selected sites serve as "honey traps."

- The second action is to create a search and download detection engine. It is possible to know the IP address of the websites one visits, and the files downloaded. If searched information looks suspicious, for example too many searches for maps, plans, and data of the

Empire State Building, then security authorities should check out the person(s) making those queries

- Third is surveillance of Internet communication devices. Emails describing the planned 9/11 attacks were found on Al Qaeda computers. These communications are not limited to email, but extend to other text and voice communication devices such as Skype or MSN Messenger. Detection software searching for suspicious information transfers can detect extremist actions prior to implementation.

- Fourth, one must identify insider help. An employee of a critical organization can help extremists get control of computer systems within an organization. Possible scenarios are opening specific ports or connecting a wireless device to the network. With insider help, extremists can remotely log into the network, access software, and cause damage. A system to gather and analyze all system transactions in an organization can recognize abnormal behavior, which may imply a potential attack.

- The fifth action, probably the basic factor for all of the above counter-solutions, is legislation. Currently there are no



*Western Wall webcam, Jerusalem.
(Window on the Wall)*

strict rules on what is legal or illegal in the cyber arena, thus many loopholes exist. In order to win the battle against cyber terror, we should be prepared to pay a price in personal freedom. What rights are we willing to give up when using the Web in order to ensure security? This question is critical and we should answer. Further, existing rules vary from one country to another. In order to succeed in this war, we must legislate strict rules—and international conventions must be signed.

Immediate Cyber Threats

Many of the terrorist threats that are being discussed today require intensive and sophisticated development. Yet two types of threats can be developed quickly, using off-the-shelf technologies and a relatively small group of people. These immediate concerns are spam/phishing attacks, and webcam exploitation.

- Spam and Phishing can become attractive to terrorist groups, not merely as a tool to spread their messages, but also to raise funds and recruit members. More importantly, spam can be used by terrorists to influence non-members of a terrorist group to carry out attacks that coincide with the terrorists' goals and plans. Such connections allow coordinate among a dispersed, heterogeneously motivated network of activists. Now we commonly assume that some Islamic terrorist organizations will only recruit staunch believers to carry out attacks (especially suicide attacks), but in the future they may use "outsourcing" techniques—and will find the right justification for doing so. The trigger may be lack of resources, or the clear logistical and operational benefits of "outsourced" activities. Worse, it may result in higher quality attacks.

The main features that make spam and phishing attractive to terrorists are:

1. Anonymity and difficulty of tracing;
2. Low cost to reach a large audience, hence the ability to engage in a large number of initiatives;
3. Leverage in reaching new and otherwise inaccessible audiences;
4. Ability to recruit operatives from within the society under attack;
5. Ability to spread fear, even without any action being taken.

After detecting and communicating with possible carriers, their communications can be moved to more secure systems.

- Webcams for Surveillance and Information Gathering: These days there are many cameras on the Web. These are very simple and cheap to install; some are wireless and others

satellite-based, and all are reasonably priced. Some webcams are private, showing entertainment places, malls, and private homes, while others are government-based, showing tourist places, traffic junctions, and streets. Webcam host sites can also serve as a webcam search engine. Combined with software products such as *Google Maps* and *Microsoft Live Maps* that use cameras combined with static photos, we can view every street corner. In the future, as network pipes become wider and network traffic faster, we will have live scenes on those same street corners. By exploiting these webcams, terror organizations can acquire intelligence on specific targets without stepping foot on them. Moreover, video information can be analyzed by computer vision algorithms. Based on technology available today, it's not difficult to access a specific webcam and analyze its data stream. For instance, how many people cross a specific street each day and at what times, or how many police cars pass? Such software would create reliable, long-term, well-analyzed information about happenings in many different places. Extremists could separately and easily monitor multiple locations, without putting their spies at risk.

Conclusion

Israel believes that IO will become an essential weapon in the future in any war or actions against terrorists. Since it will become easier to hit Western society using IO methods, Israel must be prepared to take offensive methods and measures. Resources should be invested in finding vulnerabilities and fixing them. Catching terror groups before their actual mission and detecting IO attacks prior to the point where massive damage is done is the goal of offensive actions. Legislation and worldwide cooperation should be enhanced as well in order to generate effective solutions. ☹



Tomer Ben-Ari has mainly focused on IO and cyber issues since 2003. His research is focused on helping decision-makers deal with possible threats and providing countermeasures as well. He has designed and developed a large range of software products mainly in the data management area for the following companies/institutions: IDF, Intel, GDH and currently Top Image systems (TISA). He is adept at pointing out possible threats from terrorist groups in cyberspace. He combined his research with Israel's International Disciplinary Center's International Institute for Counterterrorism. Together with Dr. Boaz Ganor and Dr. Ron Rymon, Mr. Ben-Ari published papers at conferences, including "The Security and Privacy in Information Society" held in Germany in 2005 and "The Advanced Program of the Information Management Association" in 2007 in Canada. A recognized international speaker, he has provided council to different governments. From 2001 he has served as a software engineer and system architect for many software systems for the Israeli army and the private sector. He holds a BA and an MS in computer science from the Inter Disciplinary Center, Hertzliya, Israel.

Information Operations In Senegal

By Antoine Wardini, Colonel, Senegalese Army

Editorial Abstract: Colonel Wardini notes information technology is slowly making inroads in Senegal. As a result, IO efforts focus on support to public affairs, civil-military operations, and defense support to public diplomacy. Psychological operations and winning hearts and minds are implied in such an approach. Of special interest to the US is that China has announced its intention to finance the final steps of setting up Senegal's government Intranet.

Introduction

Information is a strategic resource, vital to national security. Military operations depend on information and information systems for many simultaneous and integrated activities. Since the 1960s, there have been extraordinary improvements in the technical means of transmission, protection, collection, storage, and analysis of data, which have allowed significant improvements in the exploitation of the information domain.

Information Operations is an evolving discipline within the military. It has emerged from earlier concepts originating in the 1990s and takes into account lessons learned from the Gulf War(s), phenomena such as the so-called "CNN Effect," and the enormous advances in information technology. Today Germany leads a NATO multinational effort on developing information operations as an integrating function/joint mission area within the military, called the "Multinational Information Operations Experiment" (MNIOE).

This concept of information operations is somewhat new to most military experts. However, it is accepted worldwide that the instantaneous capability of transmitting information today is a serious issue for all, and that a "hot talking image" is worth 10,000 words.

Information operations are defined as "the integrated employment 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." In other words, information operations can be defined as actions taken to affect adversary information and information systems while defending one's own.

The purpose of this doctrine is to provide joint force commanders (JFC) and their staffs guidance to help prepare,

the commander's intent, and project accurate information to achieve desired effects. Ultimately, these should result in differing behaviors or changes in the adversary's decision cycle, which aligns with the commander's objectives.

Military capabilities of Influence Operations consist of:

- Psychological operations (PSYOP)
- Military deception (MILDEC)
- Operations security (OPSEC)
- Counterintelligence (CI) operations
- Counterpropaganda operations
- Public affairs (PA) operations

Context

With an approximately 90% Muslim population, Senegal is—and still remains—a secular country, as mentioned in the constitution and enjoyed by its inhabitants. Senegal has never undergone a military putsch (coup d'état), and besides the well-controlled rebellion in the south, has never been threatened by any kind of external instability. This sign of stability is unique in our sub-region where the countries bordering Senegal have experienced, at least one time, a putsch. Senegal belongs to the Saharan region, a remote desert-like area, targeted by Islamic extremists as a potential sanctuary for future activities.

Social Aspect

We can define Senegal's known threats as poverty, drought, disease, political issues, growing Islamic movements, drugs, and refugees. All are internal problems the government has to deal with as first priorities. In other words, today's enemy is no longer the conventional army right next door; well organized and structured, fighting



*Senegalese Forces symbol.
(Ministry of Armed Forces Senegal)*

plan, execute, and address information operations in support of joint operations. The principal goal is to achieve and maintain information superiority over the enemy.

In order to tackle our topic progressively, one must understand the military capabilities of Influence Operations. They focus on affecting the perceptions and behavior of leaders, groups, or entire populations. Influence operations employ capabilities that protect operations, communicate

for a national cause with all its assets supported by a national engagement. Rather, it is mainly a politically-frustrated opposition, concerned about the way the country is led, that tries to change the leadership for a new start. Such groups hope things can move in a better direction for the benefit of the population, and power for themselves..

In such conditions the national armed forces in sub-Saharan and Central Africa (poorly equipped and lacking resources) are used to fight subversive, wrongdoers, and insurgents, taking armies away from their constitutional missions for a majority of the time. These low intensity conflicts (LIC) fought between armed citizens and national armed forces are equated to peace restorations, in which appropriate force is recommended over excessive force in order to keep the crisis under national control and avoid any internationalization.

In this context, Senegal's priorities are not EW, CNO, OPSEC, PSYOP or MILDEC, but trying to win hearts and minds (domestically)—to kill rumors and restore confidence for a new beginning. The primary objective is peace and reconciliation, followed by consolidation of the peace and national reconstruction.

Cultural Aspect

Throughout this long process, the main actors are internal, as are the issues. Accordingly, we undertake diplomatic action with allies and neighboring countries, to help solve the crisis before it pours over to the sub region and ends up as a source of instability on the continent. The African Union's leadership is also highly committed to crisis resolution through dialogue and talks, which reminds one of Africa's deep rooted oral tradition of searching for peace, stability, and prosperity.

Senegal's Definition and Understanding of IO

Since its independence in 1960, Senegal has chosen to exercise its defense through recognition of economic realities and solidarity with neighboring countries, in order to fully carry out its assigned missions. Senegal, land of the famous



*Senegalese and US leaders discuss West African security.
(Defense Link)*

“Tirailleurs Sénégalais,” is a peaceful nation, highly committed to justice and democracy. These values serve as the basis of its current stability.

Senegal believes the definition of IO implies a high degree of technologically-oriented components that are not available in most developing countries. In such states, passive measures like 3rd generation equipment and oral procedures are still the armed forces' only available tools to collect and transmit information in the field.

In Senegal, the different functions listed in the definition of IO are not yet integrated. In fact, they are supporting each other, but as a whole do not belong to a specific cell.

Senegal's armed forces understand information operations as the employment of all means to negatively influence adversary decision-making, while protecting friendly forces decision-making. However, apart from passive measures under the management of the Signal Directorate, and classic intelligence collection and transmission procedures, Senegal presently focuses on three military functions specified as related capabilities for information operations. These capabilities are: public affairs (PA); civil-military operations (CMO); and defense support to public diplomacy. All of these make significant contributions to the successful execution of Senegal's military missions. Thus, one can see how and why Senegal's definition of information operations

is very specific, as well as how it uses the above mentioned functions when deployed. These IO-related capabilities form the bulk of our “Army Nation” concept, which is essentially oriented towards promoting Senegal's image by “winning hearts and minds.”

In fact, public affairs operations play a major role in Senegal's line of defense against adversary propaganda and disinformation. PA is essential, and credible public affairs operations are necessary to support the commander's mission. Senegal's Military Department of Communication (DIRPA) understands this very well, which is why informing domestic and international audiences is considered crucial when hunting for support. The military conducts such activities in coordination with information operations liaisons. While intents differ, PA and information operations ultimately support the dissemination of information, themes, and messages adapted to their audiences. For instance, PA contributes to the achievement of military objectives, by countering adversary misinformation and disinformation through the publication of accurate information. DIRPA does this very efficiently. PA also assists OPSEC by ensuring that the media are aware of the implications of premature release of information. In this domain, the armed forces have established credible relationships with the media that profit each party (press releases, statements, briefings, exchange of trainees, seminars,

organizing facilities). Media are sometimes invited to the front lines to cover military operations, through “embedding” ground rules established by the designated PA staff. In liaison with the ground commander’s staff, DIRPA provides ways to get friendly messages to the target audience.

In the civil military operations (CMO) field, the armed forces help to improve the welfare of the population by taking part in the country’s social and economic development. Accordingly, commanders conduct CMO to address the root causes of instability, to assist in reconstruction after a conflict or disaster, and to conduct other military operations independently—but in support of—national security objectives. CMO, by their nature, affect public perceptions in their immediate vicinity. Distribution of information about CMO efforts through PA and PSYOP can affect the perceptions of a broader audience, and favorably influence key groups or individuals. That is why we exercise our heartfelt concept of ‘Army-Nation,’ meant to assess the participation of the Senegalese armed forces in the country’s development, with 100% involvement in the following functions:

- The national integration function, exercised through military enrollment/conscription, a major factor in national cohesion assisted by the establishment of a civic (national) service more accessible for our youth;
- The economic function, reflecting countless Engineer Corps actions (the construction of bridges, ferries, wells, etc.), along with the involvement of the Air Force (MedEvac, transport of VIPs) and the Navy (marine resources protection);
- The social function which is the sole responsibility of the Health Directorate and is the backbone of public health.

The Senegalese armed forces, as a whole, take part in youth activities (sports and other activities), and play a very important role in the contingency rescue plan, known as Plan ORSEC (Rescue Operations Plan). The military health benefit institution, known as “Mutuelle des Forces Armées,” is mainly concerned with setting up prevention

and solidarity mechanisms that benefit military members and their families.

Our Military Building Cooperative (known as COMICO) is fully oriented towards helping its members become home owners in nice and safe neighborhoods. To better portray the leadership’s concern for the soldier’s welfare, two other major social structures started business in 2006:

- The Injured Military Reinsertion Agency aims to find ways to assist retirees and departing military personnel with their transition into civilian life;
- The Invalids Foundation supports the handicapped and their families.

As far as defense support to public



*Principle cities of Senegal.
(CIA World Factbook)*

diplomacy is concerned, our military contributes to peacekeeping and helps to enforce stability on the African continent and around the world. These actions are in line with our signed alliances, treaties, and international agreements, and our concept of Peace Defense. This commitment is not in vain; Senegal has a long series of humanitarian interventions that traces the history of our armed forces.

These efficient humanitarian interventions come under the aegis of the United Nations, the Economic Community of West African States (ECOWAS), the former Organization of African Unity (now the African Union), and so on. These organizations have honored our armed forces with worldwide recognition for their dedication towards peace and justice. As a matter of fact, our

forces deployed regularly in support of, or parallel to our diplomacy, playing an important role in peacekeeping around the world. In carrying out these noble missions they have given their best, to include the ultimate sacrifice, and always in solidarity with the conflict-stricken countries.

Our achievements during our 47 years of peacekeeping-engagements are highly appreciated by the international community. The sheer number of activities speaks for itself. For this successful cooperative work, Senegal’s Armed Forces were awarded the 2007 African Integration Trophy.

Senegal’s Views for Countering Extremist Use of the Internet

Our country has no precise or objective definition of what constitutes extremism on the Internet. For most people, the term refers to the propagation of extreme views, usually of a political, social, or religious nature through the World Wide Web.

The cheap Internet medium provides easy access to a lot of information and entertainment, every moment of every day. Some terrorist groups use it as a part of their decentralized and internationalized command and control structure. In this highly sophisticated domain, Senegal has a lot to learn and a long way to go. Our armed forces do not have the technology to hunt, track, or counter extremist views on the Internet. Thus, Senegal currently uses no active measures against this threat. The ‘if you see it report it’ recommendation is our only available warning system so far. However, our hierarchy is planning to train some officers in advanced software, to counter intrusion and theft by subversives or wrongdoers.

In addition, Senegal’s American allies are setting up the “ECOWAS Regional INFORMATION Exchange System” (ERIES) throughout the African continent to provide information tracking and sharing among friendly nations. The 2006 exercise Africa Endeavor took place in Pretoria, Republic of South Africa, as a major US-sponsored event focusing on the ability of coalition communication systems to work together.

Other regular computer-assisted exercises in Senegal are part of the “Trans Saharan Counter Terrorism Partnership” (TSCTP), which aims to build partnerships and strengthen the abilities of African governments and militaries. The hope is that such activities will make these nations less vulnerable to terrorist recruiting efforts, and help catch those already using the Web as a safe haven.

Last but not least, the creation of the US Africa Command (AFRICOM) will “strengthen security cooperation between Africa and the USA,” thus creating new opportunities to bolster the capabilities of the African leadership. Senegal’s armed forces look forward to such opportunities in this new era of information operations.

At the political level, some believe that Senegalese Public Telecommunication Regulatory Agency (ARTP) countermeasures currently underway are likely to be reinforced in the near future—with dedicated partners. For example, the People’s Republic of China has recently announced its engagement to fund the final steps of setting up Senegal’s government Intranet.

Some Recommendations for Countering Net Extremism


The challenge of Internet extremism urges the establishment of a global network of like-minded individuals, organizations, and opinion-leaders, to promote moderate and progressive ideas throughout the world. Some of Senegal’s ideas on how to meet this challenge include:

- Reinforcement of laws against the distribution of extremist material;
- Updating of Web legislation;
- Actions against relevant Internet service providers, who once identified, should close down extremist sites or face potential prosecution;
- Parental and teacher use of filtering software to block access to sites with particular ratings;
- Promotion of sites containing counter-extremist material, and those promoting tolerance and multiculturalism;
- Building alternative viewpoint Web sites and networks;
- Building networks to isolate and marginalize extremists and their supporters, galvanize the revulsion of the murder of innocents, and empower legitimate alternatives to extremism.

Internet users tend to reinforce their existing perspectives; therefore we must thoughtfully construct counter-extremism websites, to track the very same people who would be lured by radical ideologies.

An IO Topic of Importance

Senegal’s IO experts believe PSYOP is a very important asset for a commander’s successful mission accomplishment. There is no doubt that PSYOP has a central role in the achievement of information operations objectives in support of the JFC in Senegal. However, in order to maintain credibility with their respective audience—which is the purpose of the information operations cell—we recommend facilitating close cooperation and coordination between PSYOP and PA staffs.

Questions Senegal must further explore: Is PSYOP useful or necessary in the African environment? If yes, what is the best way to make it efficient in Senegal (or Africa), considering the lack of sophisticated and technologically-oriented components? What is the best way to counter PSYOP in Africa? Does PSYOP apply to low intensity conflicts like civil wars or rebellions in Africa? We look forward to searching for these answers. 



Colonel Antonine Wardini is an active duty officer in the Senegalese Army and presently is the military zone commander of Dakar, the capital city. He had served as the Director of Information and Public Relations for the Senegalese armed forces and acting spokesman for the military until 15 June 2007. Colonel Wardini served as infantry battalion commander, Chief G3 OPS, Chef de Cabinet of the General Chairman of the Joint Chiefs of Staff of the Senegalese armed forces, and press officer in his home country. He was deployed as a UN staff officer in the war-torn Democratic Republic of the Congo from April 2003 to May 2004. In November 2005, Colonel Wardini attended the “Media Course” in KAIPTC and later was invited in April 2006 to take part in the UN Chiefs Public Information Meeting, co-sponsored by DPKO/DPI in New York. Colonel Wardini has valuable expertise in field crisis management. He took part in two humanitarian US-sponsored exercises (Flintlock in Mali and ACRI in Thiès, Senegal). He is fluent in French and English and has experience in dealing with the media, both national and international.

Argentina: The Challenge Of Information Operations

By Dr. Javier Ulises Ortiz

Dr. Ortiz discusses several policies and strategies for protecting Argentinean and coalition critical infrastructure. He describes the functions of the Armed Forces Scientific and Technical Research Infrastructure Institute, a joint military organization that possesses an information security laboratory. He further explores the Argentine Defense Forces' creation of "computer science troops" in its Communications and Computing Systems Command.

Introduction

Ten years have passed since US military systems were cybernetically-electronically attacked by means of a computer network from an unknown country—an event known as “Solar Dawn.” The 9/11 attacks and other events, like the massive blackouts in big urban settings, demonstrate that unlimited security in a complex world is impossible.

Cyberspace is the new “Athena’s Camp” in today’s conflicts, especially “asymmetrical” ones. In developed countries the concepts of information warfare (IW) and information operations (IO) have appeared as new military doctrines.

According to sociologist Manuel Castells, 9/11 was the beginning of the first world war of the 21st century, the “net war” initiated by weak forces attempting to “impose their objectives by using the only efficient weapon in its technological and military inferiority situation.” In May 2007, the Estonian computing system was attacked by half a million computers, via the Internet. Estonia was paralyzed for weeks and needed NATO’s help to recover. NATO spokesman James Appathurai noted “the XXI century is not one of tanks and artillery.” He further summarized a June 2007 NATO chiefs meeting saying “everybody agreed that it is indispensable to improve the protection capability of the computing systems of critical importance.”

As an answer to these attacks, a new concept in defense and security matters appeared: the Protection of Critical Information Infrastructure

(PCII). It is necessary to identify and secure the CII to avoid new “Mutual Assured Destruction” vulnerabilities in this new age. Cooperative agendas for regional and defense security issues must incorporate CII-related definitions, so that member countries develop their own concepts. Telecommunications (optical fiber, digitalization, computing) represent the technological infrastructure of globalization, making strategic decision-making in real time possible on a global scale.



*Argentine national flag.
(Wikimedia)*

Nations can take on elements of new forms like the “Digital State” or “Net-State,” and a nation’s sovereign territory then undergoes change in leaders’ minds. Whether by attack or by accident (such as a blackout in a megalopolis), the risks associated with not having preventative systems, early warning, and fast answers based on emergency plans, can be devastating.

The main objective of these new types of conflict is the destruction or disability of information capabilities and critical infrastructures. This understanding of war as “not only military” has been developed in different parts of the world. Different documents in the USA, Europe, and other countries

start to define the issue and to generate doctrine for action. Information space and “physical” critical infrastructures are strategically linked. Thus, network warfare is more about organizational doctrine than technology.

The following US definitions are used in this article:

- Critical Infrastructure: systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

- Information Operations (IO): Joint Doctrine’s first IO definition in 1998 was changed in 2003 (the definition of Information Warfare was removed completely, leaving only the definition of Information Operations). The February 2006 doctrine says IO shall: “... integrate the employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operation security (OPSEC) in concert with specified supporting and related capabilities to influence, disrupt, corrupt, and usurp adversarial human and automated decision-making while protecting our own.” IO doctrine is in constant evolution, as shown by the February 2007 US Army update which “uses the joint definition of IO as well as all capabilities that compose IO; however, Army doctrine categorizes IO capabilities in themes of five IO tasks: information engagement, C2 warfare, MILDEC, OPSEC, information protection.”

Latin America had its first important computer security-related challenge in 1999, when facing the Y2K problem. Recently, new definitions related to military information technologies started to appear in many Latin American countries. Many nations are updating definitions and doctrines. This article includes: strategic perspectives for analyzing IO issues; the development of hemispheric strategies for the PCII and cyber security; Argentinean recommendations for countering extremist views on the Internet; the Argentine military doctrine related to IO; the Argentine military and other Latin American countries understanding of IO; and conclusions.

A Strategic View for Analyzing the Issue

In a changing world, conflicts become highly complex. Our concept of conflict, defined along a line from declared wars to undeclared wars, becomes more diffuse between these limits. Presently, we see continuous changes in regional military strategies, doctrines, capabilities, organizations, land operations, and procedures. Hence, it is more efficient to analyze Argentina's doctrine by including elements of NATO's IO doctrine. Yet, even NATO still does not define cyber attacks as military attacks. These wars of probable "zero casualties" can be analyzed from different perspectives, all of which include the impact of information technologies—and the potential devastating consequences. It is important to analyze different doctrinal models based on "real," and not "potential" capabilities.

Hence, it is necessary to analyze laws, policies, and national and regional strategies. Only then can one understand that information age conflicts are global, that military forces and doctrine are part of a nation's public sector, and that together with the private sector they constitute the critical and information infrastructure facing the cyberspace threat. We must consider all these elements, but even more explicitly in countries where the technological gap

is wider, and the infrastructure is more vulnerable.

Hemispheric Strategies for Protection of Critical Information Infrastructures & CyberSecurity

During the last five years, Organization of American States (OAS) member countries signed agreements forming the basis for PCII and cyber security, as follows:

1. Civil and civil-military cooperation in the fields of Defense and Security is necessary, according to the five Ministers of Defense of the Americas Conference (Santiago de Chile, November 2002). They noted "The Hemisphere faces an increasingly diverse and complex set of threats and challenges for its states, societies, and people," and that "each American state is free to choose its own defense instruments including the mission, personnel, and the composition of Defense and Security Forces needed to guarantee sovereignty, in accordance with UN and OAS Charters." There is also a "particular strategic context of each sub-region in the Hemisphere."

2. The Defense "White Book:" (Officially the *Adoption of the Guidelines on Developing National Defense Policy and Doctrine Book*.) This is a key policy document providing the government's vision for defense of the OAS (2002).

3. The OAS's "Declaration on Security in the Americas" (October 28, 2003: This agreement notes the new concept of security in the Hemisphere is multidimensional in scope, and includes traditional and new threats, concerns, plus other challenges to member states, incorporating the priorities of each state. Traditional threats, new threats, national concerns, and other diverse challenges affect member states in different ways. New threats include attacks on cyber security, and "new terrorist threats—whatever their origin or motivation—such as threats to cyber security, biological terrorism, and critical infrastructure.

4. An Inter-American strategy to combat threats to cyber security: Together with Argentina, Canada,

and Chile, the US OAS delegation presented this document May 19, 2003. This important strategy is key to the development and consideration of a common vision of critical infrastructures for all the Americas. The document notes "A multidimensional and multidisciplinary approach to create a culture of cyber security" must be developed in order to protect the infrastructure of telecommunications. It gives responsibilities to:

- The Inter-American Committee against Terrorism (CICTE): The formation of an Inter-American Alert, Watch, and Warning Network is needed to rapidly disseminate cyber security information and respond to crises. Creation of a Hemispheric network to support Computer Security Incident Response Teams (CSIRTs) is also required.

- The Inter-American Telecommunications Commission (CITEL) was formed to identify and adopt secure Internet architecture technical standards, in 2004.

5. Protect Critical Information Infrastructures (PCII): International cooperation is the key to protection of essential information infrastructure, coordination of early alert systems, analysis of vulnerability, threats, and incidents—with regard to information and to coordinate investigations of attacks against said infrastructures according to national legislation. This information can be found in the *Blue Book: Telecommunications Policies for the Americas* (2005).

6. Hemispheric Definition of Critical Infrastructure (CI): This "refers, among others, to those facilities, systems, and networks, and physical or virtual IT services and equipment, the disabling or destruction of which would have a severe impact on populations, public health, security, economic activity, the environment, democratic governance, or the ability of the government of a member state to operate effectively." This important document is key to consideration of a CI common vision in the Americas. OAS, (March 1, 2007).

Argentina's Recommendations for Countering Extremist Views on the Internet

Argentina created a national system to face these challenges:

1. The Information Technologies National Office (ONTI) is part of the Ministries Office Chief. ONTI is responsible for creating technological development and innovation policies, in order to transform and modernize the state. On August 3, 2005, ONTI approved the "National Public Sector Information Security Policy" for the development of Information Security Policies in each public area (regulation ISO/CEI 17799).

2. Argentina's Computer Emergency Response Team (ArCERT). ArCERT started operations in May 1999 under ONTI. Main roles are:

- Centralize security incident reports that take place in the Federal Administration, and facilitate information exchanges in response.
- Provide a specialized advisory service for network security.
- Enhance the coordination among federal organizations to anticipate, detect, handle, and recover information from security incidents.
- Act as a repository of information for security incidents, tools, and defense technologies.

ONTI and ArCERT define the following concepts:

- Information: every communication or representation of data or knowledge, in any form (text, numeric, graphic, cartographic, orthographic, or audiovisual) and by any media (magnetic, paper, PC, audiovisual, or other).
- Information systems: independent sets of information resources organized to summarize information's processing, maintenance, transmission, and distribution by different processes (manual or automatic).
- Security Incident: a negative event in a PC system, or PC net, that compromises the confidentiality, integrity, and availability of information. It can be caused through vulnerabilities or attempts/threats of breaking into an information security infrastructure.

• Threats to Information Security: actions against the confidentiality, integrity, and availability of information. These threats can be caused by human error, attacks, or catastrophic accidents.

3. The Homeland Security System has the following additional offices with responsibilities for the security of the information infrastructure.

• The Federal Police Division for Technological Crimes cooperates with Justice's investigations on criminal issues.

• In the National Defense System, the Armed Forces Scientific and Technical Research Infrastructure Institute (CITEFA) is the only joint military organization dedicated to scientific and technological activities allowed to conduct research and development to meet Argentina's National Defense requirements.

• The Information Security Research & Development (SI6) Office is CITEFA's Lab. It was officially created in January 2004 to develop information security R&D activities for both general and defense areas. SI6 belongs to the Information Security Division of the IT Department. Actually, SI6 is working on intruder detection, intruder classification, intruder identification, honeypots, pattern analysis, biometric authentication, virtual private networks, firewalls, digital signatures, penetration tests, and other issues. SI6's mission is the generation of information security knowledge through research & development activities. The SI6 Lab considers the sum of community efforts in applied research, using innovative technologies as one of the most efficient ways to build technological knowledge. SI6's working projects include: "Paranoid: Intruder Identification System using Honeypot Techniques;" "BioVpn: An Open-source Biometric Authentication Process for VPN;" and "Cisilia: A Windows NT/2000/XP Password Cracking Distributed Application for Linux Platforms Using Open Mosix Clusters."

Argentina's Military Doctrine Related to IO

Before analyzing the definition of IO it is necessary to look at background



Argentine provinces.
(Wikimedia)

information on Argentina's Structure for National Defense:

1. The National Defense System. Law N° 23.554 de 1988 defines National Defense as the integration and coordination of all forces of the Nation for the solution of conflicts that require the use of the Armed Forces, in a dissuasive or effective way to counter external aggression. Its scope is to permanently guarantee the sovereignty and independence of Argentina, to protect its territorial integrity and self determination, and to protect the life and freedom of its inhabitants.

The Armed Forces primary responsibility is to defend the country against military aggression from other states and protect the nation's sovereignty and territorial integrity. Homeland Security Law N° 24.059 establishes that police and security forces must be used in case of criminal actions, while the Armed Forces can, only in special cases upon request from Homeland Security Officials, confront threats of a non-military nature.

In 1998, the Defense Ministry published the *White Book for National Defense* in which it analyzed "the

Revolution of Military Affairs” (RMA). The RMA changed the quantitative criteria for “soft power.” This concept has three axes: space military information, soft power’s use in processing elements (in systems C3I2), and soft power’s use in precision weaponry. The White Book also underscores a new danger: the threat to Argentina’s own computer systems. A 2001 update to this book includes a strategic view of the RMA (with IT) and how this changed the “art of war.” This required changes in military doctrines, in weapon systems, and in the logistical and organizational structures. This document further established the need to integrate C4I2 and electronic warfare systems at the national, military, and operational-strategic levels; and included the satellite systems applicable to Defense.

Decree N° 727/06 strengthened the role of the Joint Military Staff (EMCO) as the main military strategic decision-maker under the civil government.

The mission of Chief VI - C3I2 - EMCO (Command, Control, Communications, Intelligence, and Interoperability) is to develop and control the policies, plans, programs, and projects of the C3I2 joint and combined staffs, and to provide a Joint Military Doctrine for Communications and Electronic Warfare. Each of the Argentine armed forces has similar areas. The Argentine Army has the Communications and Computing Systems Command, staffed by specially trained personnel, to include “Computer Science Troops” and officers with advanced Computer Science degrees.

2. Military doctrine related to IO. In Argentina, military doctrine is the systematic organization of principles, definitions, regulations, and procedures that constitute military knowledge—and offer satisfactory answers to military problems. Doctrine is the basic and active element in force design, including Joint Military Doctrine, Naval Military Doctrine, Air Force Military Doctrine, and Army Military Doctrine. These regulate the services’ actions to fulfill their missions as military components, and fundamental institutions of the nation. In 2007, Argentina adopted a

Defensive Strategic Operational Attitude by means of a deterrence policy derived from the Argentine Army Chief of the General Staff’s “Argentine Army 2025” vision. This plan takes into account the peace and cooperation zone created by the Southern Common Market (MERCOSUR), including the Regional Trade Agreement (RTA).

The Regulation for the Conduct of the Land Military Component establishes that secure communications are the essence of C2 so that the commander can influence operations effectively. Many IO elements are incorporated in Argentina’s military doctrine. As many Argentine military authors note, the diverse elements that constitute IO are defined by Argentina’s army military doctrine. The *Dictionary of the Argentine Army* defines operations linked with IO as follows:

Military Operations: military activities for situations when facing a real enemy. This includes employment and direction of dependent elements, to execute mission needs;

Electronic Operations: complementary operations conducted through the use of communications and special communications electronic media, in order to support other operations throughout the electromagnetic spectrum for their benefit while restricting or avoiding its use by the enemy;

Special Operations: operations different from others, either because they have particular procedures, organizations, or media, or because there is a need for specially trained forces. Special operations can be executed through conventional or non-conventional means;

Non-Conventional Operations: those executed on enemy territory or on friendly territory occupied by the enemy, and within the scope of attaining designated objectives;

Complementary Operations (military deception): multiple, synchronized actions to hide from the enemy the true intentions of one’s own forces.

Peacekeeping Operations: operations to support diplomatic efforts of international organizations to maintain,

restore, and/or enforce peace in a conflict zone.

Psychological Operations: those operations that use psychological actions in a planned way to influence the behavior and attitudes of selected individuals or groups, with the aim of facilitating the development of one’s own operations. At the operational-strategic level these operations contribute to:

- Diminishing the morale and fighting strength of the enemy;
- Increasing one’s own and one’s allies fighting strength;
- Obtaining the help of neutral parties.

Civil Military operations: support special disaster situations.

C2TI. IO doctrine includes C2TI (Command, Control, Telecommunications- Computer Science, and Intelligence) as the set of human and technological resources and procedures that allow the commander and his staff to control, communicate, and know the enemy situation in real time. This abbreviation includes the other concepts of C3I and C4I.

Electronic War: a set of military activities developed in the electromagnetic spectrum, with the purpose of providing:

- **Electronic Support Measures:** those that determine the presence of enemy activity. These are offensive measures (search, intercept, localization, analysis, identification, and evaluation among others);
- **Electronic Support Countermeasures:** those that neutralize and/or reduce the use of electromagnetic energy dispersed by the enemy. These are defensive measures (such as deception and interference);
- **Electronic Support Counter-counter measures:** those that guarantee the electromagnetic energy dispersed by one’s own means. These are offensive measures (counter-deception and counter-interference);

Army doctrine considers electronic war as an essential part of every war. Its characteristics are that it:

- Is permanent, secret, complex, and utilizes highly trained personnel;

- Is adaptable to planning, centralization, and the conduct and coordination with other electromagnetic activities;
- Is flexible and adaptable to military maneuvers but possesses security measures;
- Is used in tactical surprise and provides speedy assessments.

Computer, Electronic, Cryptographic, and Communications Security: The Functional Regulations of Computer Systems used in the Army (RFD-75-01) contain the general rules for data administration and management for the forces' computer security and define the following:

- Computer Science: is the joint technique for the automatic use of information. Computing is important for military operations;
- Telecommunications & Computer Science: is the association between telecommunications and data processors' technical effects that help process information;
- Computer Science Troops: military personnel who maintain an efficient security system that avoids both the loss of information and non authorized access to the data;
- Kinds of Computer Security: Electronic Security, Communications Security, Cryptographic Security, Transmission Security, Computer Systems Security, and Physical Security.

Education related to IO. In different educational institutes of the Education and Doctrine Command of the Argentine Army and its higher educational institutions, personnel develop the following courses including some aspect of IO:

- Technical Higher School of the Army (EST): offers Degrees in Computer Systems Engineering, a postgraduate course in "Computer Systems, Cryptography, and Security," and a "Master in Technological

Management." The EST participates in the organization of the National and International Congresses of the Telecomputing and Cryptographic Systems Security shows (CONSECRI) where civilian and military experts from Argentina and the Region exchange knowledge on cryptography, cyber attacks, IO, security, and others issues;

- The Higher School of War (ESG) has a Tactical Trainer (ADITC) with simulation software that trains commanders and staff and in a General Staff Course the curricula includes some aspects of IO. For this reason many officers consider monographs or thesis related to IO in their studies;



Malvinas War Memorial in Buenos Aires (Wikipedia)

- School of Communications develops technical courses for military specialists and provides specific doctrine to employ the communications corps;
- School of Computer Science, created in 1992, has courses in Computer Security Science;
- Other Navy and Air Force institutes, and other public and private universities such as Buenos Aires Technological Institute (ITBA), also have courses on this issue;
- The Argentine and Chilean Armies jointly developed a Training System for Peace Missions (SIMUPAS), a virtual peacekeeping operation.

- AFCEA Argentina is the South American chapter of the Armed Forces Communications and Electronics Association (AFCEA International) that unites specialists in C4ISR. AFCEA develops military and civilian courses in IW, IO, cyber attacks, and PCII.

Argentine Military Understanding of IO

The Malvinas War (1982) [*editor's note: also called the Falklands War*] served as the baptism by fire of the Communications Units of the Argentine Army, in conventional operations. This war marks the first reference to the "Computing Revolution" as applied to telecommunications, and especially to electronic warfare. In 1999, the Argentine Army first evaluated the impact of information technologies, by examining the use of the Internet and satellite connections between other elements. As a result, Argentina created a unified Army Communication and Computing System Unit, with a digital net for the Systems Integration of the Army (REDISE).

Argentina's evolving military understanding of IO over the past five years is as follows:

- Argentina has an IW doctrine - The Argentine Armed Forces have specific doctrine on cybernetic war issues to include some restricted issues. The Argentine concept of EW (electronic warfare) is valid for IW (Commander of Argentine Navy G. Repetto, 2001);
- Strategic IW - In strategic IW, it is necessary to apply "the enemy as a system" theory of Colonel John Warden, attacking the C4ISR of an enemy while maintaining capabilities in C2 & TI. The threats to the national information infrastructure are real, non-traditional, and highly diversified. It is necessary to develop operational concepts and structures to have superiority on the new

battlefield (Colonel, Ret., of Argentine Army, AA, H. Cargnelutti, 2002);

- **Cybernetic Strategy - Capturing cyberspace's power** requires a Cybernetic Strategy to organize the Cybernetic Force and develop new weapons. New national and international laws are necessary. Cyberspace, where "cybernetic operations" are conducted, is not limited as is the traditional battlefield. Hence, its duration and operational range is wider (Col A.A. and Veteran of Malvinas War, E. Stel, 2002).

- **Basic Objectives of Military Computer Security** - The security of the military computer system must accomplish four basic objectives: confidentiality, confidence, integrity, and disposability of information. IW is offensive, and it is necessary to train military personnel how to enter enemy nets. This organization would be the Army's "hackers" in conflict situations. (Captain F. Calvete, Military Engineer in Computing Systems of A.A., 2003).

- **Future Wars** - These will involve IW. Modern armies must protect their own information and nets, and attack the same capabilities of the enemy on the new cyberspace battlefield. (Col. A.A. Cerezo, 2003).

- **Need for new Strategic Military Thought in the Information Age** - Argentina's National Defense System doctrine must include IW and IO concepts. IW/IO Commission, the Center of Strategic Studies, and the School of War are all doing work in these areas (CEE-ESG, 2003).

- **Definitions** - Argentina does not strictly adopt the standard IO Definition, but the Argentine Armed Forces Information System is used in the IW context. Argentine cyber military doctrine is oriented toward a security perspective, with IW as an asymmetrical threat. If the Argentine Armed Forces include IW concepts in their doctrine, it can only help toward the identification of operational and I-D capabilities for asymmetric war. It will be necessary to incorporate both defensive and offensive IO within the definition of future complementary operations (for example, military deception). Even though there is not a doctrinal definition of IW in

computing systems, there is increasing interest in the application of these concepts (Majors A.A. Machinandiarena and Tabeada y Gaidano, 2003).

- **IO is Part of Asymmetrical War** - IO includes attempts to deceive or undermine the capabilities of enemy forces. Offensive IO includes infrastructure attacks, PSYOP, and misinformation. It is only necessary to have a PC, a modem, and a program to get into an enemy's C4 or weapon system. (Major A.A. Machinandiarena, Battalion 601 of Electronic Operations, 2004).

- **Strategic Operational Dislocation in New Wars** - Dislocation is achieved through a direct or indirect approach against an enemy force, to cause an imbalance in their forces, disconnect elements of their command, affect their moral and maneuver capability, or to weaken their defenses. Dislocation can be achieved via technological and digital capabilities, which can be improved still further with the use of IO (Col Roberto Pritz, Director of the Higher School of War of A.A., 2005).

Latin American Countries' Understanding of IO

In the Latin American region there are other studies related to IT in military affairs. Homeland Security Departments include many IT security aspects in their respective areas of responsibility. In the military camp, there are fewer precise definitions of IO/IW. However, as is the case with Argentina, IO is part of military study groups, and many IO-related opinions have a national basis:

- **Strategic Information Warfare (SIW)** - This refers to the use of computer systems against the critical infrastructure (CI) of a country. It is the new way to conduct "war and anti-war" (Alvin Toffler). Brazil has created several responsible offices designed to defend the countries critical infrastructure. (Commander Riquet Filho, Brazil Navy, 2003).

- **Cyber War is Not Yet Uniformly Defined** - Cyber war can be understood as measures taken against C2 systems, operational security, electronic war, piracy, hackers, and information

blockades. Since 2003 the Brazilian Navy has established rules of digital information management for their local nets (Commander Nascimento de Annunciacao, Brazilian Navy, 2003).

- **Cyber War** - This concept corresponds to the offensive and defensive use of information systems and information to deny, explore, corrupt, or destroy adversary values and information systems as well as computer networks. Cyber war attempts to obtain advantages in both the military and civilian realms. Twenty countries are preparing cyber guerillas as "elite troops" (4th Computing Systems Security Committee Meeting, Brazil Ministry of Defense, 2003).

- **Cyber Terrorism Post 9/11 in the Western Hemisphere** - The inability to accurately track cyber attacks may give the impression that there are a lower number of incidents in Latin America—which is wrong. History indicates political and military conflicts are increasingly accompanied by cyber attacks. A large percentage of military traffic moves over civilian telecommunications and computer systems. Trends seem to point to the possibility of terrorists using information technology as a weapon against critical infrastructure targets. Regional exercises are one of the best ways to assess such critical infrastructure vulnerabilities. There is a significant difference in the usage of computers and the Internet between Latin America, the Caribbean, and North America. International collaboration and cooperation is important to ensure security of international networks, which would in turn make local systems more secure. (Lt. Col Wanda I. Cortes, US Air Force Reserve, Inter American Defense College, 2004).

In July, 2007, the Colombian Telecommunications Committee published a study for the implementation of a National Strategy for Cyber Security. This report considers security of communication nets a secondary preoccupation for most countries in the region. Some Latin American nations have begun adopting information security labeling procedure (rule ISO/CEI 17799), but there is a juridical weakness.

• Identification of Critical Infrastructure - Mr. Aristides Royo, Ambassador of Panama to the Organization of American States (OAS) and Chair of the Inter-American Committee against Terrorism (CICTE), announced in March 2007 that CICTE will soon begin to review its work plan. It is likely the organization will identify areas related to critical infrastructure, both in physical terms (ports, etc.) and in terms of the so-called “virtual variety.”


Conclusions

During the course of history, war was fought on open battlefields. During the twentieth century, with the development of the submarine and air power, war extended its horizon from one to three dimensional battle spaces. A fourth geo-strategic battle space was also created near the end of the millennium: cyberspace. At the beginning of the twenty first century, the dimensions of war are as foggy as they are clear, as Admiral William Owens explained in his *Lifting the Fog of War*. For the military

commander, the contemporary battlefield is full of difficulties—the Net has produced a new fog of war. Cyber war forces changes in many of our objectives, strategies, doctrines, and procedures. In these new conflicts, C2TIs bring different capabilities to commanders. But the C2TIs bring new vulnerabilities too because all the public-private critical information infrastructures are integrated, and one effective attack could generate multidimensional “cascade effects.”

Within the Organization of American States (OAS), the countries of Latin America and North America agreed to a common vision of cyberspace threats, and to the first lines of protection and reaction—both physically and virtually—against them. In Latin America this situation requires the elaboration of relevant national, bilateral, and multilateral policies and strategies. It is first necessary for all member countries to secure critical information infrastructures. Each organization, especially military forces, needs to be

prepared and trained to remain mobile and to generate influence (in terms of power) on a global scale. Argentine and other Latin American armies have general doctrinal concepts to confront the new challenges in cyberspace. They can help support one another’s responsibilities along with other public areas, to include not only their countries, but also regional protection of critical information structures.

Regional military forces should permanently update their doctrines in order to generate methods, techniques, and training. Each country should develop new doctrines according to its own capabilities and national realities, to support both bilateral and multilateral mechanisms of cooperation. Those who have updated doctrines can confront new situations with confidence. In his “Strategy for Action,” the French strategist General Beaufre reminds us “it is necessary to act as a thoughtful man and to think as an action man”—because the future is now. 



Javier Ulises Ortiz has a PhD in Political Science. He graduated with a degree in International Relations (University of Salvador, Buenos Aires, USAL). He also has a Master’s Degree in Drug Conflicts (Catholic University of Salta). His postgraduate work has been in the area of strategy at the School of War of the Argentine Army (ESG); and at the Defense planning and Transformation Course of Defense Studies (US National Defense University). He is a Professor of Strategic Analysis (Information and New Conflicts in the ESG and has a Master’s Degree in Defense and Hemispheric Security (USAL, Inter-American Defense College). He is a member of the Center for Strategic Studies (ESG); has lectured at the School for Advanced Military Studies (SAMS) in the US; and at the Armed Forces Communications and Electronics Association (AFCEA). He has also lectured in South America and in several defense, military, and security institutes of Argentina, France, Colombia, Brazil, Paraguay, and Honduras.

Chile: A Vision Of Information Operations

By Igor Carrasco Neira

Mr. Igor Carrasco Neira noted that in his role as a responsible party for critical information protection in Chile, he is most interested in a global reform of the agreement on computer crime. Further, he feels that information will transform social development into a resource, weapon, and target.

Though the image of IO has shown brightly since 1991, especially in light of the First Gulf War, it was not until 1 January 1994—the date when the Zapatista Army of National Liberation (EZLN) uprising was started in Chiapas, Mexico—that we saw the practical effects of an information operation. The EZLN first utilized the Internet as an instrument of war to disseminate its ideas, to raise money, to denounce the Mexican government, and by means of cyberspace recruiting, to attack the networks of the Aztec government by sending massive emailings and computer viruses.

As a contextual fact, until that date the total number of servers connected to the Internet worldwide was 2,217,000. As a result, any given state's use of information technology was low. Yet the Zapatista's IO results could not be qualified in the same way; they gained several advantages from the use of information technology.

What Are the Innovations/ Advantages of the Information Age?

- First, technological advances have actually permitted information-based processes to reach never before seen levels of efficiency;
- Second, there is an increasingly greater dependency on technology systems for handling and transferring information;
- Third, this dependency enabled identification of new vulnerabilities and weaknesses that favor the development of new technologies and procedures for exploiting them, and as a consequence, their countermeasures;
- Fourth, political leaders' interest in rapidly assimilating their respective states into the larger Information Society has grown.

The importance of this assimilation is evident: those who ignore the information age will be left behind, both socially and economically. For example, the multimedia industry, which includes information technology, telecommunications, and mass media, is clearly affected by information age developments. The requirement for economic and societal transformations makes entry conditions into an information society a decisive theme for the future.



Chilean Forces insignia.
(Wikipedia)

Today, the cold combination of circuits and metal—the final product of an industrial process—does not make the difference. It is processed information that generates a substantial advantage in social competitiveness. Information now has a leading role in transforming social development into a “resource, weapon, and target.” Information has been converted into strategic wealth as well as a condition for competitiveness. Information technologies introduce enormous changes, surpassing pure economics and offering new social, political, and cultural promises through information and communication networks.

The products derived from intellectual activity represent a decisive

part of collective wealth. To a large extent, international competitiveness in the new century is a battle of intelligence, that is, of mental models to interpret reality.

The pinnacle of world information networks, such as the Internet, constitutes a considerable challenge for societies. There are evident benefits for the state that uses electronic media, including information media, but also by implication assumption of certain risks—understood to mean the possibility of success or failure—that should be minimized to guarantee information integrity and acceptable service performance. Since 1998, there are well-known reports indicating the presence and execution of programs designed to control and electronically eavesdrop on the different communications of our planet. In February 1999, Director of the US Central Intelligence Agency (CIA) George Tenet, warned that “Various countries have or are developing the capability to attack adversary information systems.” He later added, “to develop the capability to attack computers can be inexpensive and ultimately attainable: this requires minimal infrastructure.”

National Forces

National information technology security policy came into being in the mid-1990s because of the need to confront the “Y2K” effect. This forced us to prepare for a national catastrophe, or rather, to construct a national map of critical state information infrastructure. Even when primary attention focused on “information errors,” the strategic character of information forced the state into an in-depth analysis of the road ahead.

If there is a sector of society experiencing great changes in recent

years, it would undoubtedly be in state security and the armed forces. These changes contributed to the promulgation of Law 19.974 in 2004, whose objective is to establish and regulate the State Intelligence System (SIE), which is defined in Article Four (below), and which is chaired by Chile's Director of the National Intelligence Agency (ANI):

Article Four: *The State Intelligence System, henceforth the System, is the collective intelligence organization, ... functionally coordinated, that directs and executes specific intelligence and counter-intelligence activities, to advise the President of the Republic and those various high-levels of leadership of the State, with the objective to protect national sovereignty and to preserve constitutional order and, in addition, formulate intelligence opinions useful for achieving national objectives. The integral organizations of the System, without prejudicing their agencies and their obligations with respect to superior commanders, should interconnect among themselves through the exchange of information and mutual cooperation that this law and the legal code establish.*

The National Intelligence Agency was created in Title Three, Article Seven of the same law:

Article Seven: *The National Intelligence Agency will be created, a centralized public service, of technical and specialized character, which will be subordinate to the President of the Republic through the Interior Ministry, whose objective will be to produce intelligence to advise the President of the Republic and those various high-levels of leadership of the State, in accordance with current law.*

Among the ANI functions under Letter "C" of Article Eight: To propose protective norms and procedures for information systems critical to the State. In this context, national forces are concentrated in two areas: identifying and hardening information networks and infrastructure critical to the State; and creating the capability to influence a potential adversary.

Identification and Hardening of Networks

The tasks conducted in this field range from studies of information flows to reorganizing national networks. To this end, the government sets forth creation of a State Connectivity and Communications Network, through Supreme Decree 5996 of the Interior Ministry.

Presently, the Chilean government is contemplating cybernetic security development within the national technological development plan known as the *Digital Agenda*. The objective of this plan is to increase competitiveness, equal opportunities, individual liberties, quality of life, and the efficiency and transparency of the Chilean public sector through development and employment of information and communication technologies (TIC). At the same time, these actions help enrich the cultural identity of the nation and its native peoples.

The government plan of action for the period 2004-2006 established 34 initiatives, grouped in six areas:

1. Expanded access;
2. Education and training;
3. Online status;
4. Digital development of businesses;
5. Deployment of the TIC industry;
6. Legal framework.

Two of the thirty four initiatives are discussed here: numbers twelve and seventeen. Known as Project 5D, or *The Connective Network of the State*, Initiative Twelve encourages the telecommunications industries to develop a broadband highway voice-and-data-over-IP network for the public sector. It will connect all public branches—including municipalities, schools, hospitals, and clinics—permitting their convergence into a single network of telephone, mobile, and Internet services. Initiative Seventeen establishes a number of Interior Ministry responsibilities: to search and maintain a national response system for cybernetic incidents; administer programs; reduce threats and vulnerabilities; develop security training programs; secure the cyberspace in which the government

works; and administer national and international cooperation in cybernetic security matters.

Other decrees to improve cyber security include new technical norms to provide for the confidentiality of electronic documents. These measures establish steps for the public ministries and services to meet security standard ISO 17779, and specify security responsibilities for information circulating on state institutional networks.

Creating the Capability to Influence Potential Adversaries

Naturally, the most serious efforts to create capabilities to influence adversaries utilize information technology resources for training armed forces personnel. This is particularly critical given that modern conflicts are very different from only a few decades ago. In fact, the advance of technology is in direct relation to the decrease of men on the battlefield. Historical examples confirm that during the US Civil War, the "density of men" was approximately 8,200 soldiers per square kilometer. According to NATO doctrine, during the years 1985-1990 there were approximately 400 men per square kilometer. After observing the current war in Iraq, we estimate a density of 15-17 soldiers per square kilometer.

This decrease is due to better armament which is increasingly more lethal, more precise, and lighter weight, but also due to better prepared soldiers. We find that soldiers have greater access to information technology, beginning early in their schooling. This enables the capability to direct things, people, and equipment with greater efficiency. It also allows for the introduction of computer system training directly into the military environment.

Presently, there is an organization within the Chilean War Academy dedicated to this type of training: the Computerized Tactical Operation Training Center (CEOTAC). The center's fundamental objective is to prepare officers, but includes developing the software necessary for this task: the SETAC (Tactical Training System). This advanced military simulator



*Chile in its South American context.
(CIA)*

replicates modern combat conditions in the computer, thus reducing associated training costs. This same center created the Institution and Organization Management Training System (SEGIO) software that prepares civil organizations for emergency situations.

The technology has been very useful in educating soldiers, as well as in instructing them in weapons-handling and marksmanship techniques. The Bernardo O'Higgins Military School has a virtual firing range, with two screens that can project fixed or moving targets, offering the cadets a sensation of reality. The range includes all principal Chilean Army weapons: the Famae 5.56mm rifle, the Beretta 9mm pistol, and the Minimi 5.56mm submachine gun—all of which can be loaded, and produce a shot recoil effect. All of the preceding training saves resources, and results in excellent marksmen. Such technologies enable realistic training, produce a

higher quality Chilean soldier, and produce a deterrent effect on potential adversaries.

Combating Crime and Terrorism: Legal Status in Chile

In 1993, Chile ratified Law Number 19.223, which typified legal precepts relating to information technology. Following the French model, this law marked a milestone in Chilean legislation, since it introduced penalties for a number of IT-associated behaviors. The intention was to protect the quality, purity, and suitability of associated information.

The law was important for penalizing unlawful access to computer systems, altering and damaging computer data, and divulging such data. Nevertheless, continuous TIC innovations require consideration of a global reform on computer crimes agreements. Two bills seeking to reform our criminal code on this matter. Both initiatives address a similar type of criminal technical processing: the predominance of the protected legal right as a systematized factor. The first is a parliamentary motion that tackles reform of Law 19.223 on information technology crimes:

- Unlawfully accessing information contained in a computer system;
- Destroying a computer system or altering its function;
- Unlawfully obtaining telecommunication services.

The second corresponds to an executive message categorizing new methods that are not criminalized in our legislation, such as computer crimes:

- Falsification of electronic documents and credit cards;
- Computer fraud;
- Unlawfully obtaining telecommunication services.

Both of these initiatives are currently being processed in the Chilean National Congress. In short, the aforementioned actions seek to solve legal problems that have arisen through introduction of new types of criminal offences, or modification of existing offences based on traditional legal rights.

Chilean International Actions

In order to address the numerous international challenges related to this matter, the Special Policy Director (DIPESP) of the Foreign Affairs Ministry established an Inter-Institutional Working Group on Cybernetic Crime in 2004. The group is made up of representatives from the Interior Ministry, the National Intelligence Agency, the Justice Ministry, the Attorney General, and the Investigative Police. Among their objectives are strengthening cooperative links with other countries, as well as promoting and deepening an information exchange to confront emerging threats in this area.

Thus far, Chile has conducted international actions primarily at the regional level: The Inter-American Commission against Terrorism (CICTE); the Meeting of American Justice Ministries (REMJA) under the OAS; the General Assembly of the OAS; plus the fields of APEC and the United Nations.

In the framework of the REMJA, Chile actively participated in the Third Meeting of the Group of Government Experts on Matters Relating to Cybernetic Crimes, in 2003. A series of recommendations arose from this meeting that are still relevant, and we believe the international community should provide appropriate follow-up on these issues.

Agreement of the European Council on Cybercrime: The Chilean Position

In order to define our country's position regarding eventually joining the Agreement of the European Council on Cybercrime, Chile requested reports from all institutions competent in this matter. In general terms, members favored an eventual Chilean entry into this part of the agreement.

Besides scrutinizing the methodologies and results of the 2004 Fifth Meeting of the American Justice Ministries or Attorney Generals, Chilean representatives noted recommendations for State members to "evaluate the benefit of applying the principles of the Agreement of the European Council

on Cybernetic Crimes (2001) and consider the possibility of joining this agreement.”

Intelligence and Globalization

Themes addressing intelligence are more complicated, given the scenarios that arise from globalization. Although this process presents advantages and opportunities for society, it also gives rise to new conflicts. Emerging areas of struggle range from the research, the knowledge, the industry, and the resulting commerce, to new forms of crime that lend support to criminal organizations, insurgents, or global terrorists.

Information Technology Attack as a Threat

Knowing about and protecting against computer attacks on Chile's infrastructure is indispensable for functioning information and communication systems. Further, such knowledge is critical for public administration of the country's vital businesses—energy, electricity, telecommunications, fuel supply, transportation services, health services, and security among others. The majority of these services administer their productive processes remotely

through computer networks, and in real time, thus these have become mandatory tasks.

This subject demands a relevant example. In this context, it is certainly necessary to protect information networks, but also to clearly determine the origin and motivation of the perpetrators, given that the state's response will be completely different if the attacker is a criminal hacker, or a hostile action by another nation-state.

Other data also provides evidence of the magnitude of technological dependency and the requirement for its protection. In 1983, there were a total of 562 computers connected to the Internet across the entire world. In 1993, the number rose to 1,200,000 computers. By June 2005, counting only broadband connections, in Chile alone there were 594,000 computers connected to the Internet. Today the number exceeds one million broadband connections. Thus in two years, there has been more than a 60% increase in Chile alone.


Conclusions

All future scenarios must consider the state's dependence on information

systems and complex computing technologies, where many control processes are made in real time and from a distance. As a result, these will be extremely sensitive—if they are not already—and will be likely targets of hostile action from Internet and network experts.

Looking to the future, we see the high probability of increasing dependence on these applied technologies:

- Cheap solar energy;
- Rural Wireless communications;
- Genetically modified food;
- Rapid biotesting through nanotechnology;
- Filters and catalysts for purifying and decontaminating water;
- Managed application of medicines;
- Hybrid vehicles;
- Wireless computers;
- Quantum cryptography.

Finally, to end with the words of authors John Arquilla and David Ronfeldt, “The information revolution alters the nature of conflict and introduces new modalities in the art of war, terrorism, and crime.” Chile is in the process of preparing to meet these threats, and more. 



Igor Carrasco Neira is Chief of the Division of the Information Society (DESI) of the National Agency of Intelligence, whose mission is to protect the critical information of the State. Since 1990 he has worked in Chile's defense and homeland security system. He is a former analyst of organized crime and new threats, and has represented the Chilean government at meetings of experts on information security in the Inter-American Committee against Terrorism (CICTE) of the Organization of American States in Buenos Aires, Ottawa, and Washington. He teaches courses in Chile and foreign countries on information security, information society, and new threat issues. Mr. Carrasco is an anthropologist with a degree from the Austral University of Chile. He is a Professor in the Institute of Political Science of the National University of Chile; a Diplomate in National Strategic Intelligence, National School of Intelligence of Argentina; and a Diplomate in the Methodologies of Intelligence in the Institute of Political Science, Chile University.



Air Force Symposium 2008: Cyberspace

July 15-17

Maxwell AFB, Alabama

Symposium Co-hosted By:

*Air University Cyberspace Information and Operations Study Center, Maxwell AFB, AL
8th Air Force and HQ Air Force Cyber Command (Provisional), Barksdale AFB, LA
U.S. Strategic Command, Offutt AFB, NE*

THREE MAIN TOPIC TRACKS

Doctrine and Concepts of Operations

- *Defining Cyberspace*
- *Establish the Domain*
- *Control the Domain*
- *Use the Domain*

Cyberspace Policy and Law

- *US and Int'l Law of Cyberspace Operations (From Peacetime through Post-conflict)*
- *Cyberspace Rules of Engagement, the Law of Armed Conflict, and Interoperability with Multinational Partners*
- *DOD Cyberspace support to the Defense Industrial Base*
- *Strategic Communications, Influence Operations and Public Affairs in Cyberspace*

USAF CYBER: Supporting National Security

- *CYBER is Inevitable: Military, Media, Markets*
- *CYBER: Military and Civilian Perspectives*
- *CYBER: DOD, DHS and Interagency*
- *CYBER: Educating and Developing the Force*

Who Should Attend: Military and civilian defense personnel, industry and business leaders, academics, and others interested in the Air Force's cyberspace mission.

GUEST SPEAKERS INCLUDE

• *Gen. Kevin P. Chilton, Commander, U.S. Strategic Command, Offutt AFB, NE*

• *Lt. Gen. Robert J. Elder, Commander, 8th Air Force, Barksdale AFB, La., and Joint Functional Component commander for Global Strike and Integration, U.S. Strategic Command, Offutt AFB, NE*

• *Maj. Gen. Charles J. Dunlap Jr., Deputy Judge Advocate General, Headquarters U.S. Air Force, Washington, D.C.*

• *Maj. Gen. William T. Lord, Commander, Air Force Cyberspace Command (Provisional), Barksdale AFB, LA*

• *Dr. Rebecca Grant, Founder and President of IRIS Independent Research.*

FOR MORE INFORMATION

Web: <http://www.maxwell.af.mil/au/awc/cyberspace/index.html>

E-mail: AFSymposium.2008Cyberspace@maxwell.af.mil

Commercial Phone: 1-334-953-1153 or 5998

DSN Phone: 493-1153 or 5998