NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXIII, No. 1 SPRING 1997

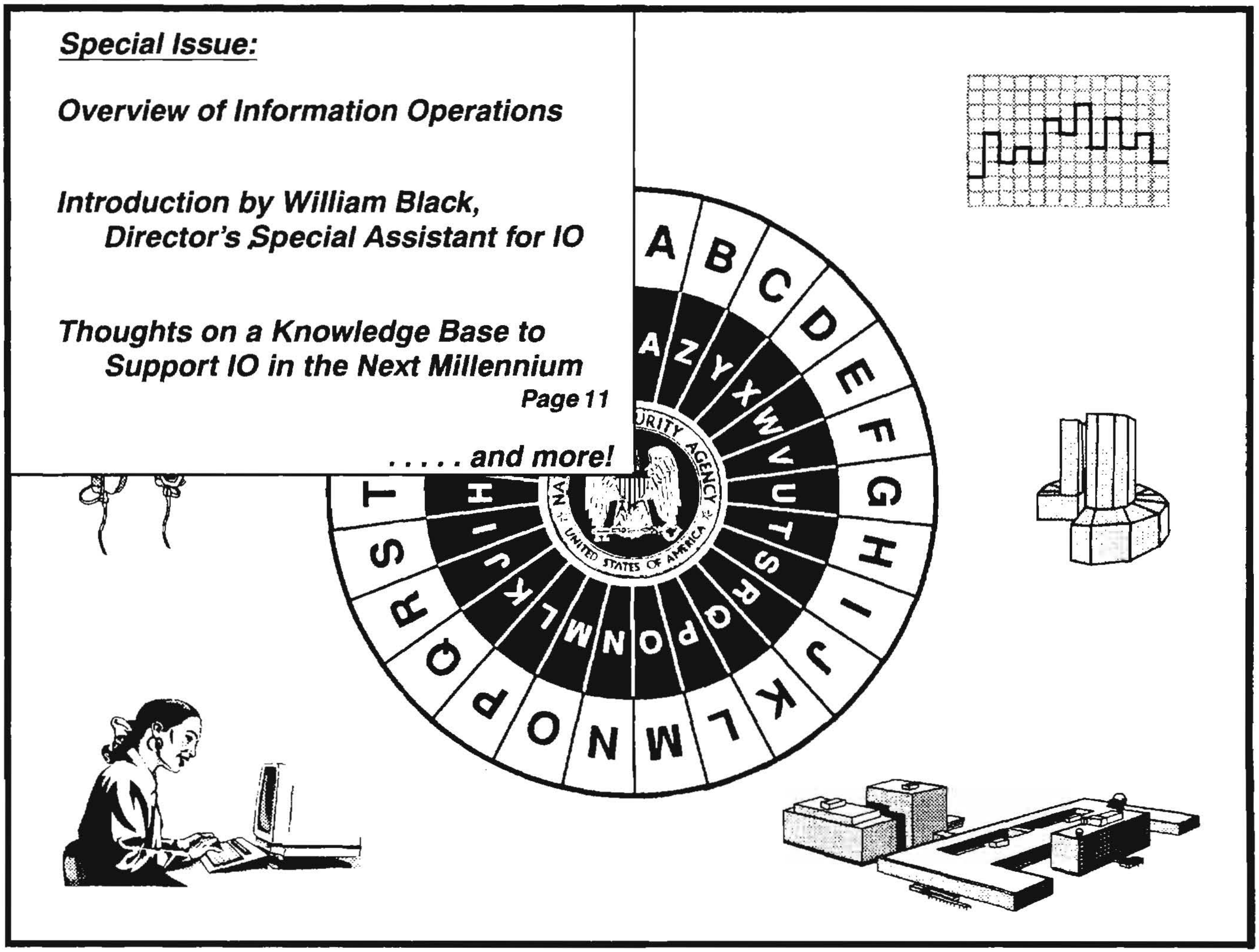
Special Issue:

Overview of Information Operations

Introduction by William Black, Director's Special Assistant for IO

Thoughts on a Knowledge Base to Support IO in the Next Millennium
Page 11

. . . . . and more!



CRYPTOLOG

Spring 1997
Vol. XXIII, No. 1

Published by P02, Operations Directorate Intelligence Staff

To submit articles and letters, please see last page.

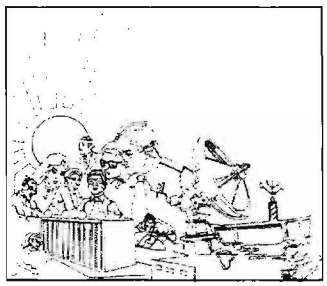


Table of Contents

P.L. 86-36

THINKING OUT LOUD ABOUT CYBERSPACE (U)

by William B. Black, Jr.
Director's Special Assistant
for Information Warfare

INTRODUCTION (U)

~~(S REL AUS CAN NZ UK)~~ On 3 March 1997, the Secretary of Defense officially delegated to the National Security Agency the authority to develop Computer Network Attack[1] (CNA) techniques. This delegation of authority has added a new, third dimension to NSA's "one mission" future. That is, in the networked world of Cyberspace, CNA technology is the natural companion of NSA's exploit and protect functions. This delegation of authority is sure to be a catalyst for major change in NSA's basic processes and its workforce. The end result, however, should remain information technology-derived products, services, and experts.

(U) The articles following this introduction were written by the staff of the Director's Special Assistant for Information Warfare. Because confusion still surrounds the emergence and history of Information Warfare (IW), these articles are intended to contribute to the common understanding of why Information Operations and its concepts are important to the future of NSA.

1. DoDD 3600.1, Information Operations, dated 09 December 1996, defines CNA as "operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves."

A HISTORICAL PERSPECTIVE (U)

(U) After World War II, an understanding of the core competency underlying the making and breaking of codes — cryptology — resulted in a national decision to consolidate both activities in one organization: NSA. Both activities benefited from this consolidation, and became stronger.

~~(S REL AUS CAN NZ UK)~~ Since the end of the Cold War, in an emerging networked world, an understanding of the emergence of a new core competency — "cyberology" — with its close technological relationship to cryptology has again resulted in a national decision to consolidate. Cyberology's central activities, i.e., "exploitation," "protection," and "attack," will be worked together, thus benefiting all of them.

SETTING THE STAGE (U)

(U) There are certain assumptions that underpin the thought processes related to preparing for our Agency's future in cyberspace. These are premises that are basic to the understanding, the preparations, and the acceptance of major changes. The following presents the main assumptions.

We're On the Edge of a New Age (U)

(U) First is an acceptance that we are on the edge of a new age, called the "Information Age." Also, that this new age is engulfing almost every aspect of society, including the very nature of our business. The basic premise is that the information technology advancements of the last 30 years far exceed any evolution of technology in the Industrial Age. These advances are so traumatic and far-reaching that they clearly represent something truly "new." It is important to note that, historically, technological advancements were called "revolutions" when they make progress of a single order of magnitude (e.g., the automobile "revolutionized" transportation because it was ten times faster than the horse). In the case of information technology, the contention is that the last thirty years have seen an advancement of not one but six orders of magnitude — 1,000,000 times! — in information technology. The end result has been a great deal of confusion and turmoil as human nature attempts to force the "new" of the Information Age into the "known" of the Industrial Age. This "new," however, does not fit; we have to change the thought process.

The Public Sees Government as the Bad Guy (U)

(U) Second, the public reaction to this new age has a direct relationship to the National Security Agency and the way we do business. At the beginning of the Industrial Age, the public centered in on industrialists and/or capitalists as being "the problem." Labor unions were created and child labor laws were enacted to curb their power. In today's Age, the public has centered in on government as "the problem." Specifically, the focus is on the potential abuse of the Government's applications of this new information technology that will result in an invasion of personal privacy. For us, this is difficult to understand. We *are* "the government," and we have no interest in invading the personal privacy of U.S. citizens. Regardless, the public's concerns are real and have an impact upon us. The Computer Security Act of 1987 is one example of this impact, for it clearly represents a first step in limiting any potential NSA involvement in the public sector.

This Age Brought Its Space With It (U)

(U) Third, a major aspect of the Information Age is that it is ushering in a totally new sphere of operations, a new environment called "cyberspace." For many, cyberspace is an ill-defined, comic-book concept — perhaps something created by a science-fiction writer or a Hollywood producer. But for NSA, in the Information Age, cyberspace is both real and virtual: while the real portion consists of physical assets (computers, network terminals, satellites, fiber optic cables, etc.) located on earth and in space, it is the virtual aspect — all interconnected, all networked, all compatible and interoperable — that is the most important. Almost every type of interaction that occurs in the physical world will have a corollary in cyberspace.

(U) In cyberspace, complex networks on networks emerge as an organizing concept upon which our future operations must focus. All networks are interconnected, and routing across the various elements of the network is automatic and not pre-determinable. Descriptors such as Defense Information Infrastructure (DII) or National Information Infrastructure (NII) refer to portions of users of the Global Information Infrastructure (GII) or better yet, the users of cyberspace's transportation system. The future global use and dependency on cyberspace should evolve much the way the use of the Internet has evolved today, i.e., because it should be extremely cost effective. The more important aspect of this inter-connectivity is the fact that, as we move into this complex networked future, computers are in charge, and physical geography becomes less and less important. While computers initially automated routine and mundane tasks, today inter-networking has turned computers and systems to networks, affording opportunities to work with greater and greater amounts of information at any distance. In the future, advances in artificial intelligence, and increases in understanding of cognitive processes, in general, will move us rapidly into a situation where computers and networks work in conjunction with each other, under broad guidance from humans, to actually make decisions and act on our behalf. This is cyberspace's future.

The Future of Warfare is Warfare in Cyberspace — a.k.a. Information Warfare (U)

(U) When we look to the future of warfare in the Information Age, we ask ourselves the question "How do you conduct warfare in cyberspace?" The answer is Information Warfare or, in accordance with DoD's new Directive 3600.1, Information Operations. Information warfare has been the subject of many speeches, scholarly papers, and popular journals. Information warfare has even made its debut in Hollywood in the film *Independence Day.* These many, differing views of IW confuse "information in war," "information technology enhancements of existing combat capabilities or weapon systems," and "warfare in cyberspace." In our view, "information in war" has been with us throughout history, i.e., intelligence on opposing forces was as valuable to Napoleon as it was to MacArthur. "Information technology enhancements" emerged during the Industrial Age with the natural evolution of weapons technology. IW for us, however, is "warfare in cyberspace" and is an exclusive feature of the Information Age. We believe that its biggest impact is yet to come.

(U) Another aspect of warfare that came with the Information Age is that actual, physical combat can be viewed in living rooms of America via television. The horrors of war cannot be hidden. As a result, in the simplest of terms, "body bags" are no longer acceptable. There is considerable societal pressure to find non-lethal means of accomplishing tasks that once called for conventional military action.

(U) For the military, the Information Age presents yet another problem. With the kind of computers, communications, and networking available in the commercial world, how can the military justify separate systems? Commercial communications networks are too inexpensive and too pervasive to ignore. The

good news for the military is that — probably for the first time — they will have interoperable communications in joint service activities and even in multinational operations. The bad news, however, is that they will also be interoperable with their adversaries!

~~(S REL AUS CAN NZ UK)~~ In Information Age terms, IW provides a "digital coercion" option. The primary target of this option is the information infrastructure of an adversary. Such information infrastructures are expected to be primarily computer controlled, operated by the commercial-civilian sector (unprotected), and the primary infrastructure upon which military forces almost totally depend. For IW purposes, access to these computer-controlled infrastructures can permit the degradation, disruption, or destruction of the network and/or the functions they serve. As a result, the "computers" become the intelligence "targets" of highest priority.

~~(S REL AUS CAN NZ UK)~~ There are specific types of weapons associated with Information Warfare. These include viruses, worms, logic bombs, trojan horses, spoofing, masquerading, and "back" or "trap" doors. They are referred to as "tools" or "techniques" even though they may be pieces of software. They are publicly available, very powerful, and, if effectively executed, extremely destructive to any society's information infrastructure.

(U) As a last thought in setting the stage, we expect the Information Warrior of the future to be very different in their thought processes. They will understand the non-physical nature of the future capabilities, will be comfortable with working across the spectrum, and have extensive knowledge of non-military targets. Probably most importantly, they will be comfortable with the concept of networks. They will understand that "information operations" are more than "operations" supported by intelligence and communications; rather, they will understand that all three function together synergistically. Finally, Information Warriors will understand that in the "tooth-to-tail" accounting of personnel, military personnel will be the "tooth" and civilians will be the "tail." Tail equates to the emerging information infrastructure, a primary strategic target of IW.

THE BEGINNING (U)

~~(S REL AUS CAN NZ UK)~~ The following articles will look in depth at various aspects of Information Operations or Information Warfare as they relate to NSA. "Cyberology" and our new CNA mission should provoke much thought and discussion. It is hoped that these articles will serve as a catalyst and basis for these activities.

~~(FOUO)~~ *Mr. Black retired from NSA in 1997 after a long career. He was the first Director's Special Assistant for Information Warfare, and oversaw the establishment of the Information Operations Technology Center.*

Kλ

IO, IO, It's Off to Work We Go... (U)

(U) The implications of the Information Age are profound. The fundamental underpinnings upon which societies around the globe have existed for the past few hundred years are shifting rapidly and without regard for our personal or organizational interests and equities. T. Michael Elliott, Executive Director of the IEEE Computer Society, sums it up rather eloquently:

> ***"...As we enter the next century, the most critical forces shaping the intersection of computing and culture will be social, not technical, as we come to recognize that "Cyberspace" is not just a pop name for a metanetwork, but a new dimension for human discourse that is effectively as real as physical space. The rules that have governed the relationships among peoples and governments in physical space cannot effectively cope with the interactions made possible by technology. New rules are necessary.***
>
> ***Historically, technological advancement has provided solutions to many social problems. However, the new problems created by our technology will require social, legal, and moral solutions, not technical ones. Current concerns about commerce, taxation, privacy, pornography, personal freedom, human rights, and national security — all approached from the multiple perspectives of different countries — can be expected to multiply.***
>
> ***Despite the differences in culture, traditions, and values, the integrating nature of cyberspace will force common solutions. Governments will never again be able to fully isolate their people from the ideas of the world or keep their guilty secrets from world scrutiny. Ultimately countries will be forced to cope with the reality that traditional national boundaries are meaningless in cyberspace. Or will they?"***[1]

(U) Information Warfare (IW) or Information Operations (IO), as it has now been recast to recognize the concept's applicability across the entire spectrum of "conflict" from competition through crisis and to war, has been recently defined in a much-debated Department of Defense directive as:

> ***Information Operations (IO) : Actions taken to affect adversary information and information systems while defending one's own information and information systems.***[2]

(U) Despite the existence of this directive, opinions on the concept differ as the various public- and private-sector elements struggle to understand the implications of the information age. In military circles, Information Operations is being discussed primarily within a traditional battlefield context and with a predominantly industrial-age mind-set.

(U) To understand the contrast between industrial- and information-age thinking, take an example from the business sector. Today, fundamental thinking regarding economic matters is rooted in industrial-age concepts. Financial analysts, familiar with industrial-age valuation, based on hard-and-fast physical plant, equipment, and inventories, find it very difficult to create an accurate balance sheet for many of the new high-tech start-ups, whose primary assets exist between their employees' ears and in digital form in the companies' computers — information-age intellectual capital.

(U) As societies transition from their indus-

1. T. Elliott, *IEEE COMPUTER*, January 1997, "The Next 50 Years of Computing", p16.
2. Department of Defense Directive S-3600.1, SUBJECT: Information Operations (IO) (U), dated December 9, 1996. Enclosure 1 page 1-1.

trial-age roots to the information age, economic thinking will be transformed[3] as will our concepts of "warfare."[4] The discussions surrounding Information Operations and Information Warfare are crucial to our future — especially in light of increasing global economic competition founded upon information-based societies and enhanced by ever-increasing global connectivity, where information is THE capital commodity.

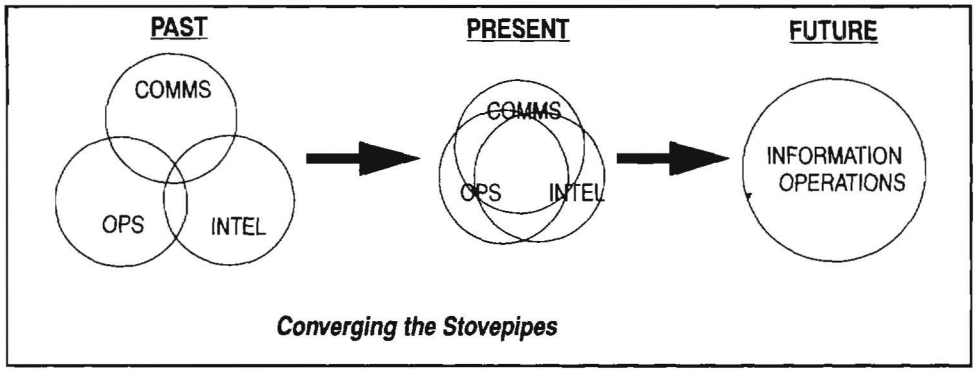
PERSPECTIVES (U)

(U) While there are many reasons for the confusion surrounding this topic, three stand out: the magnitude of the information age's impact, the convergence of organizational roles and missions surrounding the shift from industrial to information age constructs, and the fact that we tend to talk past each other, using different basic concepts of information warfare.

(U) First, the explosion of information technology, and the resultant enhancements in global connectivity, are much more than a revolution in technology — it is, to use the Toefflers' terminology, "a wave change." To understand the impact of a wave change, it's best to take a historical perspective. In the fifteenth century, agriculture was the predominant occupation and the possession of land to produce agricultural commodities the main avenue to wealth. As we moved into the nineteenth century, mechanization appeared. The mass production of simple sewing needles — of all things! — marked the beginning of an industrial revolution, fundamentally changing societies and shifting the basis of wealth and power from ownership of land to possession of industrial capacity. That shift from an agrarian to an industrial society, fraught with apprehension and difficulty for some and excitement and opportunity for others, involved issues of enormous consequence and brought with it broad and profound change. Individuals' lives were altered. Government's role was dramatically transformed. New institutions were formed.

(U) We are now at the leading edge of the information age. Just as in the last shift, we will be forced to tackle issues of like magnitude. Information technology and its age will alter our lives permanently, force the re-orientation of governments, break down old institutions, organizations, and rules, and create whole new ones.

(U) The second major cause of confusion is convergence. At a fundamental level, we see the information age blending our personal and professional lives, blurring the distinction between private and public, and collapsing functional areas of responsibility that, in the industrial age, were separate and distinct. This convergence manifests itself in government bureaucracies as "rice bowl" fights. It is not that we're trying to steal each other's missions and functions — it is that those missions and functions are beginning to overlap.



Converging the Stovepipes

(U) To use an example from the military, the J3s, or the operators of the military world, are beginning to understand that information, traditionally the J2's job, and information technology or communications support, the J6's job, are so integral to their operations that they can no longer do without them. In the information age, it will no

3. For some interesting perspectives on information-age economic thinking, see the article by Kevin Kelly in WIRED, 4.06, June 1996, entitled "The Economics of Ideas" based on concepts of noted economist Paul Romer of the University of California at Berkeley.
4. I refer the reader to the "classic" IW reference *War and Anti-War* by Alvin & Heidi Toeffler for some interesting thinking along these lines.

longer be adequate for the J2 and J6 functions to be performed in a supporting role. Lt. Gen. Guenther, the head communicator for the U.S. Army, summed it up by saying "we've got to get rid of the stovepipes."

(U) Here at NSA, this convergence is the premise behind our "One Team with One Mission" battle cry. In essence, where in the past we were perfectly capable of performing our protect and exploit mission as practically separate and distinct functions, in the information age, where our customers and targets are all on the same network and using the same equipment with the same vulnerabilities, we have got to converge on a single unified objective.

(U) Finally, our third reason for confusion lies in the vocabulary. In the Information Operations/ Information Warfare business, we tend to talk past each other, largely because we're using the same words but have different notions of what they mean. It's the whole "we've got different Mental Models" problem described in Peter Senge's book *The Fifth Discipline: The Art & Practice of Learning Organizations.*[5]

5. Senge, Peter M., *The Fifth Discipline — The Art & Practice of Learning Organizations*, Doubelday, 1990.

A Taxonomy for Information Warfare: Three Waves, Three Schools of Thought

WAVE	FIRST (AGRARIAN)	SECOND (INDUSTRIAL)	THIRD (INFORMATION)
PHYSICAL SECURITY PROVIDED BY	A Warrior Class, Mercenaries, Militia	Professional Citizens	Information Knowledgeable Leaders
DOMINANT SOCIAL, POLITICAL, ECONOMIC FORCE	Tribe, City, State	Nation-State	Global Conglomerates
ECONOMY DOMINATED BY	Trade	Money	Symbols
WAR CHARACTERIZED BY	Representational Conflict	Mass Armies	Information Attacks
ULTIMATE DESTRUCTIVE CAPABILITY	Gunpowder	Weapons of Mass Destruction	Critical Information Deletion
INFORMATION IN WARFARE	YES	YES	YES
INFORMATION TECHNOLOGY IN WARFARE	NO	YES	YES
INFORMATION WARFARE	NO	NO	YES

(U) As depicted in the chart on the preceding page, there are three fundamental concepts of Information Warfare.[5] Each has its own set of definitions, or interpretations of definitions, and its own distinct set of priority issues and concerns.

(U) First, we have the "information *in* warfare" crowd. These folks originate predominantly from the intelligence community and the ranks of military historians. They view IW as nothing new, pointing out that information has always been important in warfare. Today, there is a lot more information and we've gotten better at moving it around. This group spends its time arguing whether systems should be "push" versus "pull," and how to get the right information to the right person at the right time in the right place. These, of course, are important discussions and valid issues.

"information technology in warfare" gurus . . . view IW as a force multiplier to enhance existing combat capabilities — as another annex to an Operations Plan

(U) Secondly, we have the "information *technology in* warfare" gurus. This group, which is composed of much of the military establishment around the world, takes its lessons from the Gulf War. They perceive that the future of warfare lies in long-range, high-precision munitions. Information warfare is viewed as a force multiplier to enhance existing combat capabilities, i.e. as another annex to an Operations Plan. Along the lines of Michael Hammer's popular book *Re-Engineering the Corporation*,[6] they view information technology as an enabler that will allow them to re-engineer their current "business" and increase efficiencies. They continually look for innovative ways to integrate information and information technology into their industrial-based warfighting machine, seek out information-based targets which will expedite the fight, and push the intelligence establishment to provide greater and greater levels of detail in a more timely manner. This group, however, is still very much rooted in traditional force application.

(U) Finally, we have the "information warfare" group. Proponents who understand the information age and know the fundamental nature of warfare will be dramatically different in the digital realm. This group recognizes that Information Operations will lose its battlefield context in the next millennium. They believe that, increasingly, a society's leadership will desire to limit crisis and conflict and that those leaders will look to resolve conflict before it begins, via "digital" coercion if necessary. This group, to some extent, perceives a diminution of powers vested in nation-states and sees the emergence of trans-national "special interest" groups who will desire to further their objectives with inexpensive, efficient, surgical "bit-based" capabilities. They see the spread of global conglomerates, competing on a global economic battlefield, and point to today's increase in economic espionage as an early indicator of things to come.[7] This group views a future where Cyberspace dependency and information-based societies are the norm, where opportunities and vulnerabilities abound. This group describes "Information Warfare" as warfare in Cyberspace.

MAKING THE LEAP (U)

(U) It is important to understand that Information Operations and the associated cyber-based capabilities are very information intensive propositions. Shaping Cyberspace is a long-term activity which will require a serious continuity of effort. Maintaining an ability to operate in this ever-changing realm will demand a continuous and aggressive pursuit of information and options.

5. This chart originated on a white board at the National Defense University in one of their early Intermediate Information-Based Warfare Courses. Dr. John Alger used Toeffler's waves to describe differing perspectives of Information Warfare.

6. Hammer, M & Champy J., *Re-Engineering the Corporation —A Manifesto for Business Revolution*, HarperBusiness, 1993.

7. By the way, the increase in economic espionage, and computer-based crime in general, has already drawn a response from the Department of Justice, vis-a-vis last year's Economic Espionage Act of 1996, which redefined terminology regarding computer and information misuse and strengthened penalties.

(U) Secondly, a number of communities of interest, with varying objectives, will need to perform Information Operations at various levels of secrecy. The methods used in the intelligence world — working sustainable clandestine and covert operations, across the entire spectrum, of economic, political, and military targets to exploit systems and produce intelligence in support of a variety of customers — match, very well, the needs of tomorrow's Information Operations community. Our future demands that we devise mechanisms to coordinate among the various communities of interest to maximize our opportunities and minimize the impact of vulnerabilities — in essence, balancing the offense and defense based on a set of common objectives.

(U) Third, while enormous opportunities exist in Cyberspace, there is a down side. The characteristics that make cyber-based operations so appealing to us from an offensive perspective (i.e., low cost of entry, few tangible observables, a diverse and expanding target set, increasing amounts of "freely available" information to support target development, and a flexible base of deployment where being "in range" with large fixed field sites isn't important) present a particularly difficult problem for the defense. Detecting and/or assessing adversary Information Operations will continue to be an incredibly difficult task requiring the ability to track the evolution of an adversary's intellectual capital, and to gather and correlate, in real time, massive amounts of data from a number of non-traditional sources like law enforcement and the computer emergency response community.[9] So, just keep things in perspective; before you get too excited about this "target-rich environment," remember, General Custer was in a target-rich environment too!

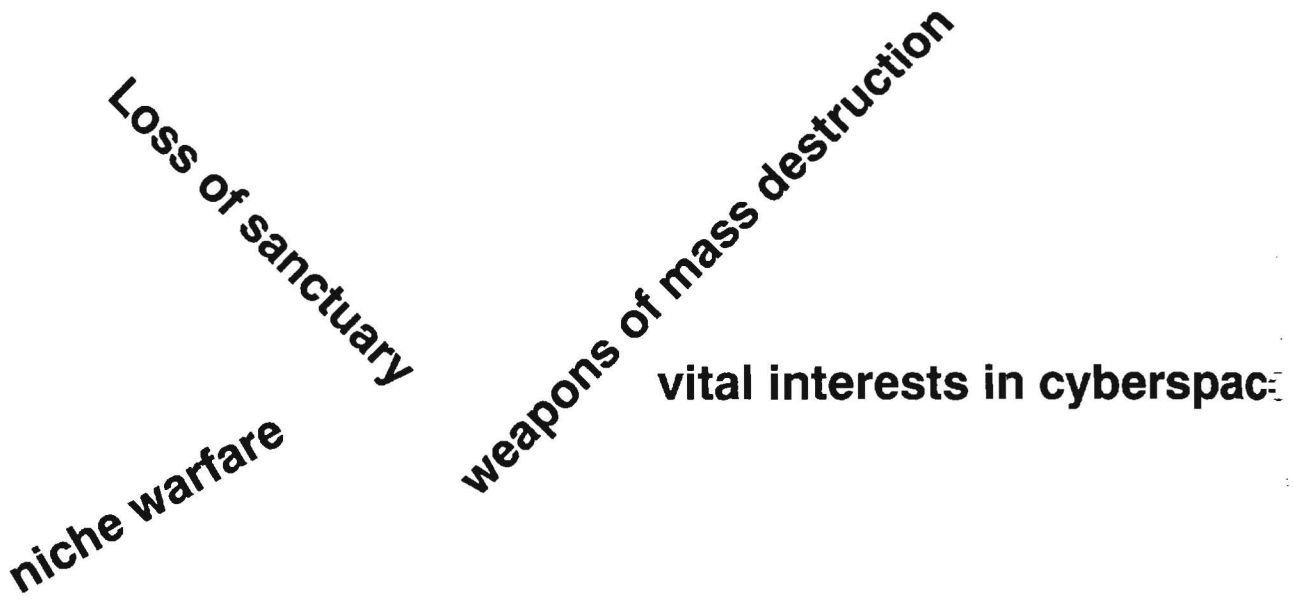
CONCLUSIONS (U)

(U) We hope you now have a sense of what Information Warfare/Information Operations is all about and, more important, that you have a feeling for the importance of this debate and are beginning to recognize amazing similarities between the expertise, capabilities, and knowledge required to perform "information operations" and those of the National Security Agency.

(U) Obviously, we have a stake in all three of the IW camps discussed earlier. And as "information providers" and "information protectors," rightfully so. We have to recognize, however, that the future is coming faster than we may care to realize. We must begin today to focus on developing the knowledge, expertise, and partnerships required to perform and/or support Information Operations in the next millennium.

Kλ

9. I direct the reader to DIA's interim report on Information Warfare Indications & Warning. It's an excellent paper that encapsulates the enormity of this task and discusses the current state of warning against this emerging threat.



The Revolution in Military Affairs

DECISIVE FORCE

Whither conventional warfare?

Compellence
Asymmetry
Anonymity
Time & Space

Connect At Your Own Risk!

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

P.L. 86-36

The Infowar Revolution(s) (U)

by [redacted]

(U) Advances in Information Technology are having profound effects on any number of aspects of societal relations — political, economic, cultural, and military. In some cases, the changes have been sufficiently dramatic to justify calling them revolutionary. In others, the changes in Information Technology allow for significant improvement in the performance of existing systems and structures, but don't fundamentally alter them. Both types of change are important, and it is important to be able to distinguish between the two types in order to better understand and cope with the rapid pace of change. Improvements to performance might generally be accommodated within existing structures and processes; revolutionary change typically requires new ones.

(U) This article describes a view of the Information Technology-related changes going on today and postulates revolutionary change on at least three levels nearly simultaneously. This construct helps to illustrate why the U.S. Government is having such difficulty reaching closure on how to organize for Information Warfare, progress on which has been slowed by the complexity of interrelated changes and the sheer breadth of activities and interests that are affected and therefore must be taken into account. For the most part, however, this is an argument for rapid and large-scale change in NSA, DoD, and the Intelligence Community to respond to the enormous and rapid changes taking place in the world around us.

The Three Revolutions (U)

The Revolution in Political Affairs (U)

(U) Information Technology (IT), by which I mean both the technology per se and its functional application, is fundamentally changing the ways in which the world works. The gradual changes in international commerce (and international crime) that have been brought about over the last few decades by improvements in transportation systems will be dwarfed by the scale and pace of change that IT will make possible. The steady erosion of the sovereignty of nation-states by the border-spanning activities of multinational corporations will be vastly accelerated by the transformation of information into a form of wealth whose movement is unconstrained by geographic borders and largely uncontrolled by governments. Traditional taxation structures and customs controls, upon which governments depend for revenues and the advancement or protection of domestic industries, will not work in the Global Network.

(U) One of the key effects of these changes will be the blurring of the already fuzzy line between international criminal activity and national security concerns. Efforts to deal with the international dimensions of the illegal drug problem have already pointed up the difficult domestic choices — whether and how to use military forces to supplement law enforcement efforts to interdict the flow of illegal drugs — as well as the impact of domestic law enforcement efforts on the conduct of foreign relations. This is hard enough when what we're dealing with is physical commodities (drugs, cash) and international travel arrangements, but just exactly who is going to protect our computers and networks from electronic intrusions that origi-

nate outside the U.S. — local law enforcement? federal law enforcement? the military? our Internet Service Providers? It could be that we're on our own: Connect At Your Own Risk! It might be an electronic parallel to life on the frontier in the middle of the 19th Century — government hasn't yet caught up to you, the Army can't protect you, and nobody (or everybody) claims legal jurisdiction over you.

(U) At the same time, enormous changes are taking place at the level of the individual. For U.S. citizens, there was a considerable sense of security for an individual in the very obscurity of living in a vast country with hundreds of millions of people. But privacy rapidly evaporates as digitized information is created, stored, accessed, and manipulated. For the U.S., in particular, there's a significant loss of anonymity that's implicit in this state of affairs. The other side of the coin, is the increase in power that accrues to the individual by virtue of the access to information, political and societal forums, and the tools and mechanisms of political and economic power. If knowledge is power, then an information-based society is home to an extremely large number of powerful people.

(U) The combination of these macro- and micro-level changes can be expected to produce truly revolutionary change in the political affairs of the nation and the world. This top-level revolution is already beginning and moving very quickly as existing technologies and infrastructures are integrated with new ones in ways so complex and unexpected as to defy any attempt to forecast its course. It's in this context that the other "revolutions" occur.

The Revolution in National Security Affairs (U)

(U) The well-being of societies and their economies is increasingly tied to information systems that provide or control basic services. As a result, a new category of "vital interests" has been created; these interests need to be protected as a function of national security. Such systems can't be defended by means of conventional military force, because there is no means of interposing military forces between the adversary and one's own systems in a networked world. As a fallback, one might attempt to deter cyber attack by threatening to retaliate with military forces. But deterrence relies on being able to identify and punish the attacker, and the anonymity conferred by cyberspace makes detection and identification difficult. In a situation where they can't defend and they can't deter, the usefulness of conventional military forces — one of the strengths of the U.S. — is seriously undermined.

Deterrence relies on being able to identify and punish the attacker, but cyberspace's anonymity makes detection and identification difficult

(U) One of the effects is what has been referred to as "loss of sanctuary": the inability to prevent attacks on the homeland. The combination of geography, conventional military force, and nuclear deterrence that served the U.S. for so many years is largely irrelevant for warding off cyber attacks on our information infrastructure, so we must devise some other means of protecting and defending this vital interest. The first problem is always to determine whose job it is to provide these defenses and who will pay for them — a political as well as a logical decision. Some form of defense will have to be created to restore at least some semblance of "sanctuary." Failure to do so threatens to severely reduce U.S. freedom of action internationally as our ability and willingness to bring military power to bear around the world is called into question. From the standpoint of an adversary, it may not be necessary to devise ways of countering U.S. conventional forces if the U.S. can be dissuaded from employing them in the first place. This is the essence of the "revolution": the concepts and realities of military power that have formed the basis for guaranteeing national security for centuries are giving way to other, non-military means of compelling desired behavior, and we have to adjust our approach to national security accordingly.

(U) Even after the "revolution" actually occurs, some of the more traditional forms of enhancing national security will continue to be in favor. First and foremost, the above-described situation unfortunately increases the incentives for numbers of countries to acquire (and maybe use) weapons of mass destruction as a "cheap fix" for otherwise insoluble security problems. It is virtually unthinkable for most countries to attempt to match the U.S. in conventional military capabilities; their economies could not support the expenditures necessary to deploy and sustain sizable forces with cutting-edge technology. But a truly modest WMD capability could be used most effectively to persuade an enemy not to launch conventional military operations. The other, related area of proliferating military technology is cruise and ballistic missiles. When combined with the coming availability of high-quality and relatively timely imagery from space, missile technology offers practically assured destruction of key strategic targets — regardless of whether the payload is WMD or improved conventional munitions. Such capabilities provide enormous disincentives to enemies to launch military operations against otherwise inferior opponents who can retaliate this way.

The Revolution in Military Affairs

(U) Over the last few years, a lot has been written on the subject of the anticipated Revolution in Military Affairs — the RMA. The problem with all this work is that the "revolution" has already happened. The Gulf War in 1991 confirmed what a few prescient souls had begun to suspect — that the nature of conventional military operations had changed dramatically.

(U) It's somewhat ironic, but not surprising, that the Russians understood some 10 years ago where U.S. progress with integrating weapons and information technologies was going. It's ironic, because for the most part the U.S. was oblivious to the implications of the various thrusts; it's not surprising, because the Russians' dedication and commitment to military science and doctrinal development has always dwarfed our own, particularly at levels above the tactical. (Weapons of Mass Destruction, Operational Art, and Revolution in Military Affairs are all terms and concepts that we "lifted" from Russian military science writings.)

(U) What the Russians perceived happening in the mid-1980's was the creation by the U.S. of a class of "systems of weapons" that integrated near-real-time targeting and fire-control information with very accurate and highly lethal ordnance. The Russians referred to these weapons generically as "reconnaissance-strike complexes" and were gravely concerned that such capabilities would cancel out any advantages they possessed in the realm of conventional (non-nuclear) combat. Their concern was based on an appreciation for the changes that the range and speed (mobility and reaction time) of these systems would have on the spatial character of the battlefield. Since their doctrine called for deeply echeloned forces to concentrate mass at critical places over the course of time, this entire construct was going to be obviated by U.S. abilities to locate, and to deliver devastating fires against, those massed forces before they could be employed — even deep in the theater on Day 1.

(U) The lethality, range, and tempo of this kind of combat was also seen by the Russians as dictating a come-as-you-are kind of war. The high levels of destruction that could be inflicted immediately at the outset of hostilities meant that one couldn't match attrition with production and there would never be more capabilities available than were in existence on Day 1. But this was part and parcel of their basic insight into the nature of the "revolution." The key elements in transforming warfare were:

- *the numbers of new weapons systems available. The technology alone is not sufficient; it must be present in large enough numbers to make a difference in the way the war is fought; and,*

- *the development and institutionalization of a doctrine that would govern the effective use of such capabilities. (In this regard, they may have read more into Air-Land Battle and Follow-on Forces Attack than we ever intended.)*

DECISIVE FORCE (U)

(U) The U.S. doctrine that emerged from the Gulf War (also influenced by the actions in Panama and Grenada) was one of applying Decisive Force to win quickly and minimize our casualties — attributes that were useful politically as well as militarily. The doctrine seems ideally suited to our posture as an engaged, but not aggressive, lone superpower.

(U) This doctrine will only work, however, if we maintain the numbers of forces, weapons, and capabilities necessary for its execution. That we will do so is not a foregone conclusion. Some contend that we fought DESERT STORM on the residuals from our Cold War investments and seriously question whether we will tolerate the expense of procuring and maintaining such high levels of forces and weapons into the future. High-tech or not, if we can't muster Decisive Force, then we can't apply it and the doctrine is hollow.

~~(S)~~ Decisive Force is an offensive doctrine, but it fails if we can't protect our forces from missile/air attack and WMD. Potential adversaries understand that high casualties might be sufficient to cause the U.S. to disengage from (or refuse to engage in) military actions that were not widely perceived as directly threatening our vital interests. It's precisely this consideration that militates in favor of such measures as:

- *Anti-Tactical Ballistic Missile (ATBM) defenses; cruise missile defenses; and Cover, Concealment, & Deception (CC&D); and,*
- *innovative approaches to neutralizing adversary WMD and missile weapons.*

~~(S)~~ The speed and spatial scope of the operations envisioned in employing Decisive Force put a premium on Command and Control:

- *the U.S. relative advantage in C^2 allows us to fully capitalize on our relative advantage in firepower and mobility;*
- *attacks on C^2 are therefore highly relevant to the probabilities of operational success — i.e., it is likely to be cost-effective for most adversaries to attack the U.S.'s C^2 systems rather than to build a comparable force/weapons infrastructure;*
- *exploiting (vice attacking) an adversary C^2 system is a highly effective and efficient way of gaining advantage, and the rest of the world is becoming more accomplished in the discipline of SIGINT exploitation for military support.*

IN THE FUTURE (U)

(U) Moving to the new plateau in conventional operations — long-range, high-lethality weapons guided by precise, real-time intelligence — is the revolution in military affairs, but there will be follow-on actions that consolidate the new way of fighting:

- *structure changes that improve on "jointness" to achieve better R&D, planning, and execution integration (we won't be able to afford the luxury of four air forces and the Decisive Force doctrine);*
- *better integration of Operations and Intelligence, with Ops becoming more "target-smart" and Intel becoming more responsive;*
- *people will get smarter about this new way of fighting and better able to make use of the information available to them.*

(U) Note that these major changes haven't yet occurred. The present structure's organizational inflexibility becomes a serious source of friction, reducing the potential for realizing the benefits of the weapons and information system capabilities; it

will have to be eliminated by major re-structuring. Ops and Intel will have to be integrated; under the present system they don't work the same problems except when a shooting war forces them to.

(U) The results of the initial application of the doctrine in the Gulf War were so dramatic that one is forced to conclude that it is extremely unlikely that the U.S. will ever again be challenged in a DESERT STORM-type confrontation. Cold analysis and calculation says there isn't a military on the globe that could hope to prevail; and the level of destruction of military equipment and personnel would be so great that few could even expect to survive as functioning entities. Of course, not all such decisions are made on the basis of pure logic, but such a monumental miscalculation has to be considered a remote possibility for the near future.

(U) Unfortunately, the fact that no opponent is likely to engage us in our preferred form of combat doesn't translate into a presumption of no challenges. In fact, potential opponents will expend considerable time, energy, and resources:

- *devising alternative modes of competition,*
- *estimating our threshold for engaging military force and carefully managing their activities to stay under it, or*
- *developing capabilities to attack critical dependencies in our basic doctrine of applying Decisive Force to achieve rapid victory with minimal casualties (for our side).*

~~(S)~~ The last of these options is what has come to be known as "niche warfare." Among the most likely and threatening of these challenges are the following:

- *threats to U.S. forces deploying to or in theater — with the most likely being WMD and ballistic or cruise missile delivery systems;*
- *actions to reduce the U.S. information advantage, probably by means of counter-C2 activities supplemented by the development and use of imagery and signals intelligence capabilities to increase their own force effectiveness.*

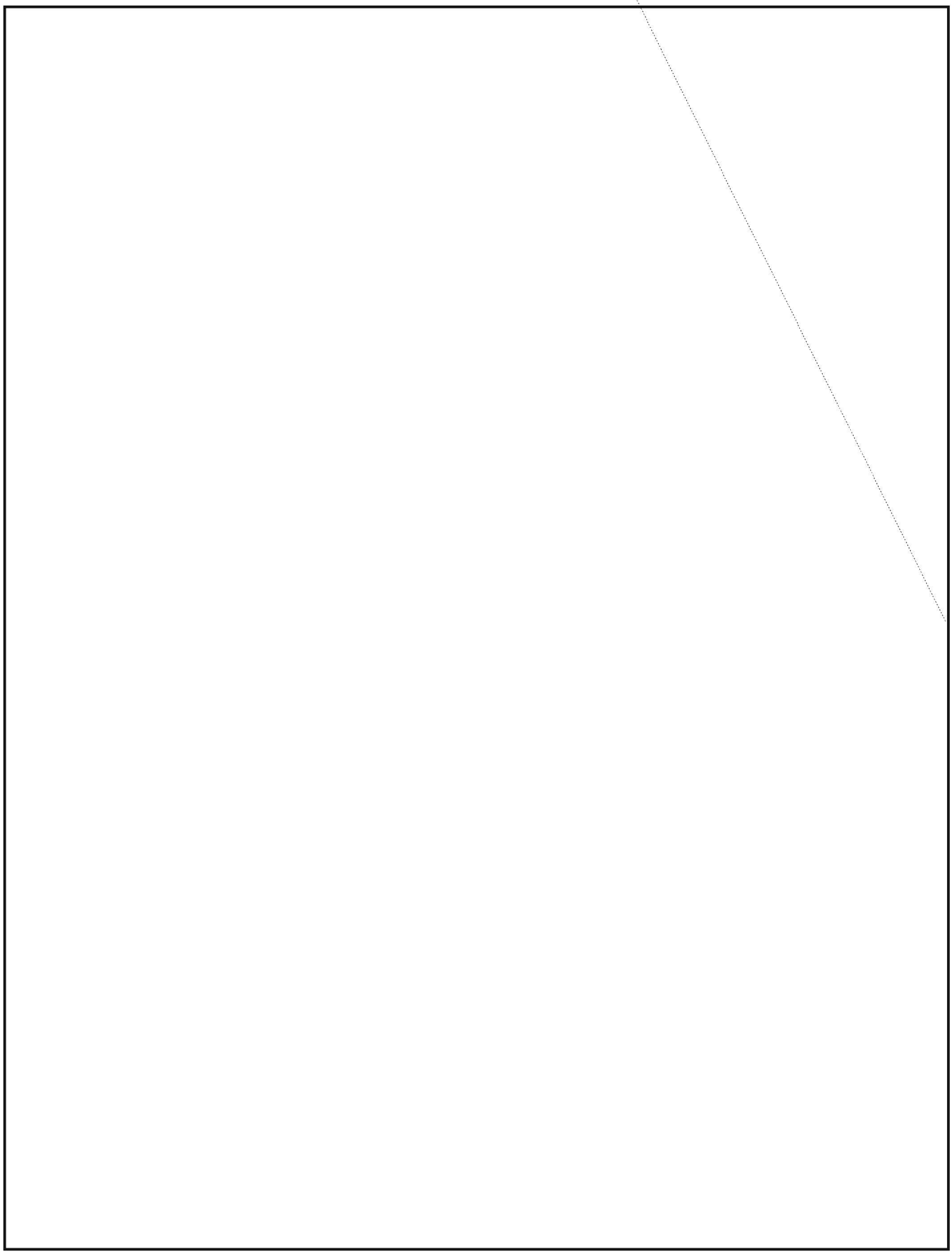
(U) The problem for the future, then, is twofold:

- *how do we deter these kinds of challenges?*
- *if deterrence fails, how do we fight in this environment?*

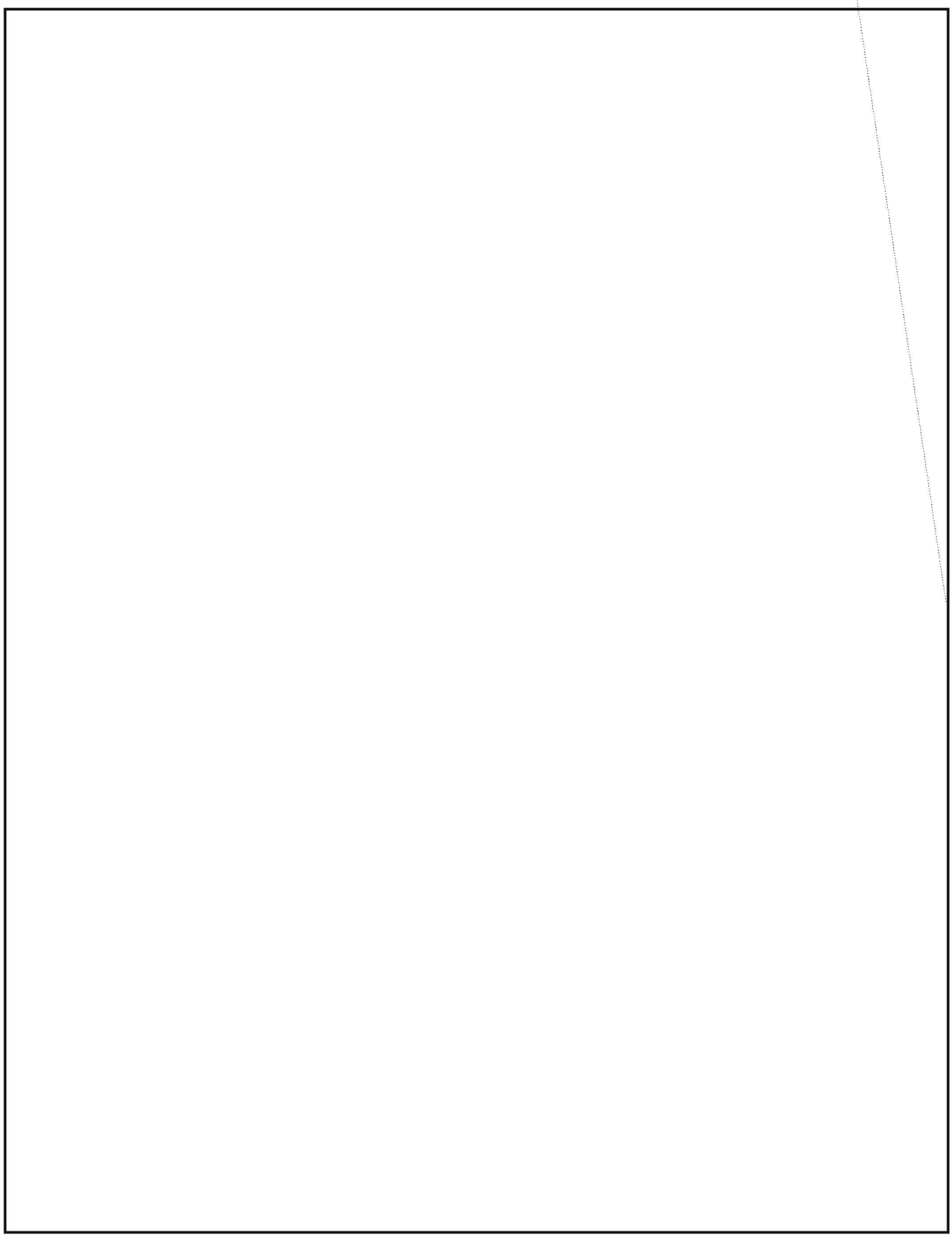
IW Today: The State Of Play (U)

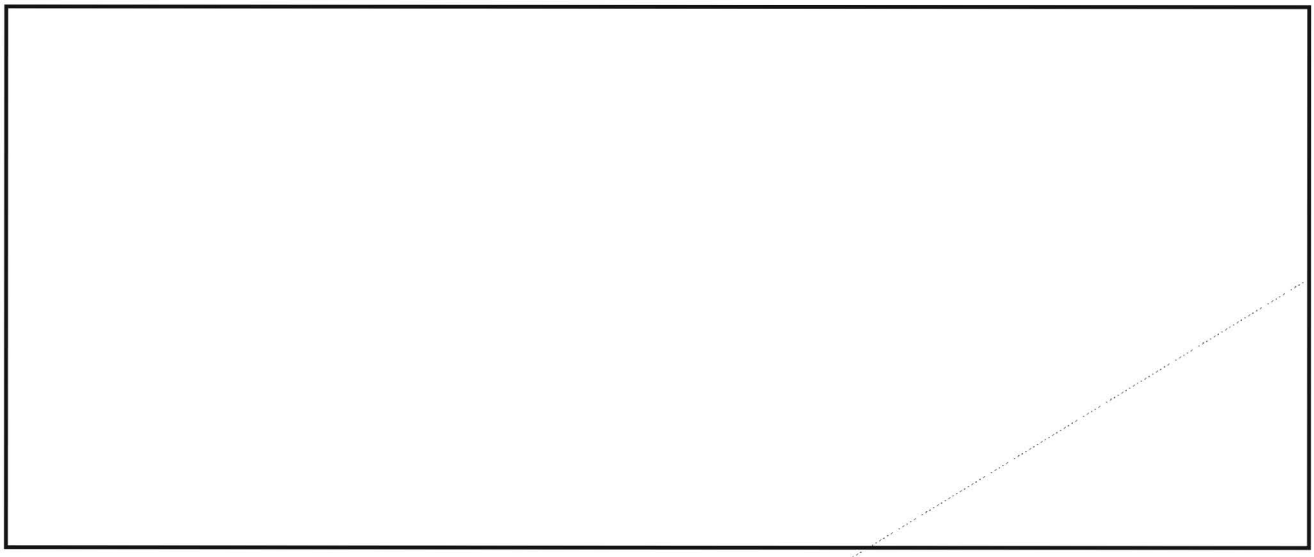
~~(S)~~ IW today is a totally unfocused concept. The description of IW has been continuously expanded since its inception, gluttonously swallowing up whole disciplines and pre-existing categories of activity in what has appeared to be a competition among departments, agencies, and consultants to devise the most all-inclusive — the grandest — definition of the term, thus demonstrating their superior view of "The Big Picture" and validating their claim to the ownership of the concept. Thus the "terminology war" has brought us from Information Warfare to Information Operations, which also includes Information Assurance as well as Information Warfare and Command and Control Warfare, which subsumes . . . Well, you get the idea. The end result of all the hyperbole is that, if IW is everything, then it is in fact nothing.

~~(S)~~ The inability to identify IW as something unique has led to a failure to refine the offensive and defensive aspects into discrete actions to be accomplished. This lack of specificity is compounded by the failure to place responsibility and the consequent absence of guidance. The key to making progress is to fix responsibility and allocate resources accordingly; the centralization of decision-making and resources under bureaucratic actors that can be held accountable is essential.



~~SECRET~~





Kλ

EO 1.4.(c)
P.L. 86-36

The Role of Information Warfare in Strategic War (U)

by [redacted]
P.L. 86-36

~~(S)~~ If the greatest contribution that an advanced Information Warfare (IW) capability can make to the security of a state is the *prevention* of conflict, then surely the second greatest contribution must be to ensure that the state *prevails* in unavoidable conflicts. Possession of an IW capability confers real advantages in war, including strategic war. It is the contention of this article that consideration of these advantages will yield the following conclusions:

• Information Warfare is neither a pipe dream nor an academic fad. Although it is only in its infancy with respect to technical development, it is apparent that it can make a significant contribution in strategic warfare, as measured by the traditional indices of success, and it needs to be integrated into nuclear war planning.

• IW is not just a "Smash & Jam" capability. It is qualitatively different from those measures executed in previous conflicts under the rubric of "Electronic Warfare" or "Command and Control Warfare." Information Warfare provides capabilities that are a quantum leap more advanced than either.

• The significance of the IW contribution will continue to grow as the U.S. strategic force structure draws down, particularly in a post-START III-world, with an evolving foreign strategic threat picture.

• To the degree that it contributes to maintaining confidence in the robustness and effectiveness of U.S. strategic forces, IW enhances deterrence and strategic stability.

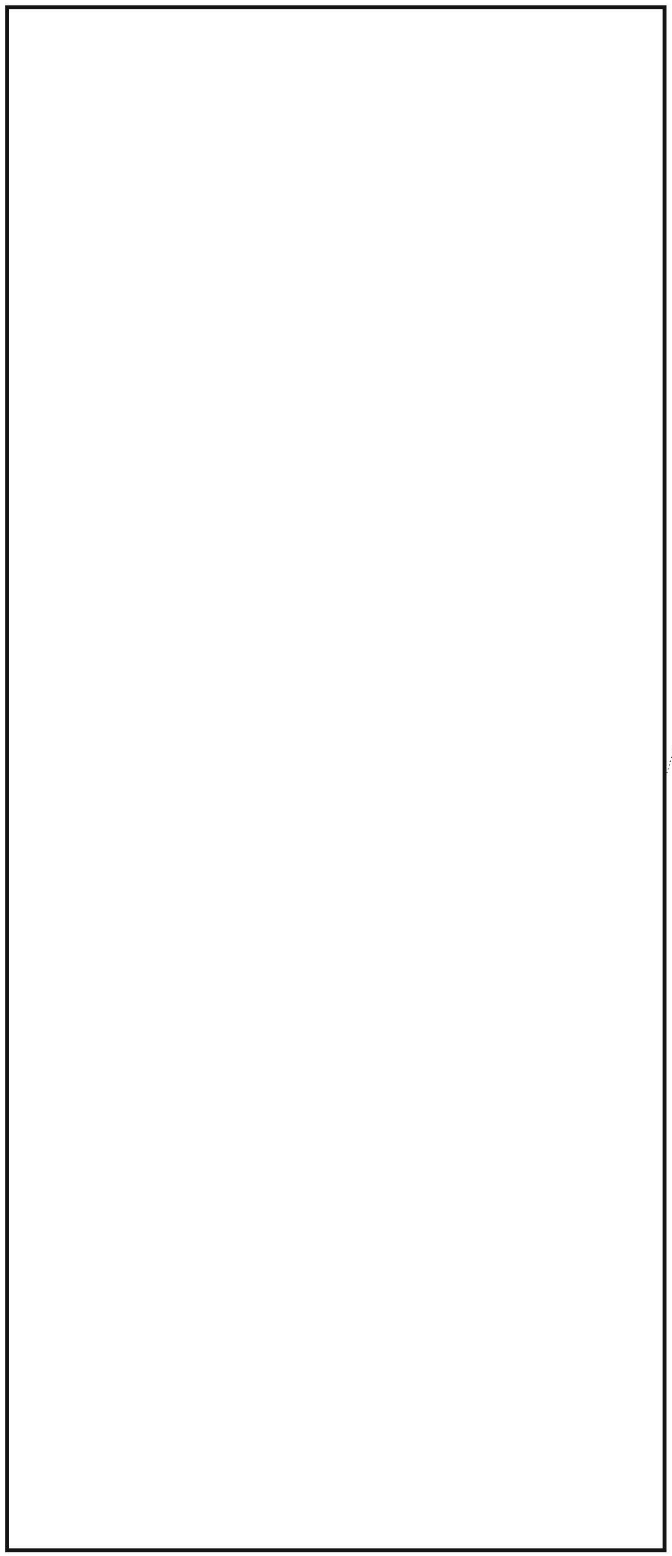
• Real IW will not be cheap. It will require substantial investments to ensure properly specific intelligence support and continuing access.

STRATEGIC WAR IN THE POST-COLD WAR ERA? (U)

~~(S)~~ Everyone recognizes the radical transformation in national security affairs that has taken place since the waning days of the Cold War. To what extent is a concern over the prospect of a strategic war — and the role of information warfare in it — a realistic one? There are several reasons to believe that such concern is not just an exercise in macabre nostalgia. They include: (1) the evolving political context; (2) the changing threat environment; and (3) possible drawdowns in U.S. and allied force structures. Taken together, these developments warrant continued intellectual engagement with strategic issues, and the involvement of IW in particular.

[redacted]

EO 1.4.(c)
P.L. 86-36



~~(S)~~ Similarly, questions need to be asked about future Chinese security policies. As the Communist Party sorts out who will rule China in the post-Deng era, can anyone seriously exclude the possibility of an increasingly assertive Chinese policy, often in conflict with U.S. or allied interests? As the PRC continues to develop economically, it can hardly escape notice that China has continuously upgraded the quality and quantity of its strategic forces, both through indigenous efforts and by upgrades through foreign purchases and by foreign expertise. By 2010, China could pose a serious security challenge to the U.S.

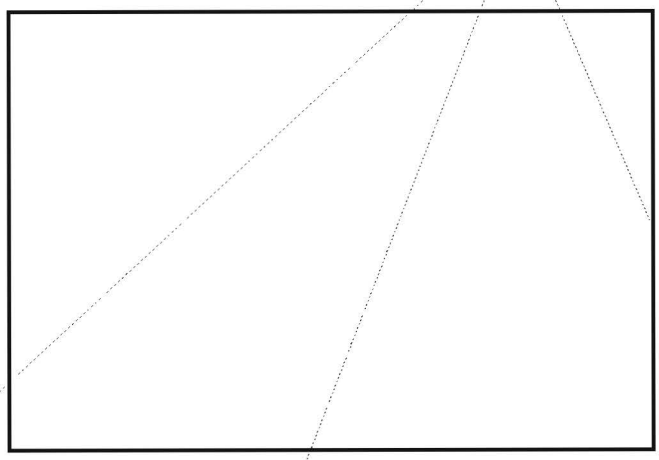
~~(S)~~ Nor should one discount the danger of the "Nth-country" threat. While the capabilities and threats posed by Russia and China are relatively easy to see, they should not cause us to overlook the emerging strategic threats in such countries as North Korea, Iran, Iraq, Libya, or an unknown state. The evidence of ballistic missile and Weapons of Mass Destruction (WMD) programs is quite clear, and these countries also learned the folly of confronting the U.S. with a conventional-only threat. It is not unreasonable to conclude that one or more of these states could pose a strategic threat to the U.S. or (more likely) its allies over the next several decades.

~~(S)~~ One last factor to consider when evaluating the chances of strategic warfare in the Post-Cold War Era is the strategic force posture of the U. S., and, to some degree, its allies. The Strategic Arms Reduction Treaty (START I) reduced the numbers of strategic warheads in the U.S. inventory significantly, but with over 8,000 warheads on ballistic missiles remaining, we were hardly unarmed. The follow-on START II Treaty imposed a ceiling of 4,250 weapons, to be reduced to 3,000 to 3,500 by January 2003. Preparations for a possible START III Agreement appear to center on reducing strategic weapons further to 2,000 to 2,500. Even this reduced figure represents an awesome capability. It is the levels of *post*-START III inventories that take on strategic significance for the period out to the first quarter of the 21st Century, under the scenarios we have been examining. If a post-START III agreement managed to limit U.S. strategic warheads to somewhere in the range of 300 to 1,000, the conjunction of rekindled Russian hostility, enhanced Chinese capabilities, or emerging N-th country threat with reduced U.S. strategic deterrent capabilities could make war "thinkable" in some quarters, undermining strategic stability.

The Role of IW in Strategic Warfare (U)

EO 1.4.(c)
P.L. 86-36

(S) At this point, it would be useful to clarify what we mean by "Information Warfare" and how we see it being employed in strategic warfare. The term "Information Warfare" has been used to describe a variety of activities over the past several years. Within the U.S. Department of Defense, IW has come to mean the application of Information Operations in wartime, and is said to comprise the so-called "six pillars" of Psychological Operations, Operational Security, Deception, Electronic Warfare, Physical Destruction, and Computer Intrusion.



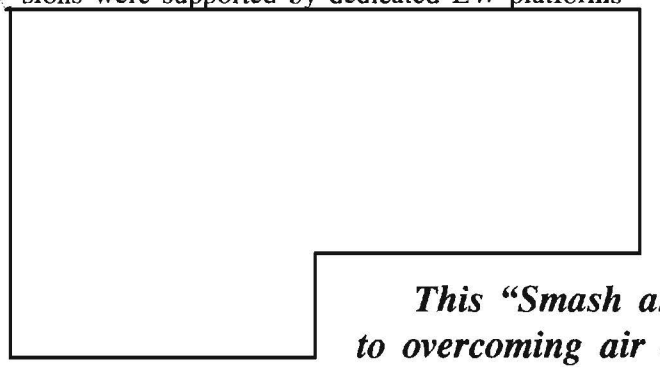
(U) The question occasionally arises whether there is anything fundamentally new about IW. After all, it is argued, the application of Electronic Warfare dates back to 1942 and even C2W dates to early 1991 in DESERT STORM. To respond to this question, I'd like to pose two general strategic problems and compare the solutions from previous conflicts with that available from IW. The two general strategic problems involve (1) overcoming enemy air defenses, and (2) neutralizing an economic-industrial target, in this case a power station.

Case I: Overcoming Enemy Air Defenses (U)

(U) Since World War II, strategic warfare has entailed delivering ordnance on important enemy targets in the rear, usually in the enemy homeland. This has meant facing concentrated, advanced air defenses during the ingress leg, during the drop, and during the egress portion of the mission. These defenses generally comprise some combination of early warning radars, reporting centers, tracking and guidance radars, ground-based fire such as AAA and later, Surface-to-Air Missiles (SAMs), air defense aviation, and the command and control necessary to lash it all together. The heavy losses suffered by the U.S. Eighth Air Force in the early years of World War II led to the incorporation of EW into mission planning. Beginning as early as 1942, USAAF operations featured the use of chaff and jamming in the counter-air defense

mission, along with providing fighter escort and targeting enemy air defense facilities for physical destruction with bombs. ***This combination of EW and physical destruction set the pattern for defeating enemy air defenses for the next fifty years.***

EO 1.4.(c)
P.L. 86-36 ~~(S)~~ During the Cold War, Strategic Air Command planners built an EW plan right into the SIOP execution. Penetrating bombers were provided with increasingly sophisticated EW suites, with both active and passive capabilities, and missions were supported by dedicated EW platforms

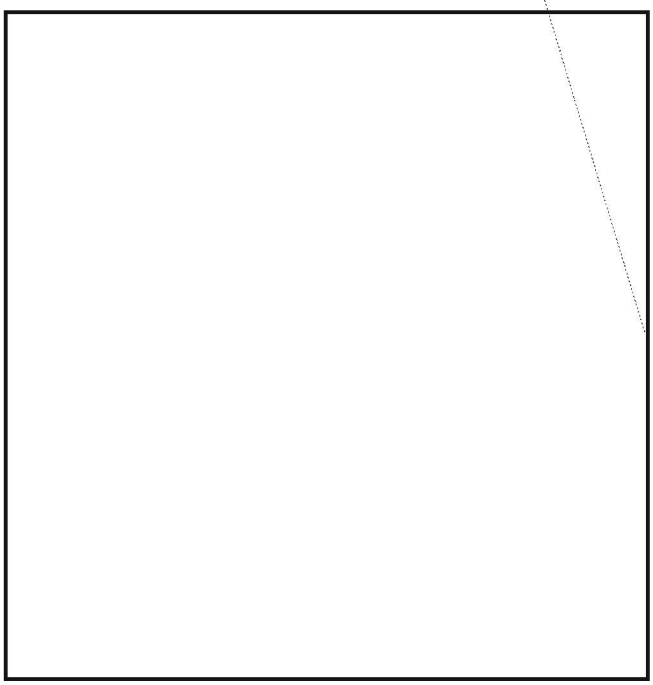


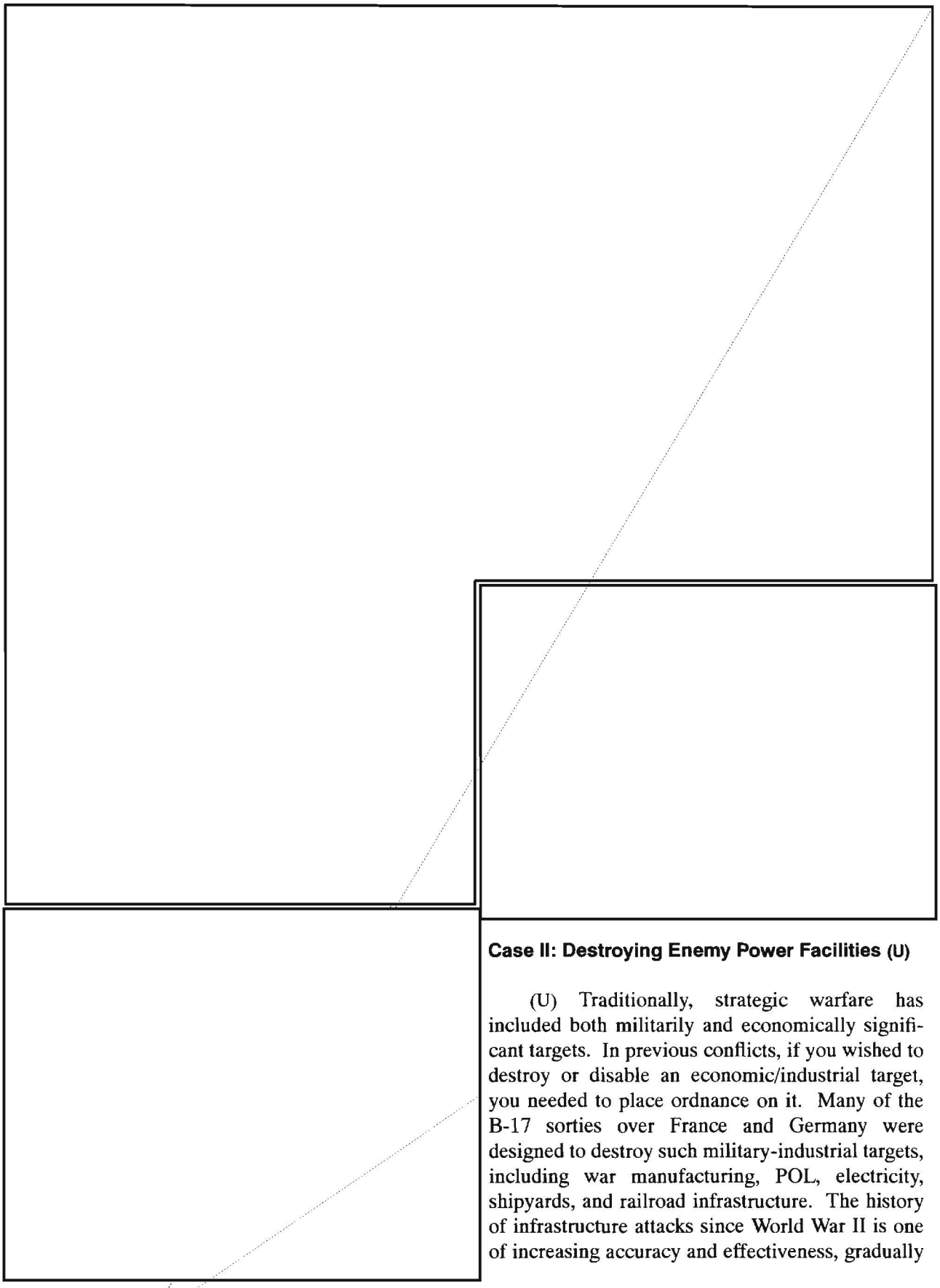
This "Smash and Jam" approach to overcoming air defenses continues to the present day.

(U) Perhaps the closest approximation to overcoming the Soviet air defenses (albeit with conventional weapons) took place in December 1972 during the JCS Operation LINEBACKER II. This round-the-clock bombing operation, involving the then top-of-the-line B-52 and F-111, targeted facilities in North Vietnam in some of the most heavily defended areas of the world. The strike operation was supported by a massive array of support operations involving tactical aviation establishing chaff corridors, performing standoff jamming, as well as active counter-SAM missions by F-4C Wild Weasels and F-105G Iron Hand missions, equipped with anti-radiation missiles (ARM). The combination of soft (ECM) and hard (ARM, iron-bombs) kills was very effective. During the 11 days of the operation, the North Vietnamese launched over 1,000 SA-2 missiles. Out of 724 B-52 sorties, a total of 15 aircraft were lost, for a loss rate of 2.1 percent. Fourteen tactical aircraft were lost in the same period. Another way of looking at these results is that in 11 days of operations, North Vietnam, a well-armed but distinctly Third-World country, had downed 7.4 percent of the participating B-52s, the U.S.'s most capable strategic bombers, putting the lives of 92 SAC crew members at risk.

(U) This combination of hard and soft kill was taken to a new level in DESERT STORM. Air defenses were the first targets engaged when Special Operations Forces and Stealth neutralized early warning and reporting positions on 17 January 1991, followed quickly by telecommunications, leadership, and command and control targets. Ultimately, some 630 sorties were flown against the French-built KARI system — the "nervous system" of the air defense forces to destroy the sector and interceptor operations centers as well as the reporting and listening posts. The EW dimension was stepped up as well: coordinated, preemptive jamming was performed in conjunction with air-launched decoys and ARM-equipped Wild Weasel F-4Gs and F/A-18s. As a consequence of the destruction of the air defense network (as well as the rest of the Iraqi command and control system), the Coalition lost a total of only 38 aircraft and 48 damaged over the period 17 January through 28 February, against an average of 2,140 daily sorties. (Seventy-one percent of those losses were attributable to AAA and IR SAMs.)

EO 1.4.(c)
P.L. 86-36





Case II: Destroying Enemy Power Facilities (U)

(U) Traditionally, strategic warfare has included both militarily and economically significant targets. In previous conflicts, if you wished to destroy or disable an economic/industrial target, you needed to place ordnance on it. Many of the B-17 sorties over France and Germany were designed to destroy such military-industrial targets, including war manufacturing, POL, electricity, shipyards, and railroad infrastructure. The history of infrastructure attacks since World War II is one of increasing accuracy and effectiveness, gradually

reducing the number of sorties required to achieve required levels of damage. IW extends this logic by making possible infinitely scalable, infinitely accurate strikes on infrastructure targets by means of cyber-attacks on the information infrastructure needed to operate it (hence the term Information Infrastructure Warfare, I^2W).

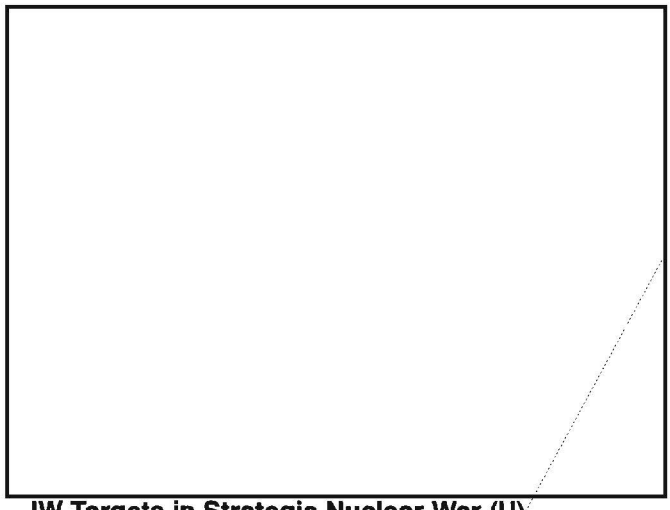
(U) Recalling the strategic bombing campaign against North Vietnam in December 1972, Operation LINEBACKER II, three separate electrical power sites were listed among the strategic targets. The Thermal Power facility at Thai Nguyen was the target of 42 B-52 sorties with a total of 2,185 bombs. The Haiphong Transformer Station was the target of 14 B-52 sorties involving 840 bombs. In addition, 6 F-111 sorties with 72 bombs were ordered on the Hanoi Transformer Station, along with 28 F-4 sorties (245 bombs) and 32 A-7 sorties (348 bombs). Thus, to cripple the North Vietnamese power grids, 122 sorties were conducted dropping some 3,690 bombs on three sites.

IW attacks on a target nation's power facilities are made possible by the growing reliance of the power industry on digital communications and data transmission.

(U) DESERT STORM strike planners mounted an energetic and sophisticated campaign against the Iraqi power system. The grid comprised some 25 major power generating stations and 140 uncollocated transformer stations. While planners had intended to minimize long-term damage to the economic infrastructure (to reduce post-war recuperation time), the majority of the 25 major power stations were struck. Three hundred forty-five strikes were delivered on power grid targets, including 60 TLAM attacks, and including carbon-filament dispensing attacks which were used to ground out power transmission lines. Ultimately, just under 88 percent of Iraq's generating capacity was sufficiently damaged or destroyed, or separated from the national grid making it unavailable.

(U) The IW approach to attacking a target nation's power generating and transmission facilities is made possible by the growing reliance of the power industry on electronic communications methods and digital data transmission for remote operation, monitoring, and supervision.

(U) Almost all modern supervisory control systems are computer-based, and consist of a master unit and remote terminal units (RTUs). The master unit is a computer with input and output equipment necessary for transmitting control messages to the RTUs and receiving information from them. The remote units are located at selected stations and are themselves increasingly capable mini- or microcomputers, programmed to perform essential functions. The RTUs are equipped with modems so that they can accept messages from the master and signal that the message has been received and the function carried out. Such functions include opening or closing selected control circuits, monitoring load limits and other system parameters, and alarming when an emergency state is detected. In addition to performing the necessary control functions, the SCADA can provide complete logs of the operation of the portion of the system under its surveillance.

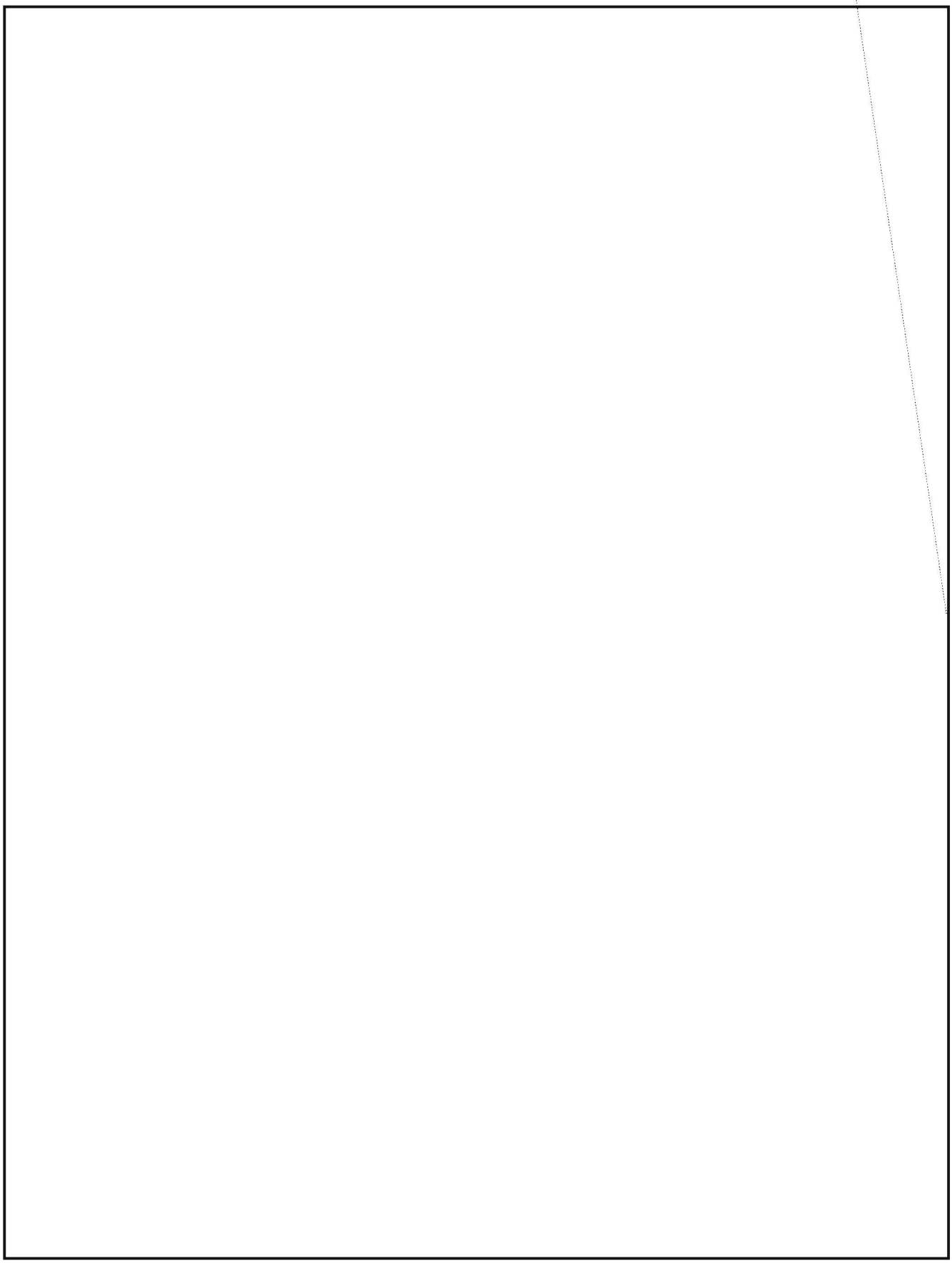


IW Targets in Strategic Nuclear War (U)

~~TOP SECRET UMBRA~~

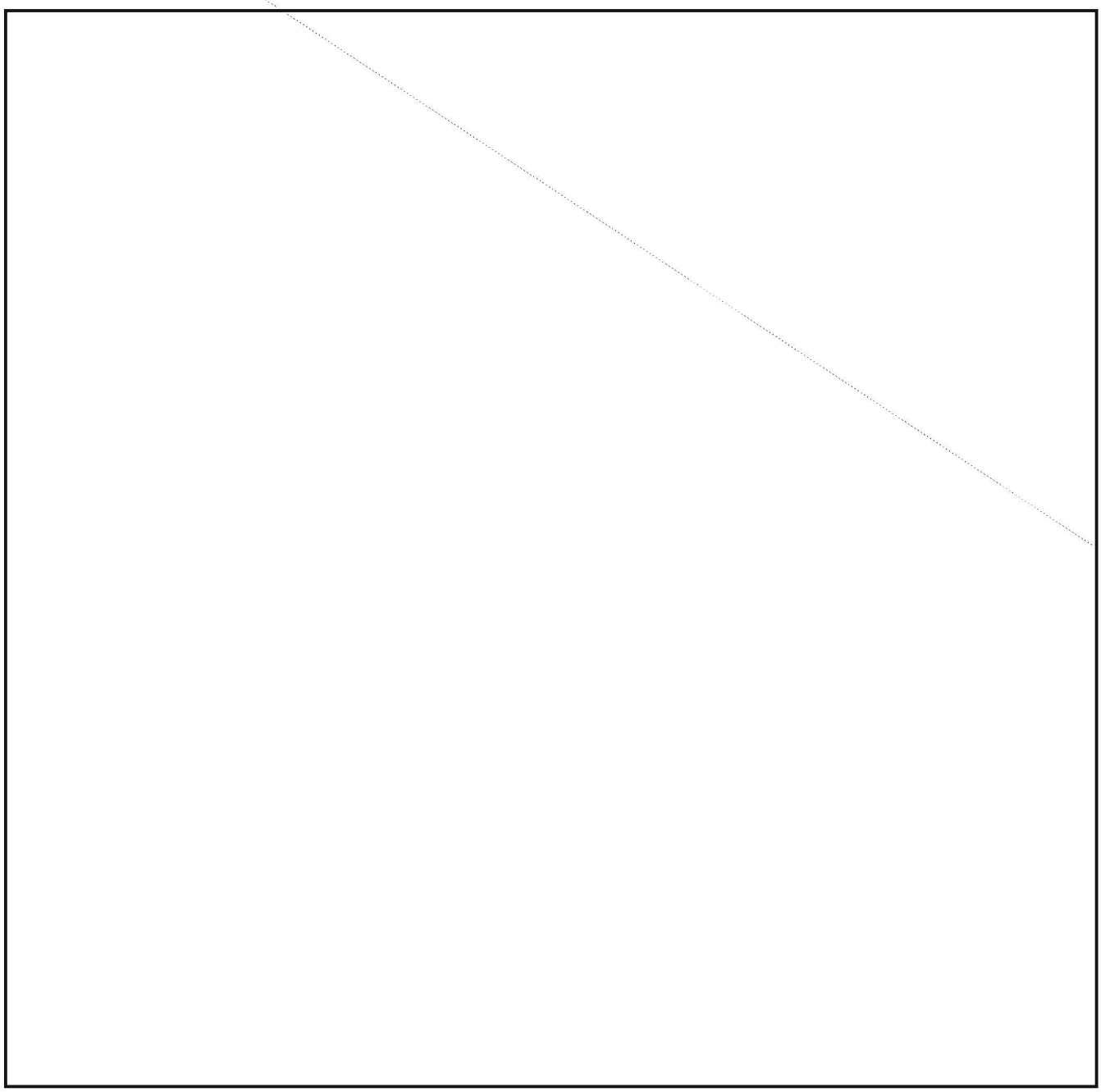
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

WHY IW? (U)



NOTE ON SOURCES

(U) In addition to serialized SIGINT reporting, the following sources were consulted during the drafting of this piece: details on LINEBACKER II were provided in Karl J. Eschman, Linebacker: The Untold Story of the Air Raids Over North Vietnam. New York: Ivy Books, 1989. Material on the air campaign in DESERT STORM was derived from Thomas A. Keany and Eliot A. Cohen, Revolution in Warfare? Air Power in the Persian Gulf. Annapolis, Md.: Naval Institute Press, 1995., as well as from Alan D. Campen, ed., The First Information War. Fairfax, Va.: AFCEA International Press, 1992. Information about DELIBERATE FORCE came from Lessons and Implications from the U.S. Air Operations in the Former Yugoslavia 1992-1995 3 Vols. (SECRET) Institute for Defense Analyses Report Number R-397. Alexandria, Va.: IDA, 1996.

Kλ

~~SECRET~~

Thoughts on a Knowledge Base to Support Information Operations in the Next Millennium (U)

by [redacted]
P.L. 86-36

(U) Tackling the information age challenges, focusing the Agency's combined efforts and coordinating a variety of activities, is no small chore. Key to keeping everything straight and aligning our resources is a central repository with which to collaboratively manage the combined intellectual capital that will fuel our nation's Information Operations in the next millennium.

A Notional IO Knowledge Base (U)

Does this mean we need yet another database? Not quite.

(U) Intellectual capital? Central repository? Does this mean we need yet another database? Not quite. Rather, we need a mechanism to collectively view relevant information and knowledge which is currently dispersed, fragmented, overlapped, and incomplete. It's best to think of this knowledge base as more of a management construct — a way to view our collective state of knowledge, understand key relationships, glean insights from linkages, and visualize gaps — dynamically, as a process that continually evolves. We can then use these insights to drive a number of communities, organizations, and even individuals to fill those gaps with information, intelligence, analysis, tools, and techniques.

(U) The Information Operations knowledge base is best described as a series of "templates." A template is simply a layer of information — information that, when combined with other layers, allows you to enhance your understanding of a situation, answer tough questions, and make trade-off decisions. At this point, we envision about nine distinct templates that, when combined together, form a very powerful and essential tool for the effective prosecution of any information operation.

(U) Let's take a look at each of these layers. A graphic representation (see figure 1) will aid in the understanding as we go along.[1] As we discuss each template, keep in mind that the contents of this knowledge base can be utilized for both the planning of offensive operations (i.e., exploit and/or attack) as well as to assess an adversary to support defensive or counter-information operations activities. Therefore, the contents in each template represent, in many cases, both "ours" and "theirs." Different portions of the knowledge base would be used at any given time, depending on whether we are supporting the development of our own operational capacity or developing an understanding of our adversary's.

1. You may notice an older version of this graphic in the Joint Staff's First Draft of Joint Pub 3-13, Joint Doctrine for Information Operations (IO) on page V-6. The original concept was developed based on work NSA performed in support of a customer IW exercise and was basically the culmination of lessons learned while categorizing the threat and vulnerabilities. The templating approach immediately highlighted the offense/defensive synergy and was further adapted to assist the customer in understanding the level of knowledge required to support their evolving IO planning process.

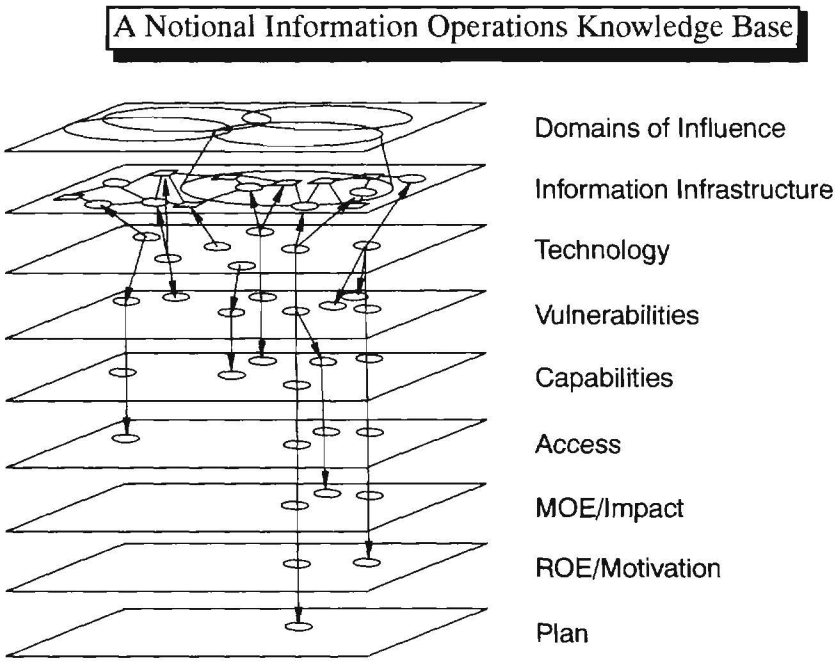


Figure 1 - Templating IO Planning & Assessments

DOMAINS OF INFLUENCE (U)

(U) At the top most level, we are trying to understand how the U.S., its allies and its adversaries, to include non-nation elements, operate. Societies and groups logically disaggregate into economic, political, social, military, and infrastructure segments or sub-systems. Without a fundamental understanding of how various segments function, we have little hope of efficiently exploiting or influencing adversaries through manipulation of their underlying information infrastructures. Likewise, if we don't fully understand our own operations, we'll never be able to assess operational impact and therefore be incapable of making informed risk management decisions. This is by far the most difficult layer of the model to conceptualize. Because of its scope, capturing the subtleties of how the various systems and sub-systems of a society operate and interrelate is enormously complex.

(U) This scope can be limited, however. From an offensive perspective, the current craze in "information warfare" wargaming is crucial. It is through these sessions, realistic operational scenarios will emerge to feed the development of operational requirements which will limit the scope of analytic efforts. On the defensive side, the President's Commission on Critical Infrastructures[2] is likewise essential. Their study will define a reasonable, critical subset of the National Information Infrastructure, which can be used to identify and

2. Executive Order 13010 established the Presidential Commission on Critical Infrastructure Protection on 16 July, 1996. In that document the President observed "Certain national infrastructure are so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United States." He noted that the battlespace will be global, threats are of both of a physical and cyber nature, the homeland's sanctuary cannot be assumed and the distinction between military and economic targets may disappear.

develop necessary public/private sector relationships, and effectively limit data gathering and analytic efforts.

(U) The population of this template requires we use various subject matter experts and those familiar with local culture, customs, and perspectives. We should take a page from the concept of operations at the Joint Warfare Analysis Center (JWAC), in Dahlgren, VA, who have evolved a very effective approach — hiring subject matter experts from key industries (power, gas, petroleum/oil/lubricants, telecommunications) and utilizing country teams — to perform focused weapon/target trade-off studies. We need to scale this approach up a notch above the industrial age's physical infrastructures and threats to view and document entire segments of societies (i.e., economic, political, military, and social). HUMINT plays the main role here as well as insights from Department of State, academia, and more and more as companies go global, industry.

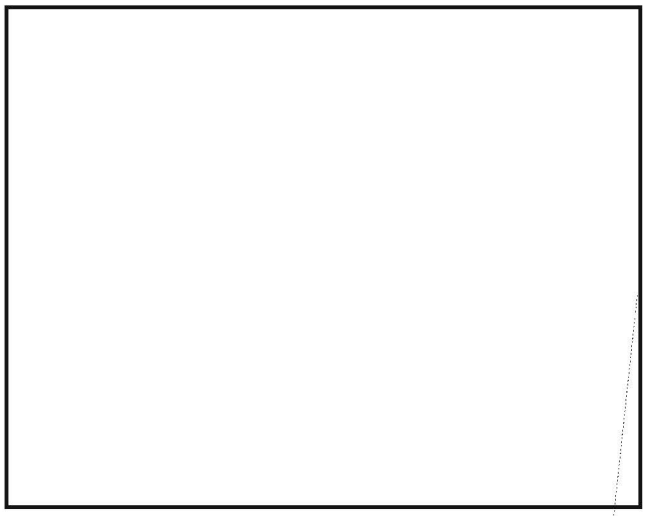
With technology life spans of a mere six to eighteen months, the global information environment moves too quickly for us to keep up our traditional target-chasing mode

(U) After the scope is defined, the most difficult obstacle will be developing a mechanism to capture the intellectual capital of these subject matter experts. This will allow rapid revision and verification, subsequent interrogation, and the establishment of linkages to the lower levels in the model — specifically to the information infrastructure template and the measures of effectiveness/impact template.

INFORMATION INFRASTRUCTURES (U)

(U) Once we understand key "customer" or "target" operations, we need to understand how those functions are supported by information, information systems, and information based processes. In other words, what hardware, firmware, protocols, operating systems, and software are being used where, to perform what functions, and for whom? This template will accumulate as much information, from as many sources as possible, to depict those portions of the global information environment that are relevant to domains of influence where we have an offensive or defensive interest.

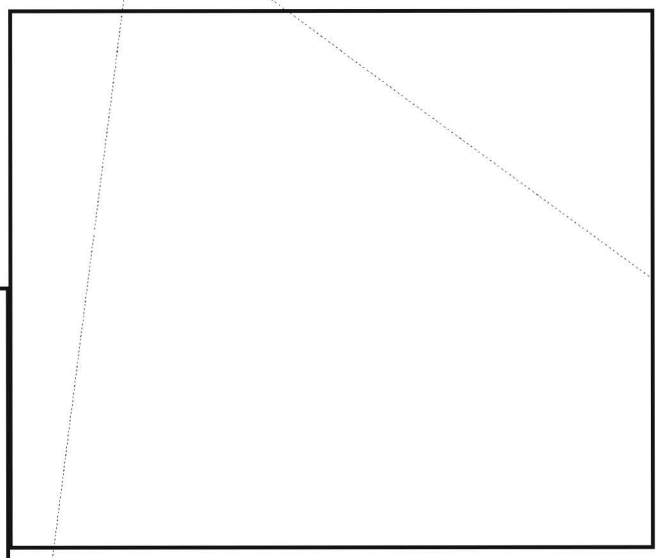
(U) The information infrastructure template is then used to track fielded information technologies, not to drive the development of capabilities, but to look for opportunities to make use of offensive and defensive capabilities that we should already have developed.

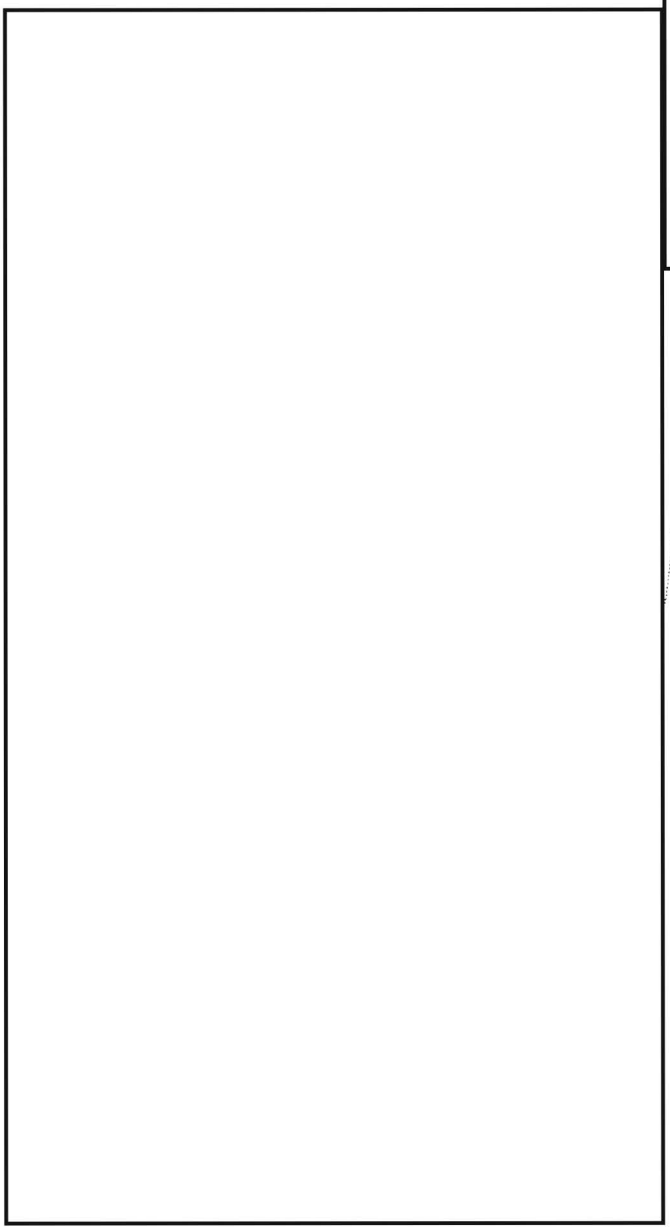


(U) Unfortunately, today, with technology life spans of a mere six to eighteen months, the global information environment moves too quickly for us to keep up with our traditional target chasing mode. The INFOSEC community recognized this a few years ago noting that chasing customer systems, or targets, to add security on after the fact was a losing proposition. Customer dependence on commercial technologies increased the rate at which fielded technologies became obsolete.

EO 1.4.(c)
P.L. 86-36

Increased security requirements demanded an understanding of underlying customer operations. The INFOSEC community responded with an Information Systems Security Engineering (ISSE) approach and various process assurance initiatives to "build security in up front" and get ahead of their "target."





(U) In addition to intelligence activities, engineering analysis plays an important role in the population of this section of the knowledge base. Clearly some of the best talent with which to perform the requisite engineering analysis lie in our support organizations — where experts gain operational insights through the hands-on design, installation, operation, and maintenance of our own systems. These experts must become full partners in the maintenance of this knowledge base, not only to document our own infrastructure but to assist in the analysis of our adversaries in order to fill critical gaps which cannot be obtained by other means. To accommodate this "non-traditional" source and adequately support decision making processes, the template must document what is known and what is postulated.

~~(S)~~ Finally, we must seek out HUMINT sources who have intimate design or working knowledge of key systems and networks. System users and operators are a potentially rich source of insight into the detailed information infrastructure data we require — if we can train the system to recognize their potential, ask the right questions, and then capture and catalog those contributions.

TECHNOLOGY (U)

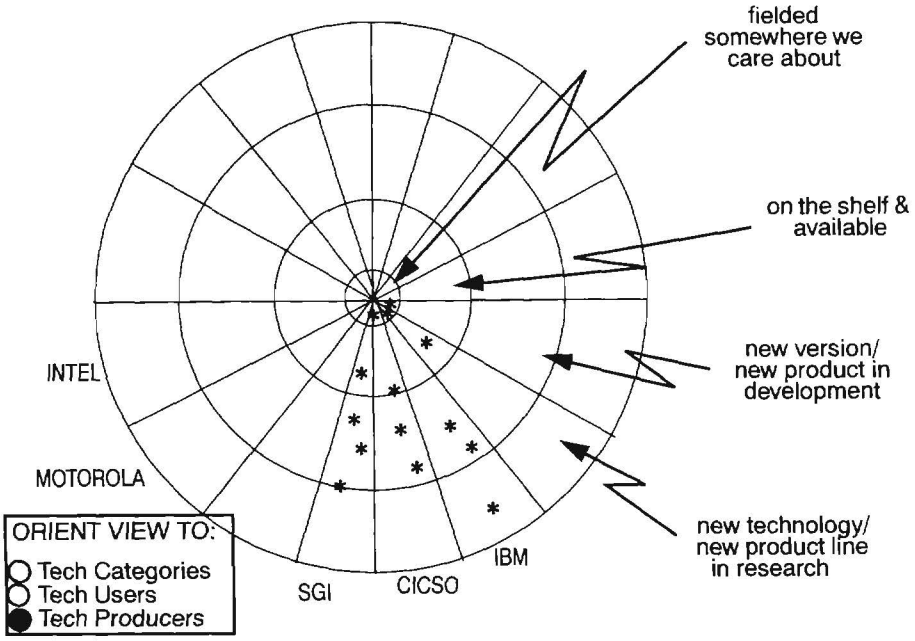


Figure 2. The Technology Radar

(U) In this section, we'll review the technology template. This template must catalog existing and emerging information technologies showing what's on the shelf, what's soon to be on the shelf, and what's a twinkle in some engineer's eye. In order to stay ahead of our targets, we must continuously monitor the information technology market from both a broad and deep perspective and establish a "technology radar" (see Figure 2) that will provide insights into new releases, new products, and new technologies before they hit the commercial shelf and more importantly before they are deployed into the target environment. Note the inner ring of the radar would actually be the information infrastructure template we discussed in the previous section.

(U) The various "range rings" on the radar require very different skill sets to perform the necessary assessments. As we discussed in the previous section, the inner ring requires the combined skills of intelligence analysts and technicians to map the target. The second ring, documenting available technology and assessing high payoff items, will require the skills of a market researcher or consumer trends analyst. The third ring, to project upcoming product releases and new product lines, will require the collaboration of production and applied research engineers, familiar with industrial capabilities, methods, and motives. Finally, the very outer ring, to identify research, determine its relevance, and understand its implications, will require the analytic perspective of core scientists and advanced researchers.

(U) Basically, the goal is to, as accurately as possible, place the "blips" on the radar and determine which are vectoring towards the center at what speeds. If we can track the information technology market in this manner, we will have the knowledge we require to begin to "chase the technologies" instead of "chasing the targets." We will be in a position to make a decision, based on understanding of market trends and customer and adversary acquisition habits, whether we need to send out an "interceptor" to work that technology target or whether we can watch it and hope the blip goes dim before it reaches the center of the screen.

~~(S)~~ Currently, we have a number of efforts across the Agency, and others, to identify and document technology trends and produce technology forecasts. These efforts do not draw a distinction between the outer two rings. They are often spot solutions, focusing on specific technologies, and specific points in time. The output is usually a briefing or hardcopy report. Our technology assessment efforts need to move towards a continual process, distributed across the workforce, with the objective of continually evolving a workable taxonomy with which to map technology evolution relevant to our targets of interest.

VULNERABILITIES (U)

(U) Some say vulnerability analysis is an art, other say it's a science. Regardless, we can agree that it does require a unique skill set — a skill set that is the core competency of the information operations community. Individuals across the community with these unique skills are very limited. By tracking the technology in a technology template and the global information environment in the information infrastructure template, we are in a position to make informed decisions to efficiently allocate scarce skilled vulnerability analysts. The results of their efforts, as well as the compilation of vulnerability information for others, will constitute the vulnerability template.

One unofficial survey within NSA listed some eighteen separate organizations who were collecting vulnerability information in one form or another!

(U) Increasingly, organizations are interested in accumulating vulnerability data to support their objectives. There are a number of computer response activities, industry collaboration groups, and elements of the intelligence community and military services working both offensive and defensive angles. Without exception, all recognize the need to track vulnerabilities in some central place and are striving to exchange data. However, there are practical problems.

~~(S)~~ Very few centers exist for the actual derivation of vulnerabilities. Most are identified, involuntarily, by end users, and gathered by computer emergency response activities who serve as conduits between their constituencies and the information technology providers. In order to maintain the support of the technology providers, vulnerabilities are treated by the company as proprietary information, with limited distribution, until they are resolved. Some are identified by industry experts themselves and shared, under strict rules of disclosure in forums like the National Security Information Exchange (NSIE).

(U) As you can see, the practical problem is classification. Companies wish to maintain consumer confidence and their competitive advantage. Computer response activities want to continue dialogs with industry in order to help their constituencies. Professional assessors want to maintain client confidentiality to bolster references. Intelligence operatives wish to protect sources and methods.

(U) To date, the answer to this problem has been to create a number of "central places" for vulnerability data. Just as an example, one unofficial survey within NSA listed some eighteen separate organizations who were collecting vulnerability information in one form or another! Without a macro view of the situation, it is difficult to formulate a workable solution. No one really knows how much unique knowledge exists in each sector.

(U) A large-scale national Information Operations capability obviously requires a macro view of the vulnerability situation. The only hope is that classification issues can be overcome by separating the technology from the operations and working vulnerabilities with a technology focus at some rather high system level. Only with this macro view could the community focus its limited resources, adequately assess threat and operational risk, and balance the offensive and defensive issues in an equitable fashion.

EO 1.4.(c)
P.L. 86-36

CAPABILITIES (U)

(U) Capabilities will leverage vulnerabilities singularly or, more likely, in combinations to exploit, deny, or manipulate target information systems. This template will catalog the various "tools" available to perform cyber operations. Two major issues impede our efforts in this area. First, from an offensive perspective, a single community wide "toolbox" will carry with it a significant compartmentation issue. Secondly, from a defensive perspective, the identification of adversary capabilities is very difficult.

~~(S)~~ Today, the tools are developed by a number of different organizations for a variety of purposes. The majority of these efforts are very

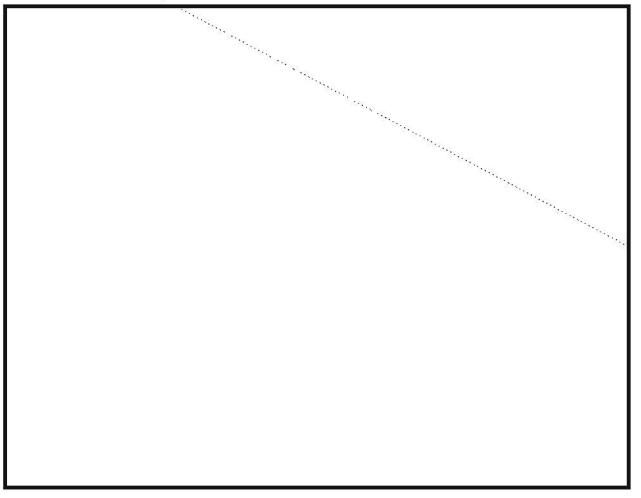
(U) Tackling the defensive issue is a bit more difficult. Today, our approach to assessing adversary capability is rooted in an industrial age mindset. We attempt to identify adversary "IW" capabilities in the same manner in which we have tracked the proliferation of traditional industrial age weapons of mass destruction (i.e., Nuclear, Biological, Chemical weapons). The problem is that the development of an information age weapon of mass corruption has very few observables, especially in the buildup phase.

ACCESS (U)

(U) Simply possessing a capability to exploit a particular computer system does not necessarily mean that the capacity can be used in any productive manner. Access, proximal or remote, is required to "deploy" a capability to its desired target. The logical analogy from the past would be possessing nuclear warheads but no missile or bomber to deliver the warhead to a target.

~~(S)~~ Some might see access as simply another dimension of the capability. It was purposely separated into its own template in order to draw attention to its importance. From an offensive perspective, access is the most difficult ingredient in the recipe for cyber operations. Many of the postulated capabilities used in today's exercises and wargames simply assume access will be available, usually provided by the Intelligence Community. That perception must be countered. As we work to devise realistic scenarios with which to drive operational requirements, we must force the operational community to think about the need for both capability and access. Likewise, our technologist's efforts must be constrained by the need for access as well. Much of what we do in this arena today is characterized as "technology push" — we develop a capability because we can. Requiring attention to the access dimension will keep us from expending energy developing weapons for the cyber ops arsenal which could never be deployed.

EO 1.4.(c)
P.L. 86-36

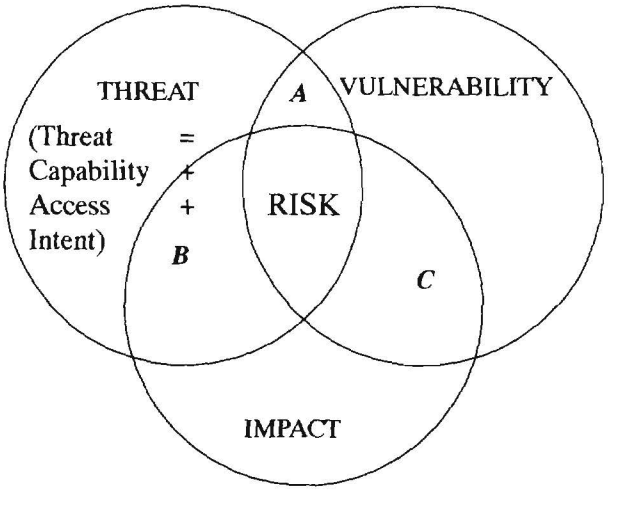


the offensive community to perform some quantitative analysis or assessment of the effects of deploying a specific capability. The defensive world has called this "impact assessment." Clearly, these assessments have to be based on a detailed technical understanding of the interrelationships in the information infrastructure. However, they must be expressed in terms of the net effect to the domain which the operation intended to influence. This is a job requiring significant modeling and simulation capabilities. In fact, this template is envisioned to contain the models and simulators required to perform these offensive and defensive assessment. The actual information to feed these tools would come from the layers above.

IMPACT/MEASURES OF EFFECTIVENESS (MOE) (U)

(U) Okay, we now have an understanding of the circumstances when certain capabilities would likely be used to take advantage of vulnerabilities in the base technologies deployed in the target environment. We still do not have the answer to the "so what?" question. In essence, the term "measures of effectiveness" has been devised by

(U) On the defensive side, risk is traditionally depicted as the intersection of vulnerability, threat, and impact (see Figure #3). Many use the words vulnerability, threat, and risk interchangeably and tend to overlook or inadequately estimate impact. With limited resources in terms of both manpower and dollar to attack residual risk, an ability to estimate or model optional impact will greatly enhance our ability to focus our countermeasure efforts on those areas where they are most needed.



A: vulnerabilities threat can exploit but have no operational impact

B: if vulnerability exists, threat could have impact

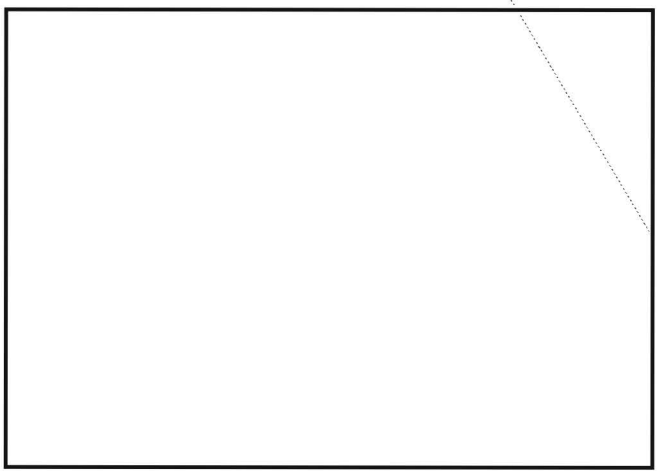
C: vulnerabilities with impact that threat cannot exploit

Figure 3. Risk

(U) As we attempt to look at entire infrastructures and large systems of systems which support entire domains of influence, the level of sophistication in our models rapidly exceeds anything we've attempted before. Cascading effects in both the information infrastructures and the domains of influence will be the norm as interdependencies continue to increase. In addition, the amount of detailed information and computational power required to support simulations of those models is immense.

RULES OF ENGAGEMENT/ MOTIVATION & INTENT (U)

EO 1.4.(c)
P.L. 86-36



(U) On our side, once moral and ethical issues are resolved, rules of engagement for cyber operations become a policy and coordination challenge more than anything else. The major challenge, from a coordination perspective, lies in the convergence of the strategic, operational, and tactical levels these type operations necessitate. In information-age, cyber-operation scenarios envisioned for the next millennium, it is very difficult to discern the strategic from the operational from the tactical in either a targeting, tactics, or decision making sense. The concepts for utilization of the "Bit Bomb," the "weapon of mass corruption" for the information age, might best be considered as similar to those devised for the Atomic Bomb, the weapon of mass destruction from the industrial age. Very stringent policies, highly coordinated practices, and central-release authority may be required. In fact, experiences from today's information warfare games and exercises seem to indicate that information warfare might best be played solely at the strategic level, separately and distinctly from traditional military operations.

(U) Regardless, we need to ensure that we capture the insights we glean from intelligence regarding adversary intent, as well as our own evolving "rules of engagement" to ensure we can adequately model and simulate information operations and support our operational planning and risk management processes.

(U) The representation of this information takes on an almost Artificial Intelligence-like, rules-based, expert-system form in order to represent complicated, compound, conditional assertions, like:

> ***"If leader X perceives an information-based attack on its financial infrastructure, and the state of relations between country X and the U.S. is best characterized as highly competitive but moving rapidly towards crisis, and depending upon the outcome of diplomatic negotiations over issue I, then leader X will most probably retaliate with the deployment of capability C, via access mechanism A, against U.S. infrastructure target T with the expected outcome of O."***

(U) As you can see, the articulation of intent is very difficult — conditional on a number of facts, hypothesis, and dependencies. To date, the best method for developing these assessments has been via prose documentation of probable scenarios based on a limited understanding of adversary capability and intent. On our side of the game, the Rules of Engagement are even more difficult to articulate! The state of the art must be improved in order respond to requests for information and assessments and to maintain the incredibly high operations tempo envisioned as we move towards an active defense.

OPERATIONS (U)

(U) We finally come to the bottom line. If we've done our homework against a specific adversary, we should come up with a list of those capabilities that we can deploy that will take advantage of vulnerabilities that exist in the adversary's information infrastructure to accomplish some level of influence over the target domain — in other words, a viable plan.

(U) Likewise, if I look at the opposite sides of the templates I should see a picture of the most probable scenarios that an adversary would run against a given segment of our society — in other words, a reasonable approximation of their plan.

CONCLUSION (U)

(U) Clearly, the National Security Agency houses a major portion of the intellectual capital discussed in the previous sections. However, the NSA cannot be the sole contributor to this knowledge base. As a community, we must develop the knowledge and expertise required to populate and maintain this knowledge base with which to manage and support a sustainable and superior national information operations capability. It is only through the collective management of our combined intellectual capital that we can maintain our nation's security in the cyberspace environment.

Kλ

~~SECRET~~

Information Operations Training (U)

by [redacted] P.L. 86-36

~~(C)~~ The end of the Cold War has brought many new focuses and challenges to the Intelligence Community. The worldwide proliferation of sophisticated computer technology, the modernization of communications in traditionally less-developed nations, and the resultant increased global connectivity combine to present a whole new intelligence concern: the capability of nearly any foreign entity to exploit or attack the information systems of the United States or its allies.

~~(S)~~ Executive Order 13010, which established the Presidential Commission for the Protection of Critical Infrastructure, coupled with Presidential Decision Directive 35 revisions, which elevated Information Warfare to a Tier 1 issue for many countries, exemplify the growing senior-level concern of the foreign Information Warfare threat to the United States.

~~(S)~~ In response, the SIGINT Requirements, Validation, and Evaluation Subcommittee (SIRVES) validated six new National SIGINT Requirements (NSRs) to support the growing needs of the customers for data to support Information Operations. These NSRs put demands on analysts to produce unique intelligence reports in a new area. To meet these demands, analysts must first understand just what Information Operations is and how intelligence can support it.

~~(C)~~ In response to DDO tasking, the Information Warfare Support Center led the effort to develop National Cryptologic School (NCS) courses IS-231 and IS-232. With support from the DO, DS, and DI organizations, the courses, while designed with SIGINT intelligence analysts and reporters in mind, have a broad enough perspective to be useful to those in other disciplines and organizations. In fact, IS-232 has been in high demand both inside and outside the SIGINT community.

~~(S)~~ IS-232 Information Operations Awareness is a three-hour seminar intended to provide a basic understanding of Information Operations and how intelligence can support it. The course covers the following:

- Defining IO
- IO Conceptual Framework
- Potential Indicators of IO activity
- IO Enabling Technologies
- IO Techniques
- Foreign Information Warfare
- IO Reporting

~~(FOUO)~~ So, in a nutshell: What is it? How to identify it? and What to do with once it has been identified?

P.L. 86-36

~~(FOUO)~~ To date, IS-232 has been presented to [redacted] throughout the Agency and the services. It is currently being offered on an as needed basis to groups of 15 or more. Additionally, the modular design of IS-232 allows portions of it to be included in other curricula and in conferences, briefings, and working groups.

~~(S)~~ IS-231, Information Operations Reporting, a four-day class, was piloted in February 1997 with ten students from analytic, computer science and collection backgrounds. This course expands on the concepts presented in IS-232 and includes a number of practical exercises. After some revisions, the NCS plans to offer IS-231 on a quarterly basis.

[redacted]

P.L. 86-36

Kλ

~~SECRET~~