

Full Spectrum Information Warfare

Information Operation Roadmap Part 1

*Brent Jessop - [Knowledge Driven Revolution.com](http://KnowledgeDrivenRevolution.com)
November 5, 2007*



When the US military refers to full spectrum domination, they truly mean full spectrum. Information operations or information warfare is a key part of the military battlespace. Recently, a document entitled [Information Operation Roadmap](#) was declassified by the Pentagon because of a Freedom of Information Act request by the National Security Archive at George Washington University. The document [was described by](#) the Council on Foreign Relations' website as:

"A 2003 Pentagon document previously classified as 'noform' (not for release to foreign nationals, including allies), this report details the US military's information operations, including psychological operations, electronic warfare, and involvement in foreign journalism. The document was made public by the National Security Archive on January 26, 2006."

On Par with Air, Ground, Maritime and Special Operations

The importance of information warfare is clearly laid out in this document.

"Key assumptions. Information, always important in warfare, is now **critical to military success** and will only become more so in the foreseeable future. Three key assumptions underscore the growing importance of information:

- (U) Effectively communicating U.S. Government (USG) capabilities and intentions is an important means of combating the plans of our adversaries. The ability to rapidly disseminate **persuasive information to diverse audiences in order to directly influence their decision-making** is an increasingly powerful means of deterring aggression." [emphasis mine] - 3

The major thrust of the document was that information operations should be centralized under the Office of the Secretary of Defence and made a core military competency.

"Objective: IO [information operations] becomes a core competency. The importance of **dominating the information spectrum** explains the objective of **transforming IO into a core military competency on a par with air, ground, maritime and special operations**. The charge to the IO Roadmap oversight panel was to develop as concrete a set of action recommendations as possible to make IO a core competency, which in turn required identifying the essential prerequisites to become a core military competency." [emphasis mine] - 4

Uniformity in Message and Themes

The major reason for centralizing the information operations under a single command was to create consistency between the various segments of the Pentagon's information operations.

"IO requires **coordination** with public affairs and civil military operations to complement the objectives of these related activities and **ensure message consistency**." [emphasis mine] - 23

"- (U) The USG [US Government] can not execute an effective communication strategy that facilitates military campaigns if **various organs of Government disseminate inconsistent messages** to foreign audiences. Therefore, it is important that policy differences between all USG Departments and Agencies be resolved to the extent that they **shape themes and messages**."

- (U) **All DoD [Department of Defense] information activities, including information operations**, which are conducted at the strategic, operational, and tactical level, should reflect and be **consistent with broader national security policy and strategy objectives.**" [emphasis mine] - 25

"Coordinating information activities. Major DoD "information activities" include public affairs, military support to public diplomacy and PSYOP [psychological operations]. The State Department maintains the lead for public diplomacy, the [half line redacted] and the International Broadcasting Board of Governors maintains the lead for broadcasting USG messages overseas, often with DoD in a supporting role. DoD has consistently maintained that the **information activities of all these agencies must be integrated and coordinated to ensure the promulgation of consistent themes and messages.**" [emphasis mine] - 25

A Trained and Ready Career Force

With the ascension of information operations into a core military competency the document recommended, under the heading "A Trained and Ready Career Force" that the:

"DoD [Department of Defence] requires a cadre of IO professionals capable of planning and executing fully integrated IO in support of Combatant Commanders. An IO career force should be afforded promotion and advancement opportunities commensurate with other warfighting areas and provided opportunities for advancement to senior executive or flag level rank." - 32

Support

The forward of this document was signed by then Secretary of Defence Donald H. Rumsfeld which contained the following statement of support:

"I approve the Roadmap recommendations and direct the Services, Combatant Commands and DoD Agencies to fully support implementation of this plan." - iv

What Are Information Operations?

This document defined information operations as follows:

"The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decisions-making while protecting our own." - 22

The following series of articles will examine the Pentagon's intention of gaining full spectrum dominance in information warfare. Including, [dominating the electro-magnetic spectrum](#) and [fighting the internet](#). Also, I will expand on the use of [psychological](#)

[operations or PSYOP](#) as defined by the *Information Operation Roadmap* and [if any limits exist in information warfare](#).

Maximum Control of the Entire Electro-Magnetic Spectrum

Information Operation Roadmap Part 2

Brent Jessop - [Knowledge Driven Revolution.com](http://KnowledgeDrivenRevolution.com)
November 12, 2007



In 2003, then Secretary of Defence Donald Rumsfeld signed a document called the [Information Operation Roadmap](#) which outlined, among other things, the Pentagon's desire to dominate the entire electromagnetic spectrum.

If you are unfamiliar with this document, more detail can be found in a previous article [here](#).

Dominate

From the *Information Operation Roadmap*:

"We Must Improve Network and Electro-Magnetic Attack Capability. To prevail in an information-centric fight, it is increasingly important that **our forces dominate the electromagnetic spectrum with attack capabilities.**" [emphasis mine] - 6

"Cover the full range of EW [Electronic Warfare] missions and capabilities, including navigation warfare, offensive counterspace, control of adversary radio frequency systems that provide location and identification of friend and foe, etc." - 61

"Provide a future EW capability sufficient to provide **maximum control of the entire electromagnetic spectrum**, denying, degrading, disrupting, or destroying the **full spectrum of globally emerging communication systems, sensors, and weapons systems dependant on the electromagnetic spectrum.**" [emphasis mine] - 61

"DPG [Defense Planning Guidance] 04 tasked USD(AT&L) [Under Secretary of Defense for Acquisition, Technology and Logistics], in coordination with the CJCS [Chairman of the Joint Chiefs of Staff] and Services, to develop recommendations to transform and extend EW capabilities, ... to detect, locate and attack the **full spectrum of globally emerging telecommunications equipment, situation awareness sensors and weapons engagement technologies operating within the electromagnetic spectrum.**" [emphasis mine] - 59

Stealthy Platforms Above Your House

"Develop a coherent and comprehensive EW [Electronic Warfare] investment strategy for the architecture that... Pay particular attention to:

- (U) Projecting electronic attack into **denied areas by means of stealthy platforms...** As a matter of priority, accelerates joint development of modular **EW payloads for the Unmanned Combat Aerial Vehicle.**" [emphasis mine] - 62

It is interesting to see the mention of stealthy platforms like unmanned aerial vehicles (UAVs) because they are now patrolling both [the Canadian](#) and [Mexican borders](#) of the United States and will soon be patrolling the [arctic](#). With funding supplied by Homeland Security, US police departments are also using UAVs to spy on the citizens below. A couple of examples are [Sacramento, California](#) and...

"one [North Carolina county](#) is using a UAV equipped with low-light and infrared cameras to keep watch on its citizens. The aircraft has been dispatched to monitor gatherings of motorcycle riders at the Gaston County fairgrounds from just a few hundred feet in the air--close enough to identify faces--and many more uses, such as the aerial detection of marijuana fields, are planned."

The Electronic Battlespace

"The ACTD [Advanced Concept Technology Demonstration] should examine a range of technologies including a **network of unmanned aerial vehicles and miniaturized, scatterable public address systems for satellite rebroadcast in denied areas**. It should also consider various message delivery systems, to include satellite radio and television, cellular phones and other wireless devices and the Internet." [emphasis mine] - 65

"Exploits other transformational EW initiatives, including use of the E-Space Analysis Center to correlate and fuse all available data that creates a **real time electronic battlespace picture**." [emphasis mine] - 62

How exactly do you create a real time electronic battlespace picture? And where exactly is the battlespace? A very similar statement was made in the Project for a New American Century document *Rebuilding America's Defenses* published in September of 2000 (more about this document [here](#) and [here](#).)

"New classes of sensors - commercial and military; on land, on and under sea, in the air and in space - will be linked together in dense networks that can be rapidly configured and reconfigured to provide future commanders with an unprecedented understanding of the battlefield." - pg 59

[An article](#) written by Mark Baard from [Parallelnormal.com](#) sheds some light on this subject.

"Philadelphia, San Francisco, Houston, and Providence, R.I. are among the cities partnering with private companies and the federal government to set up public broadband internet access. Providence used Homeland Security funds to construct a network for police, which may be made available to the public at a later date..."

"But even if the cities fail to complete their Wi-Fi projects, the military will be able to set up wireless networks within hours, perhaps even faster."

"The DOD [Department of Defense], which is in the middle of joint urban war-games with Homeland Security and Canadian, Israeli and other international forces, is experimenting with Wi-Fi networks it can set up on the fly."

"According to a recent DOD announcement for contractors, soldiers will be able to drop robots, called LANDroids... when they arrive in a city. The robots will then scurry off to position themselves, becoming nodes for a wireless communications network. (Click here to download a PDF of the DOD announcement.)"

"The Wi-Fi antennae dotting the urban landscape will serve not only as communications relays, but as transponders that can pinpoint the exact positions of individual computers and mobile phones - a scenario I described in the Boston Globe last year."

"In other words, where GPS loses site of a device (and its owner), Wi-Fi will pick up the trail."

"The antennae will also relay orders to the brain-chipped masses, members of the British Ministry of Defense and the DOD believe."

Conclusion

My next article will examine the Pentagon's desire to "[fight the net](#)" as outlined in the *Information Operation Roadmap*. Also, I will examine the use of [psychological operations](#) or PSYOP and highlight the [complete lack of limits](#) to the use of all these information operations, be it on domestic American or foreign audiences.

"We Must Fight the Net"

Information Operation Roadmap Part 3

Brent Jessop - [Knowledge Driven Revolution.com](http://KnowledgeDrivenRevolution.com)

November 19, 2007



[KDR: This article is available in French [here](#). Special thanks to Dany Quirion and Petrus Lombard for their efforts in translating this article.]

The Pentagon's [Information Operations Roadmap](#) is blunt about the fact that an internet, with the potential for free speech, is in direct opposition to their goals. The internet needs to be dealt with as if it were an enemy "weapons system".

The 2003 Pentagon document entitled the *Information Operation Roadmap* was released to the public after a Freedom of Information Request by the National Security Archive at George Washington University in 2006. A detailed explanation of the major thrust of this document and the significance of information operations or information warfare was described by me [here](#).

Computer Network Attack

From the *Information Operation Roadmap*:

"When implemented the recommendations of this report will effectively jumpstart a rapid improvement of CNA [Computer Network Attack] capability." - 7

"Enhanced IO [information operations] capabilities for the warfighter, including: ... A robust **offensive suite of capabilities to include full-range electronic and computer network attack...**" [emphasis mine] - 7

Would the Pentagon use its computer network attack capabilities on the Internet?

Fighting the Net

"We Must Fight the Net. DoD [Department of Defense] is building an information-centric force. Networks are increasingly the operational center of gravity, and **the Department must be prepared to "fight the net."**" [emphasis mine] - 6

"DoD's "Defense in Depth" strategy should operate on the premise that **the Department will "fight the net" as it would a weapons system.**" [emphasis mine] - 13

It should come as no surprise that the Pentagon would aggressively attack the "information highway" in their attempt to achieve dominance in information warfare. Donald Rumsfeld's involvement in the Project for a New American Century sheds more light on the need and desire to control information.

PNAC Dominating Cyberspace

The Project for a New American Century (PNAC) was founded in 1997 with many members that later became the nucleus of the George W. Bush administration. [The list](#) includes: Jeb Bush, Dick Cheney, I. Lewis Libby, Donald Rumsfeld, and Paul Wolfowitz among many other powerful but less well know names. Their [stated purpose](#) was to use a hugely expanded U.S. military to project "American global leadership." In September of 2000, PNAC published a now infamous document entitled *Rebuilding America's Defences*. This document has a very similar theme as the Pentagon's *Information Operations Roadmap* which was signed by then Secretary of Defense Donald Rumsfeld.

From *Rebuilding America's Defences*:

"It is now commonly understood that **information** and other new technologies... are creating a dynamic that **may threaten America's ability to exercise its dominant military power.**" [emphasis mine] - 4

"Control of space and cyberspace. Much as control of the high seas - and the protection of international commerce - defined global powers in the past, so will control of the new "international commons" be a key to world power in the future. An America incapable of protecting its interests or that of its allies in space or the "**infosphere**" will find it difficult to exert global political leadership." [emphasis mine] - 51

"Although it may take several decades for the process of transformation to unfold, in time, the art of warfare on air, land, and sea will be vastly different than it is today, and "combat" likely will take place in new dimensions: in space, "**cyber-space**," and perhaps the world of microbes." [emphasis mine] - 60

For more on *Rebuilding America's Defences* read [this](#).

Internet 2

Part of the *Information Operation Roadmap*'s plans for the internet are to "ensure the graceful degradation of the network rather than its collapse." (pg 45) This is presented in "defensive" terms, but presumably, it is as exclusively defensive as the Department of Defense.

As far as the Pentagon is concerned the internet is not all bad, after all, it was the Department of Defense through DARPA that [gave us the internet](#) in the first place. The internet is useful not only as a business tool but also is excellent for monitoring and tracking users, acclimatizing people to a virtual world, and developing detailed psychological profiles of every user, among many other Pentagon positives. But, one problem with the current internet is the potential for the dissemination of ideas and information not consistent with US government themes and messages, commonly known as free speech. Naturally, since the plan was to completely dominate the "infosphere," the internet would have to be adjusted or replaced with an upgraded and even more Pentagon friendly successor.

In [an article](#) by Paul Joseph Watson of [Prison Planet.com](#), he describes the emergence of Internet 2.

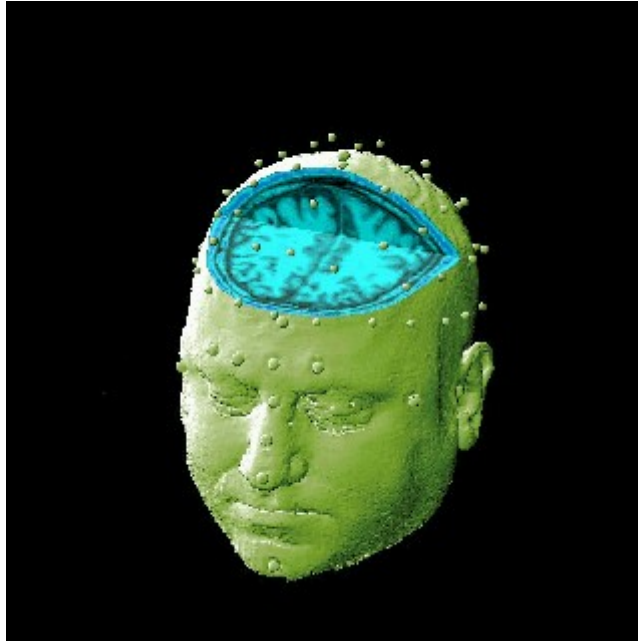
"The development of "Internet 2" is also designed to create an online caste system whereby the old Internet hubs would be allowed to break down and die, forcing people to use the new taxable, censored and regulated world wide web. If you're struggling to comprehend exactly what the Internet will look like in five years unless we resist this, just look at China and their latest efforts to completely eliminate dissent and anonymity on the web."

Conclusion

The next article will examine the Pentagon's use of [psychological operations or PSYOP](#) and the final article in this series will examine whether or not there are any [limits to using information operations](#) on the American public or foreign audiences.

Information Warfare Using Aggressive Psychological Operations

Information Operation Roadmap Part 4



The Pentagon's plans for psychological operations or PSYOP in the global information environment of the 21st century are wide ranging and aggressive. These desires are outlined in the 2003 Pentagon document signed by Donald Rumsfeld in his capacity as the Secretary of Defense called the [Information Operation Roadmap](#).

More detail about the origins and purpose of this document can be read in the first part of this series [here](#). Also, a description of the Pentagon's desire to [dominate the entire electro-magnetic spectrum](#) and their need to "[fight the net](#)" as outline in the *Information Operation Roadmap* were previously described.

What is a PSYOP?

A PSYOP is not specifically defined in this document but it does provide some insight into the wide ranging activities that are considered PSYOP.

"The customary position was that "public affairs informs, while public diplomacy and **PSYOP influence**." PSYOP also has been perceived as the most aggressive of the three information activities, **using diverse means, including psychological manipulation and personal threats**." [emphasis mine] - 26

"One result of public affairs and civil military operations is greater support for military endeavors and thus, conversely these activities **can help discourage and dissuade enemies, which PSYOP does more directly** with its own tactics, techniques and procedures." [emphasis mine] - 10

"PSYOP messages disseminated to any audience except **individual decision-makers** (and perhaps even then) will often be replayed by the news media for much larger audiences, including the American public." [emphasis mine] - 26

"A PSYOP force ready to conduct **sophisticated target-audience analysis** and **modify behaviour with multi-media PSYOP campaigns featuring commercial-quality products that can be rapidly disseminated** throughout the Combatant Commanders area of operations." [emphasis mine] - 63

"PSYOP products must be based on **in-depth knowledge of the audience's decision-making processes** and the factors influencing his decisions, **produced rapidly at the highest quality standards, and powerfully disseminated directly to targeted audiences** throughout the area of operations." [emphasis mine] - 6

"Better depiction of the **attitudes, perceptions and decision-making processes** of an adversary. Understanding how and why adversaries make decisions will require improvements in **Human Intelligence (HUMINT) and open source exploitation**, as well as improved analytic tools and methods." [emphasis mine] - 39

"SOCOM [Special Operations Command] should create a Joint PSYOP Support Element to coordinate Combatant Command programs and products with the Joint Staff and OSD [Office of the Secretary of Defense] to provide **rapidly produced, commercial-quality PSYOP product prototypes consistent with overall U.S. Government themes and messages.**" [emphasis mine] - 15

"SOCOM's ongoing PSYOP Advanced Concept Technology Demonstration and modernization efforts should permit the **timely, long-range dissemination of products** with various PSYOP delivery systems. This includes **satellite, radio and television, cellular phones and other wireless devices, the Internet** and upgrades to traditional delivery systems such as **leaflets and loudspeakers** that are highly responsive to maneuver commanders." [emphasis mine] - 15

"PSYOP equipment capabilities require 21st Century technology. This modernization would permit the long-range dissemination of PSYOP messages via new information venues such as **satellites, the Internet, personal digital assistants and cell phones:**

- (U) PSYOP ACTD. Commencing in FY04, SOCOM [Special Operations Command] initiates an Advanced Concept Technology Demonstration (ACTD) to address dissemination of PSYOP products into denied areas. The ACTD should examine a range of technologies including **a network of unmanned aerial vehicles and miniaturized, scatterable public address systems for satellite rebroadcast in denied areas.** It should also consider various message delivery systems, to include **satellite radio and television, cellular phones and other wireless devices and the Internet.**" [emphasis mine] - 65

"Rapid, fully integrated nodal and network analysis providing Combatant Commanders

with **holistic kinetic and non-kinetic solutions** for a full range of electromagnetic, physical and human IO [information operations] targets." [emphasis mine] - 39

"Capabilities such as physical security, information assurance, **counter intelligence and physical attack** make important contributions to effective IO." [emphasis mine] - 23

Third Party PSYOP

The Pentagon is also willing to use third parties for their PSYOP.

"Identify and disseminate the views of third party advocates that support U.S. positions. These sources may not articulate the U.S. position the way that the USG [US Government] would, but that may nonetheless have a positive influence." [emphasis mine] - 27

Under recommendation number 48 - "Create a Joint PSYOP Support Element" - is the following:

"Contract for commercial sources for enhanced product development." [emphasis mine] - 64

The use of third party advocates or front groups for the dissemination of US government propaganda is well documented. A couple of recent examples include the illegal payment of [\\$1.6 billion for domestic fake news](#) and [similar activities in Iraq](#) using the Lincoln Group among others.

Virtual PSYOP

Not only is the Pentagon exploiting new and old technology for aggressive behavior modification, they can also practice and refine their techniques in a virtual simulation of the entire world.

From [an article](#) by Mark Baard:

"U.S defense, intel and homeland security officials are constructing a parallel world, on a computer, which the agencies will use to test propaganda messages and military strategies."

"Called the Sentient World Simulation, the program uses AI routines based upon the psychological theories of Marty Seligman, among others. (Seligman introduced the theory of "learned helplessness" in the 1960s, after shocking beagles until they cowered, urinating, on the bottom of their cages.)"

"Yank a country's water supply. Stage a military coup. SWS will tell you what happens next."

"The sim will feature an AR avatar for each person in the real world, based upon data collected about us from government records and the internet."

How useful do you think your new MySpace or Facebook account is in helping the Pentagon develop a detailed psychological profile of you? Do you think they would be shy in exploiting such a valuable source of personal data?

AIDS Awareness

PSYOP in the past, however, often was used to support U.S. Government public diplomacy and information objectives with non-adversarial audiences. These actions include counter-drug, demining and **AIDS awareness programs** in friendly countries." [emphasis mine] - 25

It is a minor point in the context of this document, but it is worth reflecting on why US military PSYOP were used for AIDS awareness.

Are There Any Limits to Information Warfare?

An obvious question arises from the description of PSYOP described by the *Information Operation Roadmap*, are there any limits? Can PSYOP be conducted on the American public or just foreign audiences? On adversaries or non-adversaries? Can they be performed during peacetime? [My next article](#) will attempt to show just how few limits there actually are.

Information Warfare Without Limits

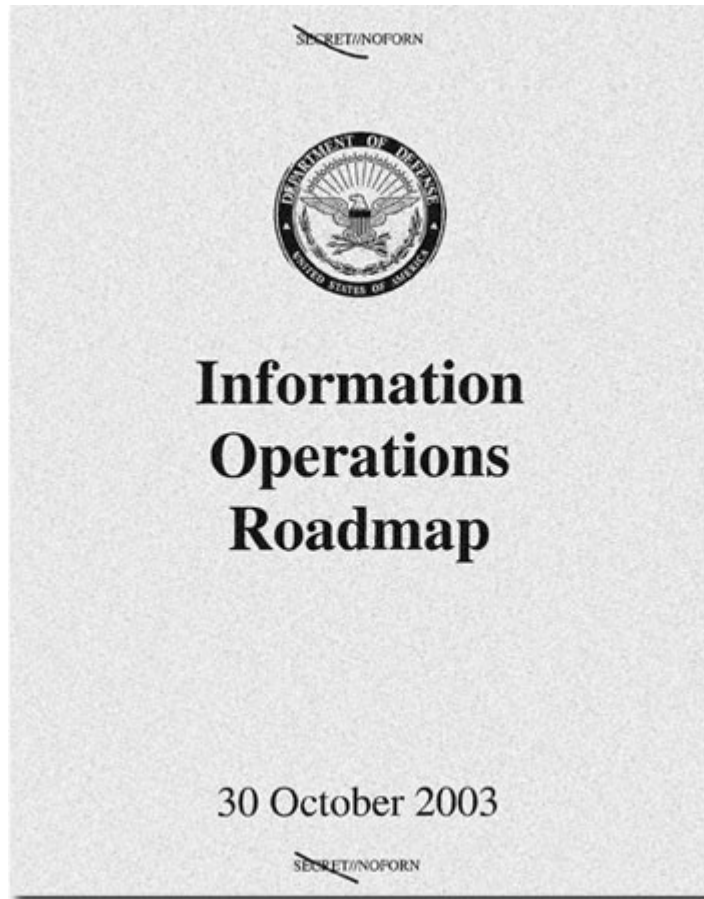
Information Operation Roadmap Part 5

Brent Jessop - [Knowledge Driven Revolution.com](http://KnowledgeDrivenRevolution.com)

December 3, 2007

The 2003 Pentagon document entitled [Information Operation Roadmap](#) describes the need to [dominate the entire electromagnetic spectrum](#), ['fight the net'](#), and use [psychological operations to aggressively modify behaviour](#). But one major question remains; are there any limits to information warfare?

If you are unfamiliar with the *Information Operation Roadmap* please read a [previous article](#) I wrote describing the major thrust of this document.



PSYOP, Public Diplomacy and Public Affairs

From the *Information Operation Roadmap*:

"In the past some basic similarities and dissimilarities between PSYOP [psychological operations], support to public diplomacy and public affairs generally have been accepted. Historically all three used **truth to bolster credibility**, and all three addressed **foreign audiences, both adversary and non-adversaries**. Only public affairs addressed **domestic audiences**. In addition, all three activities sought a positive impact for USG [US Government] interests, but with some differences in the methods employed and objectives sought. The customary position was that "**public affairs informs, while public diplomacy and PSYOP influence.**" **PSYOP also has been perceived as the most aggressive of the three information activities**, using diverse means, including psychological manipulation and personal threats." [emphasis mine] - 26

There is a lot happening in this paragraph, first, there is the almost humorous statement; "truth to bolster credibility". Does anyone remember WMDs, Saddam and 9/11, maybe some uranium from Niger? Do you believe these examples of public affairs were to inform or influence?

Secondly, "USG interests" are by no means the same as the interests of the average

American. Thirdly, the concept that only public affairs is being addressed to domestic audiences, is simply absurd given the ability of information to pass across borders. This document even admits as much:

"Impact of the global village. The increasing ability of people in most parts of the globe to **access international sources makes targeting particular audiences more difficult.** Today **the distinction between foreign and domestic audiences becomes more a question of USG [US Government] intent rather than information dissemination practices:**

PSYOP is restricted by both DoD [Department of Defense] policy and executive order from targeting American audiences, our military personnel and news agencies or outlets... However, **information intended for foreign audiences, including public diplomacy and PSYOP, increasingly is consumed by our domestic audience** and vice-versa... PSYOP messages disseminated to any audience except individual decision-makers (and perhaps even then) **will often be replayed by the news media for much larger audiences, including the American public.**" [emphasis mine] - 26

So there you have it, "the distinction between foreign and domestic audiences becomes more a question of US government intent rather than information dissemination practices". Therefore, the American public is fair game for all forms of US government propaganda, be it, public affairs, public diplomacy or PSYOP. Remember, PSYOP use "diverse means, including psychological manipulation and personal threats" among [many other things](#).

It should also be highlighted that PSYOP are only **restricted** not **prohibited** from being used on the American public. If that loophole is not large enough, the distinctions between the tactics of public affairs, public diplomacy and PSYOP are elaborated in Appendix C of the *Information Operation Roadmap*. The very last task listed for PSYOP is: "when called upon, support to local public affairs activities".

Appendix C of this document is well worth the one page read ([pg 71](#)). Some other highlight include:

Public Affairs:

"Rapid Response/Truth Squads and "Briefings Plus" "

"Humanitarian road shows"

"Media embeds"

"Combat Camera products on events not accessible to news media"

Public Diplomacy:

"Content of speeches or OP/ED pieces by senior DoD [Department of Defense] officials to foreign audiences"

"Talking points for private exchanges with foreign leaders"

"Overt dissemination of USG [US Government] policy. e.g. Asia-Pacific Forum"

PSYOP:

"Radio/TV/Print/Web media designed to directly modify behaviour and distributed in theatre supporting military endeavors in semi or non-permissive environments"

"When called upon, support to theatre public diplomacy"

"DoD advisors to assist friendly forces in developing PSYOP programs"

Changing Definitions

Definitions are another great tool if you are trying to deceive. As described above the definitions of and distinction between public affair, public diplomacy and PSYOP are left intentionally vague. Lawyers make a living out of this type of deception and their hands are all over this document.

"PSYOP **should** focus on support to military endeavors (exercises, deployments and operations) in non-permissive or semi-permissive environments (i.e. when adversaries are part of the equation).

- (U) However, PSYOP forces and capabilities may be employed to support U.S. public diplomacy as part of approved theatre security cooperation guideline. In this case PSYOP personnel and equipment are not conducting a PSYOP mission, but rather are providing military support to public diplomacy." [emphasis mine] - 27

Get that? If PSYOP forces and equipment are used in support of military endeavours, it is a PSYOP mission. If PSYOP forces and equipment are used in support of public diplomacy, it is public diplomacy.

A Quick Recap

A close read of the above quotes reveal that information operations, specifically PSYOP, can be used on both domestic and foreign audiences, in non-permissive or semi-permissive environments, and on adversary and non-adversary. Are there any other limits?

Peace, Crisis and War

"The Department's concept of IO [information operations] should emphasize **full spectrum IO** that makes a potent contribution to effects based operations across the **full range of military operations during peace, crisis and war**. [emphasis mine]" - 7

"Peacetime preparation. The Department's IO concept should **emphasize that full-spectrum information operations are full-time operations requiring extensive preparations in peacetime... Well before crises develop**, the IO battlespace should be prepared through intelligence, surveillance and reconnaissance and extensive planning activities... Similarly, considerable effort should be made to characterize potential adversary audiences, and particularly senior decision-makers and decision-making processes and priorities. If such human factors analysis is not conducted **well in advance of the conflict**, it will not be possible to craft PSYOP themes and messages that will be effective in modifying adversary behaviour" [emphasis mine] - 8

"Clear, unambiguous and streamlined DoD [Department of Defense] oversight and policy that empowers Combatant Commanders to execute **full spectrum IO before, during and after combat operations.**" [emphasis mine] - 20

Denied Areas

"Improvements in PSYOP capability are required to rapidly generate audience specific, commercial-quality products into **denied areas.**" [emphasis mine] - 26

"Projecting electronic attack into **denied areas by means of stealthy platforms.**" [emphasis mine] - 62

Conclusion

Does the Pentagon define any real limits to information warfare? Information operations can be used on both domestic and foreign audiences, in non-permissive or semi-permissive environments, on adversary and non-adversary, during peace, crisis and war, and in denied areas. Should we really expect anything less? They did tell us that their goal was full spectrum dominance.



KNOWLEDGE DRIVEN REVOLUTION