

Pentagon: The internet needs to be dealt with as if it were an enemy “weapons system”.

By [Brent Jessop](#)

Global Research, February 02, 2008

[Knowledge Driven Revolution.com](#) 19

November 2007

Theme: [Media Disinformation](#), [Police State & Civil Rights](#)

Information Operation Roadmap Part 3

✖ 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 Defenses*:

“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.

The original source of this article is [Knowledge Driven Revolution.com](#)
Copyright © [Brent Jessop](#), [Knowledge Driven Revolution.com](#), 2008

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Brent Jessop](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca