EMBRY-RIDDLE
Aeronautical University
SCHOLARLY COMMONS

International Bulletin of Political Psychology

Volume 5 | Issue 19 Article 3

11-6-1998

Information Warfare and the Hacktivist

Editor

Follow this and additional works at: https://commons.erau.edu/ibpp

 Part of the Cognition and Perception Commons, and the Other Psychology Commons

Recommended Citation

Editor (1998) "Information Warfare and the Hacktivist," *International Bulletin of Political Psychology*: Vol. 5 : Iss. 19 , Article 3.
Available at: https://commons.erau.edu/ibpp/vol5/iss19/3

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in International Bulletin of Political Psychology by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe309@erau.edu.

International Bulletin of Political Psychology

Title: Information Warfare and the Hacktivist
Author: Editor
Volume: 5
Issue: 19
Date: 1998-11-06
Keywords: Hacktivism, Information Warfare, Perception Management

Abstract. This article provides comments on the significance of hacktivism.

As defined on the Web site http://www.hacktivism.org, hacktivism is the policy of hacking, phreaking, or creating technology to achieve a political or social goal. In common English, this entails a number of formally unauthorized computer activities including (1) entering a Web site; (2) preventing the entry of others; (3) modifying the Web site's contents, structures, functions or processes; or 4) "crashing" or deactivating the Web site.

As cited in The New York Times, examples have included (1) inserting a "Save Kashmir" message over the opening screen of an Indian government Web site set up to provide information about the region, (2) placing an image of a mushroom cloud on the Web site of India's major nuclear weapons research center, (3) modifying a number of Indonesian Web sites to display the slogan "Free East Timor" and adding links to other Web sites describing alleged Indonesian human rights abuses in East Timor, (4) deactivating a Web site promoting political causes of ethnic Albanians in Kosovo, and (5) inserting a message to read a Croatian newspaper not Serbian books on the Web site of the Serbian National Library. Allegedly, the Internet operations of United States companies doing business in the People's Republic of China are to be attacked based on the rationale that the former are complicit with the human rights violations of the latter.

Although hacktivism may be a recent development in information warfare (IW), it does not present new principles of waging IW or countering it. As always, the IW initiator is employing and targeting some combination of information and medium of transmission. As always, the IW initiator is seeking to achieve some political goal--in the sense of influencing the disparity between actual and desired realities. As always, the IW initiator may effectively implement an IW operation but be ineffective in achieving the operation's goal. As always the IW initiator may be so enamored with IW media of transmission or so mesmerized by simple but incorrect notions--that more or bigger is better or that nonaction cannot be an effective option--that attaining political goals may prove elusive. As always, the IW initiator--no matter how adept--may be quite susceptible to IW at the hands of others and utterly dependent on intelligence data, analysis, and production. And regardless of the sophistication of technology, human factors will prove crucial both for IW and counter-IW. Such factors include the (1) resistance to disconfirming information, paranoid-like traits, personality rigidity or lability, empathy, and cultural sensitivity of the IW initiator; (2) the persuasability, dependence on specific information content and media of transmission, and congruence between psychological and behavioral elements of the IW target; and (3) the psychologies of observers who are neither current IW initiators nor targets but who may be in the future and/or may be current or future allies or adversaries in the world of politics.

So, does the "hack" of "hacktivism" connote someone who can hope successfully or someone who can cut and injure with repeated, if irregular, blows? Or someone who functions like an old, worn-out horse? Or someone who merely carries out unpleasant or distasteful tasks for money? Or someone who despite the best or worst of efforts is no more than a banal and trite political player? The answer depends on whether hacktivists or those who seek to counter them reign supreme with new technology in a very old

Published by Scholarly Commons, 1998

arena. (See Editorial: An ethological approach to information warfare. (November 22-29, 1996). IBPP, 1(4); Harmon, A. (October 31, 998). 'Hacktivists' of all persuasions take their struggle to the Web. The New York Times, http://www.nytimes.com; http://www.hacktivism.org; Information warfare, China, and South Korea: More than a military concept. (January 16, 1997). IBPP, 4(2); Kovacich, G. (1997). Information warfare and the information security system security professional. Computers and Security, 16; Lubicki, M. C. (1997). Information warfare. Physics Today, 50; Rodgers, J.L. (1997). Information warfare: Nothing new under the sun. The Marine Corps Gazette, 81.) (Keywords: Hacktivism, Information Warfare, Perception Management.)