

Information assurance for operations other than war — when we are the enemy

Clark K. Ray, US Military Academy

Purpose

An expanded view of Information Assurance (IA) is required to deal with new sources of risk posed by the combination of pervasive information technology (culturally and in support of military operations) and frequent US involvement in extended low intensity conflict (LIC) and operations-other-than-war (OOTW) situations. In culturally and politically complex situations, moral ambiguities put pressure on personnel and call into question the belief that loyalty to peers and nation will inoculate virtually all personnel from the temptation to misuse or abuse information assets at their disposal to the detriment of national policy objectives.

Method

The quarter-century period between the end of the US involvement in the Vietnam conflict and the current day are replete with LIC and OOTW operational examples where misuse of information technology — a failure of information assurance applied to ourselves — could have had serious detrimental impacts on operations. Intersecting examples drawn from this set of operations with current thinking on Information Operations and potential venues for future US involvement helps identify a variety of mechanisms by which US personnel may become significant sources of risk in compromising political objectives or support.

Results

Attempts to use information technology to ameliorate the morale impacts of extended or repeated deployments, or to improve efficiencies, responsiveness, or flexibility will provide opportunities for US personnel caught in ambiguous operational settings to respond by providing information which compromises perceptions crucial to successful outcomes or continued support. Such leaks of information may be intended to harm or disrupt the basis for the ongoing operation or may be simple expressions of frustration which are subsequently exploited by hostile groups or given prominence in the media.

New or breakthrough aspect of work

Most investigations of information assurance issues for LIC and OOTW focus on how groups whose interests conflict with those of the United States and its allies may attempt to exploit technological, organizational, or doctrinal weaknesses in the information infrastructure. Common points of vulnerability cited include items such as computer network attack, viruses, manipulation of the media, logic bombs, and attacks on supporting civilian infrastructure. Overlooked until now has been the potential for US personnel conducting LIC and OOTW activities to use the information infrastructure within their operational environment to undermine, deliberately or by accident, the success of the stated mission.

Conclusions

Political and psychological preparation for sustained LIC or OOTW operations will become progressively more crucial. Denying US personnel access to information technologies that could be misused will prove infeasible. National political decisions regarding the scope of operations will become conditioned by the risks posed by US personnel undermining key perceptions supporting US involvement, possibly after the occurrence of one or more spectacular compromises with an impact comparable to the deaths of US Army Rangers in Somalia in 1993.