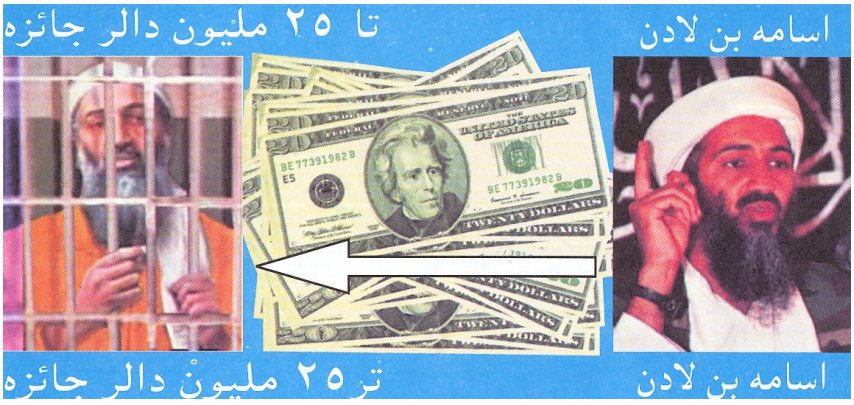
CSS Analyses in Security Policy

CSS ETH Zurich

Vol. 3 • No. 34 • May 2008

INFORMATION OPERATIONS: TRENDS AND CONTROVERSIES

Information operations have gained importance in recent years. The capabilities to influence the enemy's information or the attitudes of the civilian population in theaters of conflict, and to secure one's own information and information systems, have become important success factors in military operations. The concept has given rise to vehement controversies, however. Disagreement remains over the nature and scope of operations that can be carried out by the armed forces of democratic states under the rule of law. Clarification is also required as to the distribution of responsibility and tasks at the interface of civilian and military authority.



Leaflet distributed by the US in Afghanistan *psywarrior.com*

The factor of information has always been an important aspect of power, diplomacy, and armed conflict. As Chinese strategist Sun Tzu (~400–320 B.C.) pointed out, knowledge about the opponent and of one's own destructive capabilities is the precondition for success in battle – and the ultimate goal must be to win a war without fighting battles due to information dominance. But even though the history of information warfare is as old as war itself: Only in recent times have the means become available to influence the adversary in a comprehensive way. The importance of information as an element of effective security and defense policy has therefore increased further in the past few years.

In the 1990s, the basic and timeless principles of information strategies were bundled under the heading of "Information Operations" and complemented by new elements. On the one hand, the military doctrine – developed mainly by the US – is a continuation of the aims of classic wartime information policy. On the other hand, it is shaped by the central premise that information dominance is not only an auxiliary to warfighting, but a form of combat in its own right that is suitable for determining the final outcome of conflicts. Media and information are integrated as actual weapons into the arsenal of offensive and defensive capabilities. In this way, the concept of modern information operations reflects and reinforces the increasing blurring between military and non-military aspects of security policy. At the same time, it requires a high degree of coordination between the military-operational and the political-strategic levels as well as between state and non-state actors.

Defensive and offensive components

Due to the information revolution, our society attributes an increasingly high level of importance to the generation, management, and use of information. This tendency is driven by technology developments in the area of information and communication technology (ICT) and by the increasingly widespread use of such technology in all areas of the economy, politics, and society. The ability to master the new technologies and to influence content has increasingly become a core power resource in the system of international relations.

Against this background, the concept of information operations has constantly been gaining attention and importance. The Gulf War of 1991 was seen by military strategists as the first of a new generation of conflicts where victory is no longer ensured only by physical force, but also by the ability to win the "information war" and to secure "information dominance".

This debate was initially characterized by a great deal of euphoria. Soon after, more attention was given to the risks associated with this development: The formulation of strategies that no longer aimed at enemy capabilities, but directly targeted the opponents' flow of information, highlighted the relatively high vulnerability of networked US troops. As the debate over attacks on potential hostile information

systems progressed, the possible dangers to the own military and civilian data networks were increasingly discussed as well. The growing number of warnings voiced in the first half of the 1990s over the potential threat to national security from (asymmetric) cyber-attacks against power plants, banks, or air traffic control gave rise to the debate over protecting critical infrastructures (see CSS Analysis No. 16).

Until the late 1990s, there was no consolidated doctrine for conducting information warfare. While there were a variety of different approaches, the individual building blocks were not assembled into a coherent strategy directive until 1998, when the US Joint Chiefs of Staff released Joint Publication JP 3-13, "Joint Doctrine for Information Operations".

Since then, the category of Information Operations (Info Ops) has included offensive as well as defensive measures to manipulate enemy information and information systems as well as decision-making processes and to defend one's own information, information systems, and decision-making processes. Info Ops includes a broad range of concepts such as psychological warfare, physical destruction, electronic warfare, attacks against computer networks and defense against such attacks, military deception, counter-propaganda, counter-deception, information security, operational security, and computer intrusions.

However, a comparison of the more than 20 extant Info Ops doctrines of various NATO states shows that the concept is handled in various ways. Only few states have the political determination or capabilities to apply the entire range of instruments. Also, the majority of countries attribute greater importance to defensive measures than to possible offensive operations.

A cross-sectional and integrated task

Despite this heterogeneity, three elements can be identified that are characteristic for contemporary information operations. First of all, these operations serve a cross-sectional purpose within the spectrum of military operations. Information operations play an important role in defensive operations, as well as in missions below the threshold of war and in international stabilization missions. While some of the Info Ops measures, such as bombing radar emplacements, are only to be undertaken in the context of warlike conflict at the strategic, tactical, and operational levels, other measures, including elements of psychological warfare, are also envisaged at levels below the threshold of war, i.e., in a peacetime environment. Thus, the clear distinction between war and peace is blurred and the rules of war as specified by international law are suspended.

Secondly, information operations are not to be understood in isolation as purely military tasks, but as part of an integrated task shared by the military and civilian state and non-state actors in the context of a comprehensive information strategy. The armed forces can often only offer a limited contribution to defensive activities. For example, to ward off possible attacks by state or non-state actors against information systems and infrastructures, recourse is taken to Critical Infrastructure Protection (CIP). The latter is a task for civilian operators that must be tackled by means of internal cooperation of the state and the corporate sector as well as external cooperation with international partners. The military's role is clearly limited to protection of its own networks.

Another area that is primarily the responsibility of political decisionmakers is that of risks associated with the content of information. The intentional distribution of distorted or even false information is part of the stock in trade of conflicts at all levels. Handling disinformation in the broadest sense is part of the ordinary activities of governments and the information and communications agents instructed by them. This goes far beyond the boundaries of the military dimension and is quite clearly a political, not a military task. However, the military can contribute in significant ways to the discovery of hostile disinformation or the protection of national executive structures.

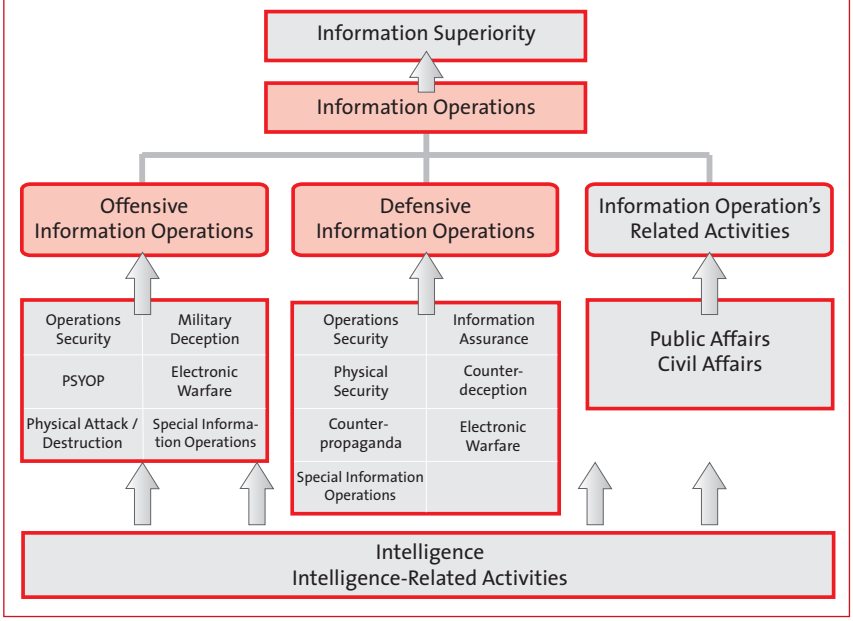
In other, primarily offensive areas of information operations, the operative and tactical levels of the military play an important role in command-and-control as well as implementation of information operations. But even these types of operations often have only a limited effect without coordinated flanking measures at the political-strategic level. Also, they frequently lack legitimacy. The requirement for cross-sectoral cooperation and coordination is increasing all the more because contemporary information operations no longer only aim at influencing information spaces and systems that are narrowly delineated in geographic terms, but are directed at an audience spanning the entire globe.

Focus on psychological warfare after 9/11

In line with this last observation, thirdly, an increasing importance of psychological operations (PSYOP) within information operations can be noted.

This is due on the one hand to the fact that after 11 September 2001, the focus shifted towards terrorist organizations and their skillful use of ICT and new

Information Operations according to US-Doctrine (JP3-13)



media. The concerns were not only related to doomsday scenarios of "cyberterror" involving militant attackers hacking into networks and triggering a worst-case meltdown. Terrorism is, among other aspects, a communication strategy. Of course, it is nothing new for terrorist actors to employ a combination of violence and media propaganda for their own purposes. However, the communications instruments available today for creating and especially for disseminating information globally are much more sophisticated. A case in point is the use of the internet to distribute decapitation videos. This macabre orchestration is intended to create fear and as a display of power, and is used as a weapon of psychological warfare against US occupation forces.

The reinforcement of both military and civilian efforts in the area of states' strategic information strategies must therefore also be examined in the broader context of the so-called "war on terrorism". The US State Department plans and carries out measures for strategic manipulative communication under the label of "Public Diplomacy". This term encompasses a variety of aspects including foreign propaganda, political marketing, and cultural diplomacy. On the one hand, it aims at exerting a positive influence on public opinion in the Muslim world, while on the other hand, its purpose is to convince a global audience that this "war" is justified. This comes under the heading of so-called "white" propaganda, referring to information that is as factual, truthful, and current as possible.

That is not the case with some aspects of military PSYOP (or perception management, as it is sometimes called). US Secretary of Defense Donald Rumsfeld in 2002 founded the "Office of Strategic Influence", the stated purpose of which was to serve as an office of subversive propaganda and disinformation policy (i.e., "black" propaganda). While the Pentagon had to shut down this office due to world-wide protests, an "Office of Global Communications" was instituted shortly thereafter at the White House that serves a similar purpose and is charged with coordinating the entire range of US foreign propaganda. In parallel, use is made of "grey" propaganda, where the information disseminated is neither true nor false, but serves to build the desired framework of interpretation. A key actor is communications consultant John Rendon with his company "The Rendon Group", which had already been responsible for handling PR for the Afghanistan campaign.

However, PSYOP is handled in different ways by different states. For example, the German armed forces (Bundeswehr), which uses the term "Operative Information" instead of PSYOP, claims to eschew the spreading of untrue information, at most influencing opinion through selective distribution of information. The eminent importance of psychological operations has been acknowledged particularly due to the experiences of multilateral stabilization missions in conflict areas during recent years. Without the acceptance of the local population, such missions are doomed to failure in the long term, which is why the dissemination and control of (truthful) information via radio programs, leaflets, internet presence, etc. is gaining increasing attention.

"Information Operations are regarded today as an integral part of warfare"

Demand for clarification

Even though information operations have gained a great deal of importance in recent years, the concept as such remains controversial. As far as democratic states with rule of law are concerned, this is true in particular for the offensive aspects of such operations. It is important to clarify some basic issues before any capabilities are built in this area.

Info Ops are regarded today as an integral part of warfare. Media are conceived as weapons not just symbolically, but in a very real sense. The spectrum of intentions of Info Ops is total, since they are aimed not only at the population of one's own country, a hostile country, or one's allies, but at the entirety of the global public, and also because information in this context no longer refers simply to information disseminated via mass media, but to the entire communication infrastructure of an opponent, including civilian and military data networks, telecommunications installations, and the mass media. It is no longer possible to draw a distinction between combatants and non-combatants in information warfare. It is therefore necessary to stipulate explicitly in which situation a state founded on the rule of law may legitimately take recourse to which aspects of offensive information operations and to what extent.

On the other hand, it seems impractical to exclude offensive operations in general, particularly since, as explained above, psychological operations play an increasingly important role for the success of multilateral peacekeeping operations. But in which context may and should a state take recourse to disinformation? It is a challenging proposition to distinguish clearly between Info Ops in combat and general public information activities. Clarification is also required as to the requirements for training of military personnel and doctrinal development, and the role of the military at the strategic, operative, and tactical levels must be considered carefully.

The distribution of roles between the armed forces and the political authorities also needs to be clearly delineated. The question here is specifically whether the armed forces can and should take on tasks in the area of offensive information operations. Further study is required as to how political control and authority over such military operations as well as coordination with activities at the political-strategic level can be assured.

Author:
Myriam Dunn Cavelty
dunn@sipo.gess.ethz.ch

Responsible editor:
Daniel Möckli
analysen@sipo.gess.ethz.ch

Translated from German:
Christopher Findlay

Other CSS Analyses / Mailinglist:
www.isn.ethz.ch

German and French versions:
www.ssn.ethz.ch