RAND Europe

Information Operations and the Kosovo Conflict

Dr Kevin A. O'Brien

Senior Policy Analyst

RAND Europe – Using Partnerships in Europe to Create Awareness in the Information Society

These are personal reflections and do not necessarily represent the views of RAND Europe, its parent RAND, or of any of its sponsors

Outline

- Information Operations Defined
- US Information Operations Generally
- US IO and Operation “Allied Force”
- Serbian Information Operations
- Lessons Learned from IO in the Kosovo Conflict
- Future Initiatives
- The Next War?

Information Operations

- "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information" (US Department of Defense)

- "deliberate..and systematic attack on critical information activities" which seek to exploit, modify, corrupt information or to deny service (UK MoD)

US Information Operations

- Offensive IO in three principle categories:
  - *attacks on infrastructure* – that 'activity that causes damage to information or information systems, or interferes with operations'
  - *deception* – designed to 'mislead an enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests'
  - *psychological operations* – 'the ability to influence the will of another society'

US Information Operations

- Defensive IO "integrates and co-ordinates policies and procedures, operations, personnel, and technology to protect and defend information and information systems"
- Defensive IO are conducted through information assurance, OPSEC, physical security, counter-deception, counter-propaganda, counter-intelligence, Electronic Warfare, and Special Information Operations
  - Offensive IO can also support defensive IO: defensive IO ensures the necessary protection and defense of information and information systems

Information Operations

- Multi-levelled
  - At the highest level, IO can be conceived of as an ideational struggle for the mind of an opponent and his supporters
  - At this level, IO encompasses the whole range of psychological, media, diplomatic and military techniques for influencing the mind of an opponent, whether that opponent is a military commander or a whole population (of particular interest in counter-terrorism)

- Multi-levelled
  - IO involves the co-ordination of not just military assets but of national information power as a whole
  - an effective IO campaign would operate at the grand strategic level, with full cross-spectoral co-ordination
  - at this level, American strategic theorists debate the use of “information power” and the exploitation of America’s “information edge” to achieve the nation’s geostrategic objectives

Information Operations

- "Netwar" – "an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organisation and related doctrines, strategies and technologies attuned to the Information Age"

- Consists of "dispersed small groups who communicate, co-ordinate, and conduct their campaigns in an internetted manner, without a precise central command"

US IO in Haiti & Iraq

- Contrary to the view of Operation "Allied Force" as the first "cyber-war", the US has – in the past – used IO capabilities at least twice
  - Iraq: even as far back as Operation *Desert Storm*, CNO capabilities (such as computer viruses inserted into the Iraqi Command and Control computers) used
  - Operation *Restore Hope* (Haiti): US used hacking to exploit knowledge about Haitian government intentions and capabilities
    - Also launched a sophisticated psy-ops campaign against Haiti's military regime

US Information Operations

- USG now includes IO as a key component of national security strategy and doctrine
- JCS have made Information Superiority (IS) one of the cornerstones of US doctrine for the 21st Century
- US *Joint Publication 3-13* defines IS as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same"

US Information Operations

- Information Superiority Strategy is based on three key areas:
  - Intelligence
  - Command, Control, Communications and Computers (C^4)
  - IO
- Concept of IO builds on the activities of Command and Control Warfare (C^2W) as a sub-set of Information Warfare

US Information Operations

- C^2W is concerned with efforts to "influence, degrade or destroy an adversary's command and control capabilities while protecting friendly capabilities"
  - Includes *Deception*, *Physical Destruction*, *Psychological Operations*, *Operational Security*, and *Electronic Warfare*, as well as *Public Affairs* and *Civil Affairs*
  - Underpinned and bound together by a foundation of *Intelligence* and *Communications*
  - *Computer Network Attack* (CNA) added recently

NATO IO in "Allied Force"

"Properly executed, IO could have halved the length of the campaign"

But...

IO operators were "too junior and from the wrong communities to have the required impact on planning and execution"

Admiral Ellis, Air Campaign Commander

NATO IO in “Allied Force”

While “the importance of such capabilities was recognised fully during Operation Allied Force”, the conduct of an integrated IO campaign was limited because of “the lack of both advance planning and strategic guidance defining key objectives.”

The “conduct of disinformation and propaganda campaigns” were essential to the Yugoslav strategy.

William Cohen and Henry Shelton

NATO IO in "Allied Force"

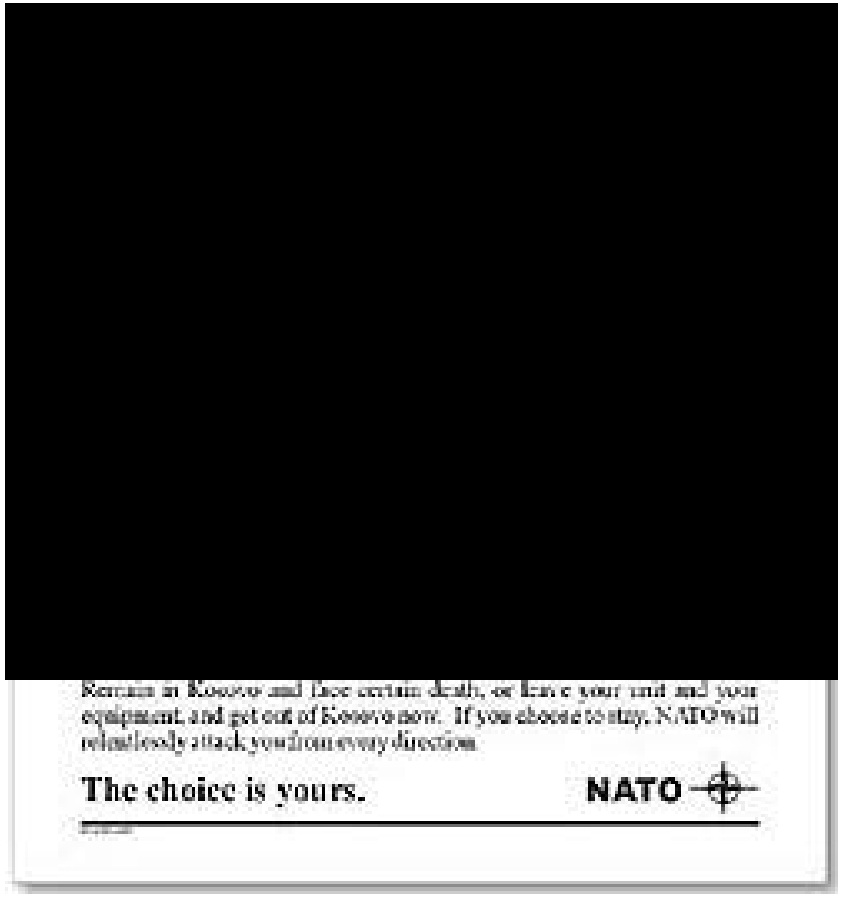
- What could have happened
  - "Offensive hacking" against Belgrade's information infrastructure and the financial assets of the regime
  - Total jamming and/or subversion of Belgrade's communications and propaganda capabilities
  - Use of microwave technology against communications
  - Use of cruise missiles armed with carbon-fibre payloads to short-out the Serb electric grid
  - Special Forces-directed C^2W
  - Propaganda Disruption and Perception Management

-

NATO IO in "Allied Force"

- Propaganda & Perception Management
  - NATO initial effort extremely limited, especially regarding management of public affairs campaign
  - Attempts to bomb Serbian media or symbolic political targets were, in part, designed to influence Serbian perceptions
  - NATO generally failed propaganda and perception management campaign, partly due to Belgrade's virtually total control over internal media and broadcasting

NATO IO in "Allied Force"



More than 19 million leaflets were dropped by NATO forces

NATO IO in "Allied Force"

- Offensive Information Warfare
  - Aimed at Serbian theatre and national C^2 systems, especially air-defence systems
  - CNA exploited for covert intelligence gathering purposes rather than for more aggressive purposes
  - "Soft kill" tools such as graphite bombs used against the electrical power infrastructure
  - Hacking into Serbian government e-mail systems
  - Some infiltration of the internet systems of banks around the world in search of accounts held by Serbian leadership but no action

Serbian IO During Kosovo

- Yugoslav government dedicated great effort to “perception management”, especially internally
- Limited attempts also made to influence world-wide perceptions through sponsoring pro-Serb websites and chat-rooms, as well as other efforts
- Disruption of NATO’s websites and public information servers also part of this effort
- Serbian cyber-attackers displayed a limited understanding of the architectures of NATO’s information systems

Serbian IO During Kosovo

- After 28 March, concerted hacking efforts by individuals supporting the Serbian side resulted in a massive slow-down of NATO and other Western government websites
- Caused largely by “spam” and “ping” attacks, as well as the introduction of marco-viruses into NATO via e-mail systems
- Overall, did not constitute a co-ordinated information campaign

Lessons Learned

- During Kosovo, NATO failed to use the full range of IO tools and concepts at its disposal
- By using non-lethal means, NATO may have avoided rallying Serb popular support around an otherwise hated regime, and would have found it easier to maintain a consensus behind its campaign
- “Perception Management” capability of NATO was sorely limited

Conclusions - “Allied Force”

1. The US military and intelligence community was reluctant to make aggressive use of some of the more exotic capabilities it has developed for disrupting information infrastructures
2. The US Armed Forces were by no means convinced that the “softer” IO techniques would work by themselves
3. US has not yet fully incorporated IO into its campaign planning and its coercive doctrine
4. Even if the US had wanted to engage in an all-out IO campaign, the political necessity of ensuring alliance cohesion would have prevented this

-

Thank you!!

Dr Kevin A. O'Brien

Senior Policy Analyst
RAND Europe Cambridge
Grafton House – 64 Maids Causeway
Cambridge CB5 8DD United Kingdom
+44(0)1223-353329 tel
+44(0)1223-358845 fax
obrien@rand.org

www.randeurope.org