Counter-terrorism Information Operations

Today's potential threat environment is complex. It includes poverty, HIV/AIDS and environmental threats as well as terrorism and weapons of mass destruction. These threats are interlinked and borderless. The new terrorism has freed itself from territory and the threat from this transnational terrorism is not only a problem for the USA and its close allies. Democratic states will have to face the threat on many fronts, even in their own backyard.1 Another important aspect of today's terrorism is the privatization of war by transnational groups such as Al Qaeda. It constitutes a major historical change in world politics that must be addressed.2

How should we describe the new conditions that are shaping counter-terrorism policies in the Information Age? This paper outlines an approach to that question through consideration of terrorism as a contest for influence, rather than for power or control. This paper also discusses the potential use of and developments in the military aspects of Information Operations, including doctrine, organisation, and capability, as well as broader developments at the strategic level.

We therefore started from the presumption, drawing on existing legal frameworks, that the preferable measures are civil rather than military. The challenge was then to identify when, if at all, it is appropriate to engage military means and then consider which military capabilities could be effective in countering terrorism.
Two arguments are extended; the way information technologies3 are enabling formerly underprivileged groups to play a role in global politics is leading to the privatization of war; and the benefits to be gained by opening and sharing our information and related information infrastructures with our allies and others, in such areas as intelligence and coalition formation.

What is Information Operations?

The military establishment is formulating new visions, strategies, and concepts that capitalize on emerging information-age technologies in order to provide its Armed Forces with significantly improved capabilities for meeting security challenges of the 21st century. Information Operations (IO) as a concept was launched by the U.S.Government to develop a set of doctrinal approaches for its military and diplomatic forces to use and operationalise the power of information. Originally developed in 1996 by the US Government as a component of Joint Vision 2010, IO was formally defined as "those actions taken to affect an adversary's information and information system while defending one's own." This document was written to establish a vision for how the U.S. military would operate in the uncertain future.4

Although Operation Desert Storm introduced the world to the advantages of this revolutionary era, it was in Somalia in October 1993 that the true power of IO came

---

[1] Armistead, Leigh (ed.*). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p.138
[2] Nye , Joseph S., *Soft Power: The means to success in world politics* (New York: Public Affairs, 2004). p.132
[3] The information revolution itself can be understood only within the context of the globalization.
[4] Armistead, Leigh (ed.*). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p.17

into force. Recent IO operations have included increased emphasis on the adversary's decision-making process. Balancing the efforts of both technology (hardware, software and systems) and the human aspects (perception management) is critical in order to achieve operational success.5

The target of IO is the adversary decision-maker and therefore the primacy of the effort will be to coerce that person, or group of people, into doing or not performing a certain action. In IO, many different capabilities, such as deception, psychological operations, and electronic warfare, are used to affect the adversary decision-maker to shape and influence the information environment.6 In the concept of IO these different capabilities and related activities that are intended to be used in an integrated fashion to produce effects.7 IO by definition is normally broken down into offensive and defensive disciplines in order to better understand the relationship between different capabilities and their related activities8.

Sweden has adopted the IO concept; the most semi-official Swedish definition can be found in the Government's information technology bill of March 2000 (1999/2000:86, p. 36):

> Information operations are combined and coordinated measures in peace, crisis and war to support political or military goals by influencing or exploiting the information and information systems of the adversary or other foreign player. This can occur by using one's own information and information systems while these assets must also be protected. An important element is the attempt to influence decision-making processes and decision-making.
>
> There are both offensive and defensive information operations. These are carried out in political, economic and military contexts. Examples of information operations include information warfare, mass-media manipulation, and psychological warfare and intelligence operations. Defensive information operations are coordinated and integrated measures in times of peace, crisis and war as regards policy, operations, personnel and technology to protect and defend information, information systems and the ability to make rational decisions.

Military commanders should therefore plan to employ offensive IO capabilities and related activities with the goal of influencing their adversary's observation, orientation and perception, thus causing them to decide to act in a way that is advantageous to that commander's objective.9 The capabilities mentioned above have existed for a long time, but the umbrella term of IO is a relatively recent development. IO is still not understood very well. To many people, IO is simply computer warfare when in fact it is about much more than that.

---

[5] The bottom line is that it will be examining the ability of certain key activities to manage influencing and shaping campaigns across the whole political spectrum.
[6] Armistead, Leigh (ed*.). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p.16
[7] Joint Information Planning Handbook-July 2002, (Information Warfare Division of the Joint Forces Staff College National Defense University, Norfolk,Virginia, 2002).
[8] A common complaint about IO is that because its definition is so broad, IO is at once everything and nothing.
[9] Armistead, Leigh (ed*.). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p.112

The Adversary

The analysis of terrorist networks is often concerned with the identification of élites and leadership, the discovery of the ways in which power is allocated to different strata, relations among leaders and between leaders, etc, but we are more concerned about the effects they 'cause' and what objectives they are after. Technology plays a critical role in the terrorist's new equation. Information technology has empowered non-actors, such as transnational social movements or terrorist groups.10 The off-the-shelf commercial availability of what used to be costly military technologies, benefits small states and non-state actors and increases the vulnerability of larger states.11

Globalisation has vastly increased incentives and opportunities for terrorist networks to easier organize, finance and sustain their strategies. Terrorists have also become remarkably innovative in the way that they handle, distribute and cover their financial arrangements. Terrorism today commonly merges with criminal activities, especially in the field of financing. 12

What impact the information society will have on terrorism has been a question of debate for some years. Especially the question if terrorists will conduct operations in the "cyber" dimension has divided the field of expertise. Parallels can be drawn to the debate in the 1970's and 1980's regarding terrorism and the use of CRBN weapons. Many scholars rejected that idea on the grounds of the inherent conservatism within many groups and for cost-efficiency reasons.13 In spite of the opinions of the sceptics, the Rubicon was crossed and the threat became reality.14

The "cyber" Rubicon has yet to be crossed, but terrorist groups have shown interest in the possibilities brought on by new information technology. Terrorist groups have adopted some aspects of what the information society has to offer. Foremost, the interest has been in fields such as intelligence gathering, communication and propaganda work. Information technology has become irreplaceable for many groups. Beyond these rather modest steps into the information age, some groups have also shown interest in digital methods and information targets.

The terrorism we face today is a complex web of local organisations and transnational networks sprung from globalizations back alleys. The Al Qaeda network involves individuals and groups from many countries and is alleged to have had cells in as many as fifty.15 The root causes of terrorism also have both local and transnational dimensions and therefore an effective response requires a coordinated local to global policy. We strongly believe in an international and multilateral approach in the forming of a coherent Information Operations strategy for countering terrorism.

---

[10] Rosenau, James N. and Singh J.P. (eds.), Information Technologies and Global Politics: the changing scope of power and governance. (Albany, NY: State University of New York Press, 2002) p.7

[11] Close cooperation of intelligence, customs, and police agencies will play a major role.

[12] For example, the underground banking networks are used by both criminal groups as by terrorist networks.

[13] Nicander, Lars and Ranstorp, Magnus (eds.), *Terrorism in the Information Age*, (Stockholm, Swedish National Defence College, 2004). p.13

[14] The Japanese cult Aum Shinrikyo crossed the line when they attacked the Tokyo underground with Sarin in March 1995.

[15] Nye , Joseph S., Understanding International Conflicts: an introduction to theory and history, 4th ed.(New York: Longman, 2003) p.220

Domestic Counterterrorism Operations

Before the terrorist attacks in the USA on 11 September 2001, the view was generally held that there was no right to military self-defence against international terrorism. The attacks on 11 September made it clear that large-scale terrorism is a threat to national security. Through resolutions passed by the UN and other international organisations, among other things, the international community has supported the view that a right to self-defence under Article 51 of the UN Charter also applies in the event of large-scale terrorist strikes. This view must now be seen as reflecting current international law.

The Instrument of Government, Chapter 10, Section 9, first paragraph, states that the Swedish Government may deploy the Armed Forces, or parts thereof, in combat to meet armed attacks against the country. The main task of the Swedish Armed Forces is to maintain and develop the capacity to engage in armed conflicts. However, while potential military threats are declining, international terrorism and organized crime are on the increase. Thus, opportunities rather than threats are the motivating concerns for the Government. That is to say, one wants to know what objectives are or can be achieved with what resources. A particularly significant factor here is the deepened cooperation within the EU, manifested through the EU's security strategy and the EU's crisis management capability.

Critical Infrastructure Protection
Sweden must be able to meet both military and other threats, such as terrorist attacks. We must also be able to prevent and manage situations that, without posing a direct threat to our independence, could still cause a rapid and serious deterioration in the ability of our society to function. Certain socio-economic activities are vital to the day-to-day functioning and security of the country; for example transportation of goods and people, telecommunications, banking and finance, and the supply of electricity and water. These underlying services and functions often referred to, as components of the nation's critical infrastructure, are essential for all other production of services and goods. Domestic security and our ability to monitor, deter and respond to outside hostile attacks also depends on some of these activities as well as other more specialized activities, such as intelligence gathering, law enforcement and maintaining military forces. The critical infrastructure also seems to hold a symbolic value that goes even beyond the functional value of these activities functional value, a value that is closely connected to the notion of trust or public confidence.

Even though we speak in terms of protection of the infrastructure, it is essential to understand that it is not the infrastructures that we need to protect above anything else. It is rather the services facilitated and provided by the infrastructures that we need to focus our protective measures on.16 Only by applying a systemic protective approach that is targeted on ensuring continuity of critical services can our protective measures be truly successful.

Serious disruption in these activities and capabilities could have a major impact on the country's well being. Attacks on computer systems, negative publicity using the mass

[16] In the light of this, Jan Metzger has argued that it would make more sense to speak of "critical services robustness" or "critical services sustainability".

media, Internet spamming, and the threat of infrastructure failure has been symptomatic of operations in this new era. Information systems are providing lucrative targets for terrorist groups.

Terrorist groups could therefore wreak havoc by attacking the information systems that control electricity for hospitals, air traffic control or banking transactions. An "anonymous" source anywhere in the world might break into and disrupt the power grids of major cities.17 Attacking the power-grid is probably the most cost-effective way of causing damage and disruption to a society, so whether or not terrorists are only seeking to disrupt societies economically and the daily lives of its citizens or if they are aiming to cause as many deaths as possible is up for debate.

Only 1-2% out of all terrorist activity is sabotage on CIP/CIIP installations, but as terrorist networks have the quality of a learning organisation we could expect an increase in this area. It might be the case that we are sleepwalking towards an abyss if we do not start to pay attention to threats like this.

Matthew Devost has developed a tool, the critical infrastructure threat matrix, which can help visualize in a structured way the almost infinite threat variations possible in post-modern terrorism. Based on the dichotomy digitally and physically applied on the variables, the tool used and type of target terrorist attacks can be placed in one out of four categories.18

Critical Infrastructure Threat Matrix		Target	
		Physical	Digital
Tool	Physical	(a) Conventional terrorism.	(b) IRA attack on London Square Mile, 4 Oct 1992
	Digital	(c) Spoof Air traffic control to crash plane	(d) "Pure" Information terrorism

What drives concerns here is a sense of the vulnerability of essential national information infrastructures to various forms of attack, especially by malicious actors who are skilled in launching cyberspace-based threats.19

We do not suggest that terrorism in the information age will be a totally different creature from the traditional form of terrorism. Rather, we expect to see a great variation in the adoption of new possibilities brought along by the evolving information technology between different terrorist groups, ranging from conservative groups that will continue to solely put their trust on the effect of kinetic energy on traditional targets, to groups in the technological forefront that will move into information terrorism – that is what this is largely about.

---

[17] Nye, Joseph S., Understanding International Conflicts: an introduction to theory and history, 4th ed. (New York: Longman 2003) p.220
[18] Nicander, Lars and Ranstorp, Magnus (eds.), *Terrorism in the Information Age*, (Stockholm, Swedish National Defence College, 2004). p.14
[19] Arquilla, John and David Ronfeldt, The Emergence of Noopolitik: Toward an American Information Strategy (Santa Monica, CA: RAND, 1999) p.1

Interagency co-operation and interoperability
According to the Swedish 1996 defence programme, one of the overall objectives of the total defence system and the associated allocation of resources is to strengthen the capability of our society to prevent and manage severe peacetime emergencies. Total Defence consists of both a civil and a military part. These two parts work together, with their operations based on the same fundamental needs and concerns. Working together, the civil and military parts of the Total Defence organisation must be able to counter attacks and other serious threats to Swedish security.

Civil Defence includes the whole of the society and all its functions. Health services, emergency services, and the supply of power are examples of activities that must continue even in times of war. The Civil Defence organisation is thus more than just a public body - it comprises the vital functions of society. The issue of a nationwide joint radio communications system for the Swedish so-called protection and security services is of great importance for the capacity of our society to combat large-scale terrorist strikes and other similar events in Sweden.20

Terrorist attacks that are not of such a substantial kind that they can be classified, as armed attacks against a state should, as to date, basically be a matter for the Police. However, the Police do not always have the capacity to intervene against violent acts. For example would attacks from the air or underwater call for competence outside the Police. It should be considered that a competent authority from within the Police or Coast Guard, subject to certain preconditions, should be able to call for the assistance of the Armed Forces in such a situation.

The Ministry of Defence plays a coordinating role within the Government Offices and is also responsible for limiting the consequences of radioactive fallout, floods and dam bursts, as well as accidents involving chemicals and maritime discharges of hazardous substances, etc. Should a large-scale terrorist strike occur involving the use of NBC weaponry or if a threat is made that such means might be used, great demands may be placed on the special competence and material resources of the Police. In such a situation, the Armed Forces have NBC protective resources, primarily at present through the NBC Rapid Reaction Force, which can be deployed to temporarily support the Police.

The role of the Swedish Armed Forces in protection against terrorism is mainly to support other government authorities. Military responses alone are rarely successful, instead counter-terrorism operations have to be planned and executed in close cooperation with intelligence, customs, and police agencies. However, the laws governing this support impose some restrictions, and continued investigation is therefore needed urgently.

Intelligence and Information Sharing
In an environment dominated by threats of a non-military nature, there is an apparent need for transformation of the intelligence community, which fundamentally is a Cold War heritage. The threat from transnational terrorism has highlighted this need for

[20] SOU 2003:32. p 35, http://www.regeringen.se/sb/d/108/a/424, 2005-04-01

transformation. Meeting a dynamic and constantly changing threat will require agile and adaptive organisations, more capable of reorganizing themselves around new challenges as they arise. To achieve this the intelligence culture has to change. We also need to harmonize our strategic intelligence and analysis capacity, and agree on standards and methods for processing information and intelligence.

It is generally stated that defence intelligence operations may not relate to tasks that, according to law or other rules, fall within the framework of the crime combating and crime prevention work of the Police and other authorities. However, there is a growing consciousness that the intelligence assets of the Armed Forces should have a role also in combating terrorism.

We have seen how the part of the defence intelligence operations conducted to support Swedish foreign, defence and security policy has continued to grow in importance. The activity also includes Swedish participation in international security cooperation and, in assisting with intelligence to support our society in the event of severe pressure in peacetime. The Armed Forces have, in contrast to the Security Police, personnel abroad, which means that obtaining intelligence reports abroad that are important for the protection against terrorist strikes and also processing and analyzing such information, must reasonably be a task for the Armed Forces[21]. The Armed Forces, within the framework of their own intelligence operations, need to enhance their capacity in order to collect, process and analyze intelligence concerning international terrorism.

We need to develop forms and forums for the exchange of intelligence methods as well as operational information between the military and civilian parts of the intelligence community. We also need to create the necessary judicial and organisational arrangements so that the limited resources of the National Police can be reinforced with special competences from the Armed Forces. Collaboration of this kind would necessarily be based on permanently employed military personnel being put under the command of a Police Commissioner.22

Existing inter-governmental undertakings in this field can be greatly enhanced. Exchanges between national services will always be on the basis of trust. It is difficult to assess whether or not transformation to a joint armed forces-police intelligence board is likely to enhance the confidence for these types of operations. However, it is likely that a new order would, from this perspective, have rather positive consequences.

International Counterterrorism Operations

The horrifying terrorist attacks on 11 September 2001 made it clear that international terrorism is a threat to international peace and security. The use of force is permitted only as a last resort and when authorized by the Security Council, unless it is an act of self- defence. Sweden is a staunch supporter of the UN. While advocating reforms, we believe that the core principles of the UN Charter remain as valid as ever. Threats to

[21] SOU 2003:32. p 34, http://www.regeringen.se/sb/d/108/a/424, 2005-04-01

[22] SOU 2003:32. p 27, http://www.regeringen.se/sb/d/108/a/424, 2005-04-01

international peace and security must be met collectively. The development of the European Security and Defence Policy changes the prerequisites of Sweden's security and defence policy.

The decisions taken in recent years have radically changed the tasks assigned to the Swedish Armed Forces, and the capability to undertake operations, above all international operations, is the single factor that will have most influence on the activities of the Armed Forces.

The creation of a better international coordination and joint action are essential and should help to compensate for the fact that judicial and law enforcement systems are still mainly national, whereas national borders have become much more porous in ways that facilitate international terrorism and crime-syndicates. The UN and the EU are central actors in this process, but NATO and the OSCE have each shown the potential for more consistent and comprehensive counter-terrorism cooperation.

Bringing Soft Power23 into the Equation

Policies for the advancement of democracy and human rights demand tact and serious consideration of soft power instruments. Soft power encompasses the ability to influence the international political agenda and thereby shape the preferences of others.24 If a country's culture and ideology are attractive, others more willingly follow, for example if the United States manages to represent norms and values followed voluntarily by other nations, it will have less reason to use expensive hard power instruments. Soft power, then, is more than persuasion. It is, above all, the ability to encourage emulation, to a large extent founded on attractive ideals.

When a country's culture includes universal values and its policies promote values and interests that others share, it increases the probability of obtaining its desired outcomes because of the relationships of attraction and duty that it creates.25
Soft power and free information, if sufficiently persuasive, can change perceptions of self-interest and therefore the way in which hard power and strategic information is used. For example, closed societies can more easily deny knowledge to rival open societies than open societies can to them. On the other hand, a technologically advanced society can more easily gain access to information about its less technologically advanced opponent, even if the adversary's society is a closed one, than the opponent can gain about it.26

---

[23] Joseph Nye and Robert Keohane argue in favour of a fundamental division of power into two categories, one consisting of actions and the other based on resources.[23] Action power, in turn, can be divided into hard and soft power. Hard power means the ability to make others behave in a way they would not otherwise do. This is accomplished primarily by threats and punishments or by rewards. Soft power is derived from appealing assets like cultural attraction, political values, and social conditions esteemed by others. This is not a new phenomenon. Historically, the United States and other great powers have always tried to capitalize on their reputation and ideology. While hard power will always be the core means for a state to secure its sovereignty, soft power is gaining in importance when it comes to solving transnational problems.

[24] Political philosophers like Machiavelli and Hobbes believed that violence and coercion were at the root of all politics, and Max Weber believed that the foundations of the state itself are predicated upon its possession of a monopoly of legitimate violence.

[25] Nye , Joseph S., *Soft Power: The means to success in world politics* (New York: Public Affairs, 2004). p.11

[26] Vertzberger, Yaacov Y. I., *The World in Their Minds: Information Processing, Cognition, and Perception in Foreign Policy Decision-making* (Stanford CA. Stanford University Press, 1990. p. 23

Government policies can reinforce or squander a country's soft power. Soft power, then, is more than persuasion. It is, above all, the ability to encourage emulation, to a large extent founded on attractive ideals. 27 One could argue that while the aims of a war or military campaign have not changed, the methods of waging it have.

Influence Campaign

As we mentioned in the introduction, the root causes of terrorism can be interlinked with poverty. It is not per se a cause of terrorism, but it cannot be ignored in the fight against terrorism. Poverty together with oppression, insecurity, intolerance, absence of democratic structures and a lack of political freedom are all part of the breeding ground. For most people, it is clear: fanaticism and fundamentalism exploit people's sense of injustice and lack of hope.

In the US-led invasion and occupation of Iraq, it has intensified many Muslims' worries about America's global intentions, and made some more sympathetic to Osama bin Laden's propaganda. Both bin Laden and Saddam's regime characterized an attack on Iraq as the opening of Pandora's box. The regime also advanced the argument that a war would create more terrorists, since an attack on Iraq would be considered as an attack on Islam as a whole. To mobilize the sympathy the regime cited the large number of innocent civilians affected by an invasion. The al-Qaeda leadership has, after the 'war' ended, been able to portray the Iraq war as confirmation of the view that Washington wishes to dominate the Arab and larger Muslim world politically and militarily, and that Washington intends to loot Islam of its economic resources, in particular, oil.

The terrorists use mass media and the Internet to reach their target audiences and they have become skilled in using the media to reinforce the psychological effect of their strikes.28 Terrorists are depending on getting their messages out quickly to a broad audience. This means that terrorists depend crucially on soft power for its ultimate victory.

Intelligent action for bringing about a result of some kind in a political system, such as a change of policy or a settlement of an international dispute, requires knowledge in how to produce or cause these results. The ability to attract support from the crowd is at least as important as the ability to destroy the enemy's will to fight.29 Terrorists are not able to pay attention to all sources of information available to them and then decide what is relevant. Attention is often a scarce resource and is therefore selective. Using Influence Operations, which is the integrated planning and employment of military capabilities to achieve desired effects across the cognitive battle space in support to operational objectives, could be the way to go[30].

---

[27] Keohane and Nye's soft power is related to actor interest that has been taken for granted. These static notions are under scrutiny by analysts situating their arguments in historical sociology, a growing tradition in international relations, usually referred to as constructivism.

[28] An example of this is the widespread dissemination of bin Laden interviews after September 11 and the gruesome hostage decapitation videos.

[29] Nye, Joseph S., *Soft Power: The means to success in world politics* (New York: Public Affairs, 2004). p.22

~~30~~ Psychological operations (PSYOPS), military deception (MD), operations security (OpSec), counterintelligence (CI), and public affairs (PA) are elements of influence operations.

The core of any decision-making and information processing operation is the human being, whose personality has a decisive and sometimes dominant effect on the manner and outcomes of information processing. We have to comprehend how information becomes available and is attended to, being analysed, integrated and interpreted- in other words how terrorists construct a view of the world in their minds.31 In order to proceed, we need to assume that terrorists in a confrontation would be rational with a substantial degree of rational thinking and calculation, even though this rationality may not be the same as a Western mind would pursue.

It may also be helpful to bear in mind that, unlike in the wars against drugs and crime, in the struggle against terrorism, increasing favourable exposure to democratic societies and values is crucial. Shaping opinions becomes even more important where authoritarian governments have been replaced by new democracies. Indeed, in an article published in 2002 in *Foreign Affairs,* Sir Michael Howard writes "it is fundamentally 'a battle for hearts and minds' ... without hearts and minds one cannot obtain intelligence, and without intelligence terrorists can never be defeated."32

With the advancement of technology and in this context, military advice on how to keep the public domain informed in a real-time manner is crucial. In addition, the military needs to advise on how to operate and tailor reports in a news cycle that is now 24x7x 365".33 If military forces are to take advantage of information, their behaviour must seem credible. The numerous examples of how human rights and fundamental freedoms are put aside in the name of fighting terrorism go against this notion. For this reason Sweden has advocated that efforts for fighting terrorism should be carried out in compliance with human rights. Therefore there is a need to discuss critical issues, such as the legal challenges and responses to international terrorism.

Particularly in peacetime, perception management and psychological operations are, like the intelligence services, "an extremely forbidden necessity" for the strategist who wishes to succeed. The means with which one could define the "war of ideas" has grown to include television, the Internet, and other means of informing the world. For an influence campaign to succeed, you therefore cannot wait until hostilities have begun. By trying to force governments to be proactive instead of reactive, and concerned with the politics of ideas— the concept of Information Operations is to be seen as a way of harnessing and expressing the "soft power" of Western ideals, so as to attract, influence, and lead others.

A Coherent Information Operations Strategy

In addition to changes in academic theory, there has been a substantial change in the nature of strategic, operational, and tactical issues as well. Previous military theories held that strategic concerns were normally a global issue. Now there are numerous events at the tactical level that can quickly elevate to affect the global level with the

[31] The epistemological quest for securing the bridge between the self and the world is replaced by a description of modes of being in the world.
[32] S/PV.4453, Säkerhetsrådet, Fifty-seventh year, 4453rd meeting, Friday, 18 January 2002, 10 a.m., New York
[33] Urrutia-Varhall, Linda R. *Public Diplomacy: Capturing the Information Terrain On The Way To Victory*. (Maxwell Air Force Base, Alabama, 2002) p.7

use of advanced technology or mass media.34 In fact, as many people realize, with today's new technology often the smallest incidents can spark international or strategic concern. In such circumstances, public diplomacy and strategic communication aimed both at public opinion and to counter terrorism can become as important to outcomes as the traditional classified diplomatic communication among leaders.35

Meanwhile, less attention has been given to the development of soft power as a basis for a national strategy for Information Operations. Strategists rarely convene to discuss this concept, and mainly a small number of publications measure its influence, although increasingly. If 'soft power' can be applied more usefully in the coming year it can, become an important instrument - along with a more comprehensive set of tools - with which to combat the al-Qaeda network, as well as its regional affiliates. Our analyses suggest a long-term strategy that should reduce the incentives and opportunities for terrorists to sustain their activities.

In fact, in this fourth generation of warfare, the global information environment has become a battle space in which the technology of the information age is used to deliver critical and influential content in order to shape perceptions, influence opinions, and control behaviour. "This new battle space is focused on the "wetware", that is, the "grey matter" of the brain in which opinions are formed and decisions are made. The most, perhaps only, effective "weapon" in this battle space is information, and the hallmarks of that revolution, such as the transparency of events and the global immediacy of coverage, have only heightened the importance and impact of Information Operations."36

Therefore, in this post-Cold War era, the fungibility of information and the use of soft power by nations have greatly increased the need for a mechanism to coordinate a coherent message. Consequently, a coherent IO strategy, integrated with the day-to-day operations, is essential to counter these asymmetrical adversaries.

Concluding remarks

Democratic governments have a particularly difficult position in confronting the new terrorism. There are no short cuts; human rights must be respected, international law must be followed. All states must work together to preserve a democratic, secure and open society. Since the fight against terrorism requires a multidimensional and multinational approach, it calls upon a strategy that combines military and civilian sectors to collaborate in combating terrorism.

Al-Qaeda may be increasingly dependent on local groups and subject for dispersing impulses, but it remains a viable transnational terrorist organisation. To win, nations must successfully integrate political action to gain international support and neutralize the terrorists, thereby not having to utilize military power to destroy the ability of the terrorists to sustain themselves. The force that binds these elements of national power

---

[34] Armistead, Leigh (ed.*). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p.15

[35] Nye , Joseph S., *Soft Power: The means to success in world politics* (New York: Public Affairs, 2004). p.105

[36] Armistead, Leigh (ed.*). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p. xvii

together is information.37 Finally, as the RAND Corporation's John Arquilla and David Ronfeldt argue, security in the global information age will come not just from strong defences, but also from sharing information. As we share intelligence and capabilities with others, we develop common outlooks and approaches that improve our ability to deal with the new challenges.38

[37] Armistead, Leigh (ed.*). Information Operations: Warfare and the Hard Reality of Soft Power.* (Washington D.C, Brassey's Inc, 2004). p.6
[38] Nye , Joseph S., *Soft Power: The means to success in world politics* (New York: Public Affairs, 2004). p.134