Journal of Information Warfare

Volume 5, Issue 3

Contents

Journal of Information Warfare

Published by:
School of Computer and Information Science,
Edith Cowan University, Western Australia
ISSN 1445-3312

Online version published by:
Teamlink Australia Pty Ltd
ISSN 1445 3347

www.Jinfowar.com

Editorial

The last issue for 2006 includes a paper on propaganda, two on deception and another on the state of Belgian intelligence agencies. Taylor starts by outlining and critiquing the West's propaganda effort after illustrating its past. A renowned expert in this area, it would be interesting to see some comments about his assertions from readers. In the first paper on deception Yuill, Denning, and Feer posit a model for deceptive hiding. The second paper on this topic is by Brumley, Kopp, and Korb who examine the Orientation stage of the OODA loop and its relationship to deception and self-deception. Vanhorenbeeck closes this issue with an evaluation of Belgian and European intelligence services.

It is pleasing to see such distinguished academic contributing to the journal. Please keep the papers coming in. Your contributions help to keep the Information Operations community informed of work going on around the globe. The authors provide this service and I hope they continue to do so.

Bill Hutchinson

November, 2006

Email: w.hutchinson@ecu.edu.au

Authors

Lachlan Brumley graduated from Monash University, Melbourne with a Bachelor of Software Engineering. He is a doctoral student studying the effects of various perception errors on evolving life forms.

Dorothy Denning is Professor of Defense Analysis at the Naval Postgraduate School. She is author of *Information Warfare and Security*, and the recipient of several awards.

Fred Feer is retired from a career with the U.S. Army counterintelligence, CIA, RAND and independent consulting. Deception has been an interest and area of professional specialization for over 40 years.

Carlo Kopp, MIEEE, MAIAA, Carlo graduated from the University of Western Australia, in Electrical Engineering. After more than a decade in industry engineering positions, he completed a research Masters in Computer Science in 1996, and a PhD in 1999. His research interests include long range microwave data links, airborne ad hoc digital networks, strategy, doctrine and fundamentals of information warfare. He is a Research Fellow in Regional Military Strategy at the Monash Asia Institute, since 2005

Kevin B. Korb is a Reader in the Clayton School of Information Technology, Monash University, Australia. His research concentrates on machine learning and the philosophy of science and the interrelation between the two, and especially the automation of causal discovery. He is co-author (with Ann Nicholson) of *Bayesian Artificial Intelligence*, (2004). He was a co-founder of *Psyche: An Interdisciplinary Journal of Research on Consciousness*.

Philip Taylor is Distinguished Visiting Professor in the Faculty of Media and Communications, UiTM, Shah Alam, 2006, Professor of International Communications at the Institute of Communications Studies, Leeds University, UK, and Fellow of the Centre for Public Diplomacy, University of Southern California. He is the author of numerous works on information operations and propaganda.

Maarten Vanhorenbeeck is currently undertaking a Masters degree in Information Security and Intelligence at Edith Cowan University, Australia. He is a Service Delivery Manager with global information security services specialist *Cybertrust*.

Jim Yuill is a PhD candidate in the Computer Science Department at North Carolina State University. His thesis is on deception for computer security. Jim previously worked at IBM in operating systems development.

Conferences

7th Australian Information Warfare and Security Conference
4th and 5th December, 2006

4th Australian Information Security Management Conference
4th December, 2006

4th Australian Network, Information and Computer Forensics Conference
5th December, 2006

All held at Edith Cowan University, Perth, Western Australia.
Details from: http://scissec.scis.ecu.edu.au
or email: c.valli@ecu.edu.au

ICIW 2007: 2nd International Conference on i-Warfare and Security
Naval Postgraduate School, Monterey, California, USA
8-9 March 2007
Details from: http://www.academic-conferences.org/iciw/iciw2007/iciw07-home.htm

ECIW 2007: The 6th European Conference on Information Warfare and Security
Defence College of Management and Technology, Shrivenham, UK
2-3 July 2007

Details from: http://academic-conferences.org/eciw/eciw2007/eciw07-home.htm

International Conference on Human Aspects of Information Security & Assurance (HAISA 2007)
Plymouth, United Kingdom
10-12 July 2007

Details from: http://www.haisa.org

Strategic Communications and the Relationship between Governmental 'Information' Activities in the Post 9/11 World

Philip. M. Taylor

Institute of Communications Studies
University of Leeds, U.K.
Email: P.M.Taylor@leeds.ac.uk

Introduction

For most people, the word 'propaganda' conjures up all sorts of negative connotations – from brainwashing to dirty tricks to outright lying. Theoretically, this is misguided. However, although it is now probably too late in the day to attempt to strip away the negative connotations in the popular mind of this 'P word', nonetheless there is a need to first understand what propaganda actually is conceptually, and to understand how the word itself has acquired such a pejorative meaning, before examining what its contemporary alternative word descriptions (euphemisms) actually involve and mean.

Propaganda: 'a good word gone wrong'

Before the twentieth century, propaganda was not thought of negatively in the same way that it is today. The Vatican invented the word in the 17th century and used it in the name of a body it created in 1622 to counter the advance of the Protestant Reformation in Europe. The *Congregatio de Propaganda Fide* was formed to reinforce the believers in the Catholic faith – which was of course seen as the 'true faith' - against the challenge of what were then regarded as a new set of heretical ideas, namely Protestantism. However, this notion of competing faiths (or beliefs or ideas or values) was even older than this, and can be dated back at least to the Ancient Greek concept of 'rhetoric' which in modern usage means debate or communication. The word 'communication' derives from the Latin word *communicare*, which means 'to share'. Further back still, Sun Tzu in the fifth century BC discussed what is now called psychological warfare in his text, *The Art of War*. It was his advice that one needed 'to know the enemy and to *know yourself*' and, if this could be achieved, one might never need to take recourse to war. Victory could be achieved through persuasion and outsmarting your adversary. His text should be mandatory reading for anyone interested in today's practice of Strategic Communications, not least because we are still witnessing a battle of ideas, only this time on a global scale.

But it is no coincidence that the Vatican should come up with a new word within a hundred years of Guttenberg's invention of a revolutionary new form of spreading ideas other than by word of mouth, namely the printing press. In the late middle ages, the printing of books and pamphlets was the equivalent of the internet and helped to usher in the modern age, just as the internet today is leading us today to a post-modern – or Information – age. Although the ability to read in those days was limited to a relatively small number of people (that is, priests and princes), their role as opinion-formers in relating new ideas to their subjects or congregations created a power of the pulpit that was to remain significant until the arrival of the mass media at the end of the nineteenth century.

Although propaganda had been used in nineteenth century conflicts such as the American Civil War and the Crimean War, it was the Great War of 1914-18 which saw its modern use come of age (Sanders and Taylor, 1982)· The Great War saw the amalgam of propaganda as

ISSN 1445-3312 print/ISSN 1445-3347 online

both an art and a science. Its principal functions were twofold: to bolster morale at home by promoting civilian support for the long armed conflict, and to attack the enemy. Just as the invention of printing had created the word 'propaganda' by the Vatican, so the arrival of the mass media by the time of the Great War gave modern propaganda the characteristics is has today. But it also opened up a gap between image and reality. The new technology of cinema, for example, though still silent at that point in time, was deployed to maintain morale on the home front - and put paid in the process to the myth that the 'camera never lies'. Indeed, one would have had no idea of the mass slaughter taking place on the battlefields of the Western Front by watching such films as *The Battle of the Somme* (1916) (Reeves, 1986). Soldiers returning home from the front on leave were shocked by the war fervour and enthusiasm they encountered amongst the civilian population back home, and by the consequent perceptual gap that had clearly opened up between the civilian image of the war and the reality of the soldiers' experience.

In Britain, atrocity propaganda about the 'Beastly Hun' who had raped and pillaged his way through 'Poor Little Belgium', bayoneting babies and burning churches in the process, may well have sustained the civilian populace's will to continue to support the war by hating the enemy despite all the hardships it brought (Read, 1942). But it also did much to discredit the word 'propaganda' and to associate its popular meaning thereafter with negative connotations. After the war, when it was discovered that much atrocity propaganda had been contrived, the practice of propaganda came to be associated with half-truths or, at worst, lies. Arthur Ponsonby's best-selling book, *Falsehood in Wartime* (1926), even went so far as to suggest that 'the injection of the poison of hatred into men's minds by means of falsehood is a greater evil in wartime than the actual loss of life. The defilement of the human soul is worse than the destruction of the human body'. In other words, it was, as one British official stated in the 1920s, 'a good word gone wrong' (Taylor, 1999). What was essentially a word describing a value-neutral concept, was ruined, perhaps forever.

So what is propaganda?

The very first academic investigations of the wartime propaganda, notably Lasswell's *Propaganda in the Great War* (1927) tried to look at the experiment more dispassionately than did Ponsonby. Lasswell was also, of course, the author of the famous transmission model of communications which defined it as a process involving who said what to whom, in what channel (that is, how?) and with what impact. But, curiously, there is a word missing here, betraying perhaps Lasswell's training as a psychologist and political sociologist. That word is 'why?' For it is only when we add this question to the transmission model that we can begin to distinguish propaganda from other forms of persuasion such as marketing, public relations and advertising. In the considerable body of research into propaganda as a form of communication since Lasswell's pioneering work, many scholars have come to the viewpoint that propaganda can only really be studied as a *value-neutral process.* In other words, propaganda is neither a 'good' nor a 'bad' thing – although it can be used for good ('positive') or bad ('negative') purposes. The key point here concerns the source and who benefits. If we therefore ask the question 'why is the propagandist disseminating this message to a certain target audience?' we can begin to make value-judgements about those motives rather than about the process itself. Although there is such a thing as accidental propaganda, most campaigns since the First World War have been carefully *planned.* As such, they have an *intention*, and it is those intentions we need to study carefully. Whether any given campaign was successful or not (that is, with what impact) is irrelevant for the purpose of definition - except in terms of evaluating whether the propaganda was 'effective' or 'ineffective'. If, therefore, the intentions of the persuader are studied, and someone is able to judge whether they were motivated *more by a desire to benefit the source rather than the recipient*, propaganda is beginning to be distinguished from other forms of communication. Think of propaganda as being on a spectrum of communications with deception at one end and education at the other. Deception is about lying – although in wartime especially, it can be justified if it aids victory against an enemy. On the other hand, in most educational systems that are dedicated to discovering 'the truth', the curriculum is designed to benefit the recipient (or student) rather than the source (or teacher or educational institution) although sometimes, one does question whether this actually applies in practice.

There are many definitions of propaganda, including those from the opposite school of thought which argues that propaganda can never be justified because it is always about manipulation of information and it is always designed to benefit those doing it. This line of thinking can never accept philosophically that the means justifies the end. This school of thought (which includes the French writer Jacques Ellul (1965)) points to the historical *abuse* of propaganda by the Nazis and other totalitarian regime's like Stalin's Russia or Mao's China. Because these historical examples have invariably created negative effects, and because propaganda in such cases involved what Joseph Goebbels called 'The Big Lie', this school of thought can never accept that propaganda can be anything other than manipulation of information and communication to benefit the 'bad' intentions of those doing it. However, we need to remember that while propaganda does indeed involve the manipulation of information by omission as well as by commission, so do other forms of communication – including journalism. It would be thus disingenuous to suggest that propaganda is something quite different from other forms of persuasion that are equally designed to benefit the source, such as advertising ('commercial propaganda' designed to increase profits), public relations (sometimes called 'spin' in order to make the source appear in a positive light) – or even journalism (also 'commercial propaganda' designed to increase profits of proprietors).

Journalists in democratic societies, of course, will always insist that their role is to 'search for the truth', and to act as a watchdog of the ruling elite on behalf of the people. This is also problematic because it assumes that there is such a thing as 'The Truth' instead of more realistically recognising that, in our complex information age, there are in fact 'Many Truths'. This is because there are 'Many Voices' in a world which encourages the democratisation of information through the spread of communications technologies such as computers, the internet and mobile phones. Since the invention of printing, we have been undergoing a 'communications revolution' – a revolution which is getting faster and faster. Indeed, now communications has become the lifeblood of the twenty-first century and it is every bit as significant as oil and gas were for the twentieth. Those 'many voices' who communicate their 'many truths' today are, in fact, in competition with each other to establish which set of truths has most *credibility*. Credibility is the most important quality for anyone wishing to convince others that they should accept 'truth x' rather than 'truth y'. And the easiest way to lose credibility is to lie, to be exposed as a false source of information or as a source of misinformation and disinformation. In other words, propaganda is really a competition for credibility or for 'credible truths'.

One definition of propaganda used by the NATO Alliance is now examined. This definition is interesting because it was originally agreed by 16 *democratic* nations, and adopted by a further 10 nations as the alliance was expanded to include newly democratised nations that were formerly members of the Communist block before the end of the Cold War. The NATO definition of propaganda is as follows:

> *Any information, ideas, doctrines or special appeals, disseminated to influence the opinions, emotions, attitudes or behavior of any specified group,* ***in order to benefit the sponsor****, either directly or indirectly (emphasis added).*

The thing to note here is that there is no indication of whether propaganda under this definition needs to be truthful or deceitful. However, if it is deceitful, and is found to be such, it is unlikely to have any impact because it will lack credibility. The key point rather is that it is designed to benefit the source.

The transformation of the terminology

In fact, during the course of the twentieth century, democracies have developed certain 'rules' for conducting propaganda which distinguishes their techniques from those used by authoritarian regimes. The first and most obvious of these rules is that they avoid the word 'propaganda' like the plague. Instead, all sorts of euphemisms have been used – from 'information' policy to, now, information warfare or, less harshly, strategic communications – in an effort to distance what democracies do to influence public opinion from what authoritarian and totalitarian regimes have done and, at least for those such states which survive, continue to do. So 'they' have Propaganda Ministries which 'tell lies' while 'we' have 'Information Ministries' and therefore 'tell the truth'. Such polarization is, of course in itself, a form of propaganda.

The second rule – or perhaps self-deception is more appropriate – is that democracies only conduct 'white' propaganda. Most propaganda analysts identify three different types of propaganda (and related activities such as psychological warfare), which are once again related to the source or originator. These are black, white and grey. 'Black propaganda' is another of those frequently used but, rarely understood, terms. Politicians often use the phrase when referring to propaganda which they see as designed to 'blacken' their character or reputation. In fact, the term relates to the way the source either tries to hide, or blatantly deceives about the nature of, its real identity. Black propaganda pretends to be from somewhere other than what it really is and, because it is born of a lie, it can be a lot more 'economical with the truth' than other forms of propaganda – until the real source gets uncovered. One suspects that the popular suspicion of propaganda as a negative process comes from this type of activity although black propaganda depends for its success upon its ability to keep its true origins secret. One of the realities of today's global information environment is that it is very difficult, if not impossible, to keep such activities secret anymore – or at least not for very long.

However, in the past, black propaganda has been used to great effect, especially in wartime. It is very close to another time-honored wartime device, namely deception, but with a twist. For example, in World War Two, the Nazis were so afraid of 'alternative truths' that they banned the listening to foreign broadcasts, under penalty of death. This created a severe conundrum for Allied propagandists – how to get their message across to people who dare not listen to it. So they came up with the idea of pretending to be Germans speaking to each other. For example, they would broadcast conversations between seemingly disaffected German soldiers or resistance fighters on domestic frequencies in order to foster rumors and spread disaffection so that any 'innocent' German listener would think that the war was not going as well as the Nazi authorities were maintaining. How effective this black propaganda actually was is impossible to say – but it certainly worried the Nazis.

Because its source was secret and disguised, black propaganda could be a little more liberal in its adherence to the 'truth', although it still needed to be credible. To attract audiences, it would frequently use banned music such as jazz and the language used could be florid. White propaganda, on the other hand, openly admitted its origins. Leaflets were usually white because their messages obviously came from the enemy whereas in World War Two white radio broadcasts were left to organizations like the BBC. It is known that the BBC was widely listened to in German-occupied Europe – despite fear of the death penalty - and it developed a reputation during World War Two as a highly credible source of information that would survive well into the late twentieth century. Credibility takes time to establish but can quickly disappear. The British wartime white propaganda 'rule' was to tell 'the truth, nothing but the truth and *as near as possible the whole truth*'. It was, of course the British version of the 'truth' – it was their truth deployed in order to attack enemy 'lies'. When the Americans entered the war in late 1941, they adopted a similar approach, which they labeled the 'Strategy of Truth'. Both could perpetuate this appearance because their black propaganda activities were conducted in such secrecy that it was only after the war that they came to light.

This was what the British called 'political warfare'. But when the Americans entered World War Two after Pearl Harbor, their preferred label of Psychological Warfare (or PSYWAR) eventual prevailed in the semantic evolution. PSYWAR became a subset of propaganda, and was usually referred to as propaganda directed against an enemy or potential adversary, chiefly with the purpose of generating behavior that would lead to surrender, insurrection, desertion or defection. It also had black, white and grey forms. Leaflets dropped over enemy lines, or messages transmitted by loudspeaker teams were usually white PSYWAR. Radio broadcasts could be both black or white but because, in wartime, listening to enemy radio broadcasts could be construed as an act of treason, black radio messages were most likely to produce the desired effect. Grey propaganda is usually defined as that in which no source is identified.

During the Cold War that lasted from shortly after the Second World War to the end of the 1980s, however, white radio broadcasts became a significant weapon. The Cold War was essentially a struggle between two political ideologies, between two different ways of life, and between two contrasting 'truths'. It was a global struggle for hearts and minds and it saw propaganda in all its forms transform from a military weapon into a strategic necessity. Propaganda permeated every aspect of national and international affairs, from national democratic elections to international events such as the Olympic Games, the Space Race and the small wars or 'low intensity conflicts' that were waged instead of a fully blown nuclear war. For the first time, the western democracies created elaborate peacetime propaganda machineries, with the United States Information Agency (USIA) being created in 1953 to co-ordinate the combat against the spread of communist ideas. Once again, however, the West insisted that this was not propaganda or counter-propaganda but rather 'information' designed to enlighten the 'truth-starved' peoples of the Soviet Union and Eastern Europe. To deliver that 'truth', Radio Liberty and Radio Free Europe were created to supplement the Voice of America to enlighten the oppressed and the ignorant. The Soviets responded with widespread jamming, spending more on preventing the western version of the truth from reaching their own people than they actually did in responding with their truth via Radio Moscow. Together with the highly credible BBC World Service, these western broadcasts were known to the KGB as 'the voices' – but ones that must be silenced.

The battle of ideas 'won'

This competition lasted for just over 40 years. It was in many ways a forerunner of the new 'battle for hearts and minds' that characterizes the post 9/11 era. However, as will be illustrated, the global information environment of the 21st century is markedly different from the Cold War era. Indeed, it was during the transformation period of the 1980s, when new communications technologies like commercial satellites and computers first appeared to challenge the limitations of the old mass media, that the battle between free market liberal capitalist democracy on the one hand and communism on the other was 'won' by the West. Some scholars would argue that this battle was in fact 'lost' by the Soviet Union as it imploded in the wake of its invasion of Afghanistan, the deaths of a succession of its leaders after Brezhnev and its economic collapse. However, the American President, Ronald Reagan, must also take some credit. Known as the 'Great Communicator', Reagan fully understood the power of communications to spread ideas, perhaps learned during his period as a Hollywood movie actor. In the 1980s, he reinvigorated America's external propaganda efforts against what he described as an 'Evil Empire' and the full force of American technology was mobilized to bring light to the darkness of the Soviet system. He had an unwitting ally in the form of Mikhail Gorbachev, who became Soviet leader in 1984. Gorbachev knew that reform of the Soviet system was inevitable if it was to survive in the era of transformation and he introduced the policy of *glasnost* ('openness') to facilitate internal debate as to how this should come about. He stopped jamming the western broadcasts and encouraged hitherto unknown phenomena such as investigative journalism. He recognized that information from outside could no longer be blocked with the arrival of satellite television, fax machines and even the internet. In other words, he allowed 'the voices' to be heard. In the process, Gorbachev seriously miscalculated: the end product of his initiatives was not reform of the Soviet system, but its collapse.

Public Diplomacy

Reagan reinvigorated two key elements of American informational power. The first of these was known as Public Diplomacy (PD). This phrase was first coined in 1965 by Edmund Gullion, dean of the Fletcher School of Law and Diplomacy at Tufts University, USA, when he established the Edward R. Murrow Centre of Public Diplomacy. The founders were keen to avoid using the word 'propaganda' but recognised privately that that was what they were dealing with. One of the Centre's early documents, however, described PD in the following terms:

> *'Public diplomacy… deals with the influence of public attitudes on the formation and execution of foreign policies. It encompasses dimensions of international relations* ***beyond traditional diplomacy****; the cultivation by governments of public opinion in other countries; the interaction of private groups and interests in one country with another; the reporting of foreign affairs and its impact on policy; communication between those whose job is communication, as diplomats and foreign correspondents; and the process of intercultural communications.' (Emphasis added)*

This new phrase formally recognised information as an instrument of national power, alongside diplomatic, military and economic power (sometimes known as the DIME paradigm - Diplomatic, Information, Military and Economic power). Although Public Diplomacy had been a feature of international relations for some time – the Europeans had coined the phrase 'cultural diplomacy' many years earlier – it was now a norm in international relations, part of the very fabric of the Cold War.

Public diplomacy not only embraced international broadcasting as a short-term measure to provide news and information to foreign audiences but also long-term activities such as educational exchanges, international conferences and exhibitions, and the establishment of libraries in foreign cities - all of which were designed to build long-term *mutual* understanding, benefiting *both* source and recipient. It was in this sense that Public Diplomacy differed from other forms of international propaganda because, although it was obviously designed primarily to benefit the source, it had *mutual* benefits for the recipient as well. Public Diplomacy was based on the principle that 'to know us is to love us' – a risky business because sometimes, as the old phrase has it, 'familiarity breeds contempt'. However, the democracies felt that Public Diplomacy was a useful lubricant to normal diplomatic activities, especially during an era when thousands of nuclear warheads were aimed at the cities of the world threatening global annihilation. The Cuban Missile Crisis of 1962 brought this terrible possibility to its closest point. Public Diplomacy's principal goal was to foster greater mutual knowledge and understanding and, in the process, foster greater co-operation rather than conflict. It was, in a sense, 'propaganda for peace'.

Unlike 'the voices' which were aimed at audiences that possessed short-wave radio receivers, Public was largely directed at elite audiences – the 'movers and shakers' of foreign societies. These included opinion-makers rather than foreign public opinion *per se* – people like journalists, teachers, politicians and other influential people who might transmit their knowledge down to their own domestic audiences. The importance of educational exchanges cannot be underestimated in this activity. It was believed, in the 'to know us is to love us' philosophy, that if students were able to study in the West (or East) they would learn not only the language of their host country but also its culture, people and dreams. They would hopefully adopt their host country as their 'second home' and, upon returning to their own society as the 'movers and shakers of tomorrow', would be able to counter the stereotypical domestic propaganda disseminated by their own governments which, for whatever reasons, were pursuing their own agendas. Of course, if this did happen, it would benefit the host country – which is why it can be legitimately be described as propaganda.

The problem with Public Diplomacy is that it is very difficult to measure its effectiveness. It is about 'influence' – a very intangible concept. And because, historically, it has been conducted by the richer powers, it has been accused of being a form of media or cultural imperialism. The British have the British Council, Germany has its Goethe Institute, the French have the *Alliance Française* and the Italians have their *Dante Alighieri Society.* The Americans have avoided a similar institution, preferring instead to let trusts such as the Carnegie and Rockefeller Foundations look after the educational exchanges while US private enterprise – from Hollywood films to McDonalds and Coca Cola – are left to spread American products – and presumably capitalist values – in their wake. This has led to charges of 'McDomination' and 'Coca-colonialism' – a negative accusation – but this really misses the point about Public Diplomacy, namely that it is about mutual co-operation rather than conflict or what some describe as imperialism of the mind. But if it is to be truly mutual, in the age of globalisation, smaller nations also need to get into the business of public and cultural diplomacy if their voices are to be heard amidst the competition that takes place in today's global info-sphere. Rather than being seen in a negative light, Public Diplomacy is really 'propaganda for peace' because the intent is to promote international understanding and to remove negative stereotypes that can lead to international tension and even war. But the question remains that, if it benefits the recipient as well as the source, is it really propaganda?

Psychological Operations (PSYOPS)

The second area reinvigorated in the 1980s by Ronald Reagan was military psychological operations (or PSYOPS). After World War Two, the Americans allowed their psychological warfare capability to go into decline although, within five years, they found they needed to communicate with enemy soldiers once again on the battlefields of Korea (1950-53). Most of this activity was confined to leaflet drops and loudspeaker messages, although there was a radio station based in Japan that was used to address the North Korean population. After the war, in recognition of the specialised nature of this communication, the military established the Fourth Psychological Operations Group at Fort Bragg, North Carolina. In 1953, the USIA was also created to act as a dedicated Public Diplomacy agency to oversee the strategic communications elements of the Cold War. But as American and Soviet soldiers never actually faced each other directly on the battlefield, the use of PSYOPS was limited. The British, however, found it a necessity as they engaged in small wars and insurgencies created by their retreat from Empire. The undisputed master of this art was General Templar whose experience of out-psyching the communists in Malaya in the 1950s made him a man the Americans needed to consult when they found themselves increasingly embroiled in the Vietnam conflict of the 1960s.

But with America's defeat in Vietnam, PSYOPS once again went into decline – until Reagan became President in 1980. Thereafter, the Fort Bragg capability was built up and the results could be seen during the 1989 invasion of Panama when PSYOPS units were an important part of the campaign to capture General Noriega. However, the real breakthrough was to come in 1990-91 in the aftermath of Iraq's invasion of Kuwait and the formation of a US-led, UN backed, international coalition of 30 nations to use 'all means necessary' to expel Saddam Hussein's forces. Operation Desert Storm, as it was known, proved to be a triumph for PSYOPS when almost 70,000 Iraqi soldiers chose to give themselves up in response to US messages that they should 'surrender or die'. The US had by then an impressive array of communications equipment to get such messages across, including mobile print facilities for leaflet production (almost 30 million were dropped over Iraqi lines), portable radio transmitters and a unique flying broadcast platform known as Volant (later Commando) Solo. This was a converted Hercules EC 130 aircraft capable of world-wide broadcasts on radio and television. The majority of surrendering Iraqi soldiers told their captors that they had either heard the radio messages and/or seen the leaflets – even though it was forbidden to do so.

PSYOPS now began to be heralded as a 'combat force multiplier' – a form of military communications that, if deployed effectively, could play a significant part in assisting the military mission. It could also save lives, especially by getting soldiers off the battlefield who did not want to be there in the first place. In less than 50 years, the moral philosophical condemnation by Ponsonby that 'the injection of the poison of hatred into men's minds by means of falsehood is a greater evil in wartime than the actual loss of life' had turned full circle. The difference was that white PSYOPS had learned that 'truth was its best propaganda'.

It was quite a different matter when it came to black operations. In Kuwait, the international coalition's function was to expel Iraqi forces from the country – and nothing else. After a month of coalition bombing and a land offensive which lasted just 100 hours, the coalition had succeeded in its role. However, something then happened which was to have serious long-term consequences – or 'blowback'. Certain radio stations purporting to be something they were not – that is, black radio – began to encourage the Kurds in the north of Iraq and the Shias in the south to rise up against Saddam Hussein's regime. The overthrow of Saddam was not sanctioned by the international community – at least not yet – and hence these black radio messages broke a golden rule of propaganda: do not promise what you cannot deliver. They were probably run by 'other governmental agencies' (that is, the CIA) rather than the white propaganda inclined people at Fort Bragg. When Kurdish and Shia uprisings accompanied the end of the war, no help was forthcoming from the coalition; how could there be assistance when it was not part of the policy? Saddam's forces brutally crushed the uprisings, while the legacy was a sense of betrayal and resentment that was to come back and haunt the coalition just over ten years later when, once again, American and British forces invaded Iraq in 2003. When one British PSYOP leaflet reassured the Iraqi population that 'this time we will not let you down', the legacy of betrayal from the 1991 war merely prompted the response that 'we do not believe you'.

The legacy of this 'Desert Storm blowback' on the Global 'war' on terror cannot be underestimated, especially on the American experience in Iraq after 2003. It is an example of how short-term thinking in black PSYOPS campaigns can have long-term consequences for white strategic communications. Deception in today's info-sphere is bound to be found out because there are too many 'info-players', too many voices searching to expose one version of the truth as a lie. This is the reality of today's communications environment.

The American definition of PSYOP is:

> *Operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups and individuals.* [Joint Publication 3-53, 2003]

Like Public Diplomacy, therefore, this is communications directed at foreign audiences. In fact, it is technically illegal for the US government to conduct propaganda (including Public Diplomacy and PSYOPS) against the American people, under the 1948 *Smith-Mundt Act*. Does this mean that no form of official communication to domestic audiences takes place? For an answer, yet another 'P' word needs to be examined – namely Public Affairs.

Public Affairs

Certain American Presidents – Franklin Roosevelt, John F. Kennedy and Ronald Reagan amongst them - were extremely adept at communicating a positive image to their own electorates. However, not every President was so naturally skillful and, especially following the Watergate scandal in the early 1970s which saw Richard Nixon ousted by a disgrace revealed through investigative journalism, there has developed a machinery for the 'selling of the President'. This is what is now called political communications – or political propaganda since the intention is to keep the President's policies before a supporting electorate, and thus to see him re-elected. American Presidents since F D Roosevelt can only be elected twice, so this intention is more evident in any given President's first term of office. Second term Presidents, where they have occurred, tend to be characterized by their 'legacy to history'.

In Europe, the government's information activities with the media and public tend to be called 'Public Information' or 'Press or Media Relations'. Once again, it needs to be remembered that democratic governments do not like to admit that they are in the business of propaganda and argue instead that this type of activity is part of their democratic responsibility to keep their people informed with facts and factual information. If they lie –

and get found out – political heads usually roll. But does this mean that they only tell 'the truth'? In fact, rarely is the 'whole truth' being told. Facts are selected to support political arguments and this process of selection has given rise to the label of 'spin'. The phrase 'spin doctor' is relatively recent, but the use of the word 'doctor' to describe this form of political communications implies that they are trying to 'fix' (or heal) something that is already sick. There is an old phrase that 'when war breaks out, truth is the first casualty'. It could be cynically added that 'when politics breaks out, the first casualty urgently requires a spin doctor'.

Of course, a great deal of academic research has now been undertaken into government-media relations, in war as well as peace. In order to ascertain whether the free media are being used by governments for propaganda purposes, again the question of intent needs to be examined. Is the communications process being undertaken to benefit the recipient (journalists and, through them, the public) or the source (the government)? And is there anything wrong with that, especially if no one is lying? In a sense, techniques of official communication like those used in PSYOPS need to be confronted with the question: is it better to blow someone's head off rather than to persuade that head to lay down his weapon and live? Persuasion, after all, is an inherently human characteristic. From the clothes worn or the perfume used to the way people speak, every human being is sending out a message of some form. Why should politicians be any different? In other words, as long as these processes are understood, and are judgments are able to be formed about the intentions of those doing this activity, it should be accepted that, in a modern information age, politics *is* communications.

As such, Public Affairs are an official information activity of modern democratic governments that are riddled with propaganda intentions on domestic audiences. The intention is to benefit the source, although the pretension is that it informs the public. It may of course do both, which puts it closer on the spectrum of communications processes to Public Diplomacy. In the business of propaganda, there are no clear demarcations. For example, nations still talk in terms of 'domestic' and 'foreign' affairs but, in the age of the Internet, where does the domestic line end and the international begin, and vice versa? Is there any difference any more between what is said abroad and who hears at home? Can Public Affairs continue to pretend that its impact is solely domestic when the global flow of information is truly global? Marshall McLuhan's 1960s theory of a 'Global Village' is now a reality thanks to the internet.

9/11 and its aftermath

Nobody understands better that politics is communication than terrorists. Terrorism requires what Margaret Thatcher once described as 'the oxygen of publicity'. Media coverage of the carnage created is perhaps their greatest weapon, especially if it generates fear and prompts counter-measures which restrict the liberty of ordinary people. Older terrorism campaigns, such as the IRA in Britain or ETA in Spain, worked on the rule of 'minimum casualties, maximum publicity'. But on September 11th 2001, a new form of terrorism in which maximum casualties in simultaneous attacks for maximum global media coverage entered centre stage. If Pearl Harbour will be remembered in the USA as a 'day that will live in infamy', then 9/11 is likely to be remembered as a day that changed America (and possibly even the world) forever. The George Bush Junior Presidency took a month to respond, first by launching an attack on the Taliban regime in Afghanistan and the Al Qaeda fighters which it harboured. Next, it formulated its new National Security Strategy which has been called simply the 'Bush Doctrine'.

Before outlining what this means, together with its consequences for the conduct of propaganda, it is necessary to rehearse what happened in the previous decade since the 1991 Gulf War. For it was the arrival of western troops into the Holy Land of Mecca that infuriated a certain Saudi Arabian called Osama bin Laden. This once-US backed *Mujahadin* fighter against the Soviet invasion of Afghanistan now turned against his former sponsors, formed Al Qaeda ('the base') and plotted to bring down the World Trade Centre in 1993. After years of attacking US targets, including American embassies in Africa and the *USS Cole*, 19 western educated Arabs succeeded finally on 9/11, also attacking the Pentagon in the process. Shocked American headlines asked 'why do they hate us so much?' That this question should have even been asked suggests a serious failure in US Public Affairs over the previous 10 years, and the very fact that the hijackers were members of that same target audience for Public Diplomacy, namely the elite, suggests a serious failure of that form of official informational activity as well. What had happened, especially when Richard Holbrooke famously asked 'how can a man in a cave out-communicate the leading communications society?'

With the end of the Cold War and the bi-polar (or Manichean) world it created, there was a tendency to assume that America's role as the world's surviving superpower was so obvious that this power would speak for itself. Although PSYOPS was used as a tactical and operational 'weapon' in the military interventions in Somalia, Haiti, Bosnia and Kosovo, Public Diplomacy went into decline in the 1990s. This culminated in 1999 with the closure of the USIA, with its activities being folded back into the State Department. This meant that during the 1990s, the absence of American fostering of mutual understanding created a vacuum in terms of the strategic communications environment. Into this vacuum came all sorts of information, disinformation and misinformation from all sorts of new info-players who recognised that they now had access to a global communications system called the World Wide Web.

Power should not be left to speak for itself. It needs explaining if it is to be accepted. Nor should a nation-state of whatever rank allow an information vacuum to form because its enemies will fill that vacuum with propaganda that needs to be countered. If a nation is not proactive on the information front, then it can only be reactive - and if it is reactive it is always on the defensive. Al Qaeda understood this and realised the importance of *information as an asymmetric weapon* against powerful nation-states, and especially the United States, at a time when the US was trying to define what it meant by the creation of a post-Cold War 'New World Order'.

Thanks to 9/11, we are now in a different age: the so-called 'global war on terror'. The threat now is not so much between nation-states – although long-standing tensions and territorial disputes remain. Whatever Al Qaeda is, or has become, most analysts are now talking of it in terms of an *idea* as well as a network of loosely aligned terrorist organisations. The idea hates the notion of a nation-state; instead Islamic extremists want to create a caliphate – a sort of non-secular superstate. The Caliphate tradition of government within Islamic thought can be best described by looking at the Sunni thinker, Rashid Rida (1935) in his idea from *Wilayat al-Faqih*. He contended that the Caliphate is a vital condition for the organization of Islam. Islam requires both the state and the law in order to function. To do this successfully, Islamic law must be flexible without sacrificing its fundamental principle. To do this, and to generate unity and strength, well trained *ulama* should be headed by a Caliph for the whole of Islam.

Very little of this was understood in the West where the media stereotyped and classified all extremists and all Muslims as 'Muslim extremists'. Instead of asking 'why do *they* hate us so much?' the question should have been 'why do *some* hate us so much?' But the nuances of religious debate and differences within the Islamic world were lost amidst the rubble of the World Trade Centre and the subsequent declaration of a global 'war' on terrorism.

Although the global war on terror has recently in 2006 been re-branded as 'The Long War', one must question the wisdom of calling it a 'war' in the first place. Wars have historically and legally been defined as armed conflicts between two or more nation-states. But if you are to wage war against a non-state actor like a terrorist organisation, how do you end such wars? It has been accepted by most states that you do not negotiate with terrorists, but how do you negotiate a peace treaty with people you will not do business with? One can deduce therefore that, if this is a war in any normal sense, it is a war without end – the Forever War.

President George W. Bush has indeed called it 'a new kind of war', and if it is really a war of ideas, how do you wage such a conflict? You certainly need propaganda machinery, although of course it is not called that. The Bush administration has recognised its deficiencies in national self-projection overseas – and those of the previous Clinton administration - and attempted to rectify them by the construction of a new propaganda machine including the Office of Global Communications in the White House, (although this is now closed) the failed attempt by the Pentagon to create an Office of Strategic Influence (Gilmore, 2002), the reinvigoration of US Public Diplomacy programmes, the establishment of Coalition Information Centres in Washington, London and Islamabad, and the expansion of its international broadcasting services through the creation of *Radio Free Afghanistan*, *Radio Sawa* ('Together') to replace the hopeless *Voice of America Arab Service*, and the newly created *Radio Farda* for Iran. There is also *Al Hurra* ('the Free One') TV for the Middle East.

Whether all this will be enough to 'win' the propaganda war remains to be seen. In a long war, it is important to recognise the inherent difficulties of hunting down an elusive enemy such as the Al Qaeda terrorist network as well as 'winning hearts and minds' over the lifetime of at least one, and probably more, generations of potential future terrorists. This commitment, enshrined in new American laws such as the Patriot Act and Freedom Promotion Act (2002), is shared – to a greater or lesser degree – by almost half of the nation-states on the planet, although many of their governments are more implicit than explicit in their support, preferring to co-operate on the less visible 'fronts' of the war in such areas as intelligence sharing, law enforcement, financial and humanitarian matters. There are many reasons why these partners in the global war on terrorism are nervous about showing their heads above the parapet and are happy to let their publics continue to perceive the conflict as *America's* war on terrorism (with a little help from Great Britain). As a result, most people in those coalition countries – perhaps with the sole exception of the military, intelligence and diplomatic communities – do not perceive themselves to be 'at war' at all.

U.S. versus the rest of the world?

This is not the case in the United States where the media and the public have rallied around the flag. There, dissenting voices were largely mute or uttered in whispers until the 2003 war in Iraq started to turn into an ugly uprising against the western 'invaders'. At home, intrusions into civil liberties are accepted as inevitable due to recognition that Homeland Security restrictions are a necessary evil in a 'war of national survival'. It is this perception which distinguishes the American psyche from the mindset of the rest of the world – even in traditional US allies – where, following the unprecedented invocation of Article V of the NATO Charter the day after 9/11 ('an attack upon one is an attack upon all'), – world public opinion largely continues to see it as 'America's war', and one about which they continue to harbour considerable doubts. European publics, whether in Greece, Italy, Spain, Germany, France or Britain, have over time grown accustomed to the threat posed by terrorist groups, and this perhaps helps partly to explain the differences in perception on the other side of the Atlantic, where terrorist acts on US soil are a comparatively recent phenomenon (Storin, 2002). Nor, of course, has anyone else had to endure an experience on anything like on the scale of 9/11, despite the subsequent bombings in Bali, Istanbul, Madrid, London and elsewhere. Europeans tend to respond to terrorism by utilising the police, rather than the military. But one still cannot avoid the suspicion that many world leaders have failed to appreciate that, if the world has not changed after 9/11, the Americans most certainly have – and that is why the Pentagon has the lead in the 'war' on terrorists, not the FBI. The President has stated that 'we must fight them out there to prevent them coming here' – indeed a new kind of approach to counter-terrorism.

Many propaganda analysts are agreed that the most difficult propaganda to conduct effectively is that which attempts to change people's minds. The easiest is to reinforce the belief systems of the already converted. This is why the American government did not at first have much of a Public Affairs problem in persuading most Americans to accept the demands of the war on terrorism. Around 70% of Americans were prepared to accept that there was a connection between Saddam Hussein and 9/11 (USA Today, 2003) until, finally, President Bush admitted to having no evidence of this in the late summer of 2003. That was partly because the war against terrorism has been 'sold' to the American people under the umbrella of the Bush Doctrine.

This doctrine has three discernable strands. President Bush first outlined his new post-9/11 position during his State of the Union speech in January 2002, signalling a significant break with American foreign policy of the past (Bush, 2002). The first strand of this doctrine is that, because its terrorist enemies 'view the entire world as a battlefield', the United States must be proactive in 'pursuing them wherever they are'. This exercise of active American global leadership, especially with the threat of impending proliferation of chemical, biological and nuclear weapons of mass destruction, could involve the USA acting *pre-emptively*. For all the diplomatic manoeuvres involving UN Resolution 1441 and a possible subsequent resolution justifying military action against Iraq, it was this element of pre-emptive war which found its doubters amongst American allies who appeared concerned that the United States would henceforth act unilaterally not so much in the war against terrorism (where international co-operation amongst the intelligence services remained marked) but in so far as the second element of the Bush Doctrine was concerned.

This second element was 'regime change'. Traditionally, and indeed since the creation of the international state system at the Treaty of Westphalia in 1648, it was an unspoken but universally held principle of international affairs that one state did not interfere with the internal affairs of another, short of war. An interesting twist to the ongoing Iraqi crisis since Operation Desert Storm in 1991 was the puzzlement of why the American led coalition had failed 'to finish the job' when military victory in that Gulf War had been so decisive in expelling Iraqi forces from Kuwait. Yet that previous conflict was not about 'regime change' in Baghdad; it was about the liberation of Kuwait. There could be no greater indication of how the world had changed since 9/11 than this American shift away from this position.

Regime change against a clearly identified 'axis of evil' – Iraq, Iran and North Korea – was a dramatic reversal of centuries of international relations, and indeed from a principle that was enshrined in the UN Charter under Article 2.7, giving rise to further alarm that the era in which Washington would only act multilaterally was over. It certainly stood in stark contrast to the multilateralism of the previous Clinton administrations. Vice President Dick Cheney elaborated on this point in August 2002 when he stated that: 'The President has made very clear that there is no neutral ground in the war against terror. Those who harbour terrorists share guilt for the acts they commit. Under the Bush Doctrine, a regime that harbours or supports terrorists will be regarded as hostile to the United States' (Cheney, 2002). Of course, this had been the main justification for the war in Afghanistan.

The third element was the 'non-negotiable' promotion of liberal democratic values as part of the American global mission. This was essentially an overt expression of what had been implicit in American foreign policy during the Cold War, namely the selling of democracy, US-style, to areas where it did not exist. As Cheney again elaborated: 'In the Middle East, where so many have known only poverty and oppression, terror and tyranny, we look to the day when people can live in freedom and dignity and the young can grow up free of the conditions that breed despair, hatred, and violence' (*Ibid*). Regime change was not just a political issue; it was an economic, social, cultural, philosophical and psychological aspiration to extend democracy to the non-democratic world. Whereas the Public Diplomacy of the past had attempted to sell democratic principles and values through persuasion, it would appear now that Americans were considering a much harder version of this 'soft power' as a better option. The international status quo ante 9/11 was, in other words, not an option.

That the President should finally concede that there was no known connection between Iraq and 9/11 (Bush, 2003) indicates the degree to which propaganda plays a central role in the justification for the war on terrorism. Propaganda is not just about what you say, and the ways you say it, at the time you say it, but it is also about what you do *not* say. Timing is crucial if the message is to have maximum impact. By the time President Bush conceded the point, the combat phase of Operation Iraqi Freedom was over, Saddam was deposed and the second battle of Operation Enduring Freedom was won. It was time to 'move on'. Tony Blair enjoyed no such luxury as the Hutton Enquiry dominated the media headlines in the summer of 2003. But the debates over semantics, especially the notorious 'dodgy dossier' issued by the British government prior to the Iraqi war with its claim that Iraq was 45 minutes away from being capable of deploying weapons of mass destruction, became even more important in Britain where public trust in the Blair government fell to its lowest point. 'So where are they, Mr Blair?' demanded *The Independent* a week after the official combat phase was over (Independent, 2003) as the so-called 'smoking gun' of weapons of mass destruction failed to fire and as American casualties mounted in the post combat period.

Given the rising levels of anti-Americanism in the world since then, the propaganda designed to 'sell' the war on terror to the rest of the world has clearly been a disaster. If the intention was to convince the world that the Iraq war was justified, it has clearly fallen on sceptical ground. Since 9/11, an unprecedented amount of debate about Public Diplomacy took place in the public domain. This was not a subject that normally attracted American media attention, but the debate was attractive now because it helped to give some answers to the agonizing that surrounded 9/11 as to 'why they hate us so much'. As Christopher Ross explained:

> *Our task is to reach out to a large silent majority, which heretofore has not been very active in countering the extremist reading of Islam that Osama bin Laden has presented. We are reaching out, first, with an exposition and explanation of our policies, putting them into context, ensuring that our policies are understood correctly for what they are, and not for what other people say they are. That carries us a certain way, but there will always be policy differences where there are differences in interest*. (Ross, 2002)

Yet, he continued,

> *But we see, also, a much longer-term task at work here, a task of trying to create a future in which extremism and terrorism no longer have a place, and we seek to do this in several ways. We're developing a strategy for mobilizing our resources, encouraging others to mobilize their resources in support of a strategy: first, of representing what this country is about and the American values that define us; second, to encourage a process of greater democratization, greater openness, stronger civil society in the countries of the region; and, third, to help to develop educational systems that give the younger generation the tools that they would need to participate in modern life in a way that is diametrically opposed to the program of someone like Osama bin Laden.*

Here was the third strand of the Bush Doctrine in the larger and longer war for hearts and minds. But by the time Ross said this, however, it was becoming clearer and clearer that the second battle of the war on terrorism in Iraq was not far away. Whether this short-term military policy would impact upon the longer-term 'perception management' campaign (as it was beginning to be called) would depend upon how Operation Iraqi Freedom would be perceived around the world. As the *Washington Post* put it, 'almost by definition … a war waged on live television is a war in which political and public relations considerations become inextricably bound up with military tactics and strategy…. how victory is won is almost important as victory itself'.[24 March 2003].

It could equally be said that how credible the justification for war against Iraq was perceived worldwide was almost as important as the US-British decision to implement regime change against Saddam Hussein. This was less important for Bush at home than it was for Blair in Britain where public support for a war against Iraq was in the lower 40s – far below any rating for sending British troops into battle since the Suez crisis of 1956. While the German, French, Belgian and Russian governments openly opposed military intervention – at least pending further UN resolutions about giving more time to Dr. Blix and his weapons inspectors – and while their national media and public opinion reflected those official positions, the British government's support for the US caused deep divisions within British society. Robin Cook, the Foreign Secretary who had championed an 'ethical foreign policy' during the NATO intervention in Kosovo, resigned. *The Daily Mirror*, which had traditionally supported British wars when 'our boys' were involved, was proudly anti-war. And although the 'support our troops' factor kicked in when war did begin, raising levels of British popular support to the higher 50s, this was still around 20 points below the 70-80% levels of public support that previous British governments had enjoyed in earlier conflicts, including the controversial 'humanitarian intervention' in Kosovo. Even in America's staunchest ally in the war against global terror, the British media and public were deeply divided over the connection between Iraq and 9/11 and therefore whether the war to get rid of Saddam Hussein was both 'just' and justified.

Strategic Communications Today

The roots of a massive propaganda failure thus lay in the decision to go to war against Iraq. A Special Task Force reported in September 2003 that:

> *Beyond the threat of a direct attack by al Qaeda and those influenced by that movement, the United States is now facing a more fundamental loss of goodwill and trust from publics around the world. The Task Force argues that this loss has damaged America's ability to protect itself and to attain its foreign policy goals, and that in the run-up to the U.S.-led war in Iraq, botched diplomacy on all sides left a legacy of resentment, fear, and anxiety.*
> (Foreign Relations, 2003)

In other words, the situation had become worse, not better, as a result of Operation Iraqi Freedom. In the same way, the subsequent arrival of foreign *Al Qaida* fighters into Iraq to help loyalist attacks on American forces had ironically created a direct link between bin Laden and Saddam where none had existed before. But at least this development, ex post facto, added some credence to the insistence that Americans were still fighting the war on terrorists. The challenge indeed remains, as another recent public diplomacy report put it, one of 'Changing Minds and Winning Peace' (US House of Reps, 2003).

The momentous events of the past five years have placed propaganda – or strategic communications as it is now being called – at the centre of international affairs. The 21st century global information space has so many voices capable of inputting this environment – from a 'citizen journalist' with a mobile phone or digital camera (or now both are combined) that can be connected to the internet to international satellite television stations - that it is virtually impossible for one voice to prevail. Official propaganda must compete and, if it is to succeed, it can only do so on the grounds of its credibility. Image and reality must go hand in hand, but if the reality is incredible – and many find the Bush Doctrine incredible – then no amount of skilful marketing will be able to sell it to people who simply do not want to buy it. Until recently, this tended to be thinking of a Washington administration guided by Charlotte Beers, recruited from Madison Avenue to 'Brand America' to the rest of the world. Her resignation early in 2003 did not seem to signal a new phase in the global propaganda war but that is what her successor, Karen Hughes, will need if she is to stand a chance of winning the war of ideas.

Reframing the war on terror into a long war of ideas

Given that the United States has now been fighting the current war on terror longer than its involvement in World War Two, and that it is frequently claimed that the West is losing the propaganda war, the time has now come to take a hard look at what has gone wrong and how to put it right. The former is easier to do than the latter, but it is essential to diagnose the illness before a cure can be prescribed. There is little point in revisiting the obvious mistakes that have damaged western credibility, from Jessica Lynch to Abu Ghraib to Guantanamo Bay, except with people who still refuse to accept that these were indeed propaganda own-goals. Even the American President in mid 2006 accepted that some of the early rhetoric, such as his use of the word 'crusade', was unfortunate, while Secretary Rumsfeld has conceded that closing the USIA in 1999 was, in retrospect, a mistake. Why it has taken so long to realise the obvious is, perhaps, a symptom of the disease so the diagnosis should start with the first symptom: political short-termism.

It is a characteristic of our modern political age that our western democratically elected politicians tend to think temporally in terms of the next election. In the case of the American President, it is perhaps two elections. Their primary political objective is to govern. When Francis Fukuyama wrote of the 'end of history' at the end of the Cold War, he should perhaps have talked instead of an 'end of ideology'. For now strongly committed ideological convictions seem to have befallen the same fate as communism - mostly deceased with a few isolated and stubborn pockets remaining. Many of the current Bush administration are former Democrats while Tony Blair's New Labour policies would sit quite comfortably with Thatcherism. If your core political ideology is driven by the desire to govern rather than to pursue a set of political beliefs, then your policies are shaped by a populist agenda to win votes rather than to change society for the benefit of its citizens. It means a near horizon perspective, and an improvisation approach to crises, especially if there is a media storm around them. The Bush Doctrine may appear to be a long-term vision of the future but how to get there step-by-step rather than war-by-war does not seem to have figured in the thinking.

As a consequence of this short-termism, image becomes central to political behaviour. The way you are perceived is more important than what you actually do. Western politicians today are the first to have been born in the age of television but they are only just beginning to adjust to the consequences of real-time television and reality television. When, for example, the British Parliament allowed TV cameras into the House of Commons in the late 1980s, they did not allow unedited 24 hour coverage because they knew the reality of filming empty chambers would discredit the political process in the eyes of the voters. You have to have a gap between image and reality if you do not want reality – in peace or wartime – to jeopardise your survival. Ceaucescu was the only dictator who allowed live coverage of his performance in his final days – and he ended up before a firing squad. Democratically elected politicians spawned by the TV age understood better that it was more important to create *an illusion of reality*, but the subsequent proliferation of cameras in the digital age – from CCTV to mobile phones – meant that it was harder and harder to create, or at least sustain, that illusion. In other words, in the past 15 years they have lost the ability to control or edit their own image. It is inconceivable today that the media would self-censor their coverage of a President who suffered from polio and appeared publicly in a wheel-chair – yet that is what they did 50 years ago with President Franklin Roosevelt. It is inconceivable not just because the media has changed but also because it would be impossible in an age when the media no longer monopolize the images taken of the few who govern to the mass who vote. Or, rather, who increasingly do not vote, which in turn prompts ever more desperate stunts to attract popularity. It is why western politicians today prefer to appear on chat shows playing saxophones or being grilled about their childhood fantasies about Margaret Thatcher than being interrogated by serious investigative journalists on political current affairs programmes that fewer and fewer people watch.

Why our mass publics today suffer from short attention spans is perhaps more the remit of a sociological analysis. But broadcasters and politicians alike have responded to these developments with their respective phenomena of infotainment and short-term politics. Not everyone has become obsessed with Big Brother or WMD but our politicians know that they can say to the majority 'Move On' and get away with it, or at least get re-elected. Why young people pay to vote for the eviction of Big Brother housemates when they will not vote in national elections may well be linked to massive changes in society that are reflected in such phenomena as Universities where students are more interested in getting better grades than in understanding how the world really works. But politicians are products of the society that throws them up and thus the military have to live with the consequences of their decisions, especially in matters of war and peace. In the era from Vietnam down to the combat phase of the 2003 Iraq war, the assumption was that the public only had the attention span to tolerate short wars, with minimum casualties, and for clearly justified reasons against bad guys like General Galtieri, Noriega, Saddam Hussein or Slobodan Milsoveic. The military have had to adjust to this world in a way that not even Clausewitz could have anticipated.

Information Warfare and Information Operations

If war, as Carl von Clausewitz said, is the continuation of politics by other means, and if politics has become theatre, then that old phrase 'the theatre of war' assumes a new significance. In such a world, soldiers become actors and their performance on the battlefield is brought into sharper scrutiny on real-time television. In the old days, you could keep cameras away from this performance, or at worst you could manipulate or censor the images that were taken of them. But now the cameras are everywhere, the journalists are 'embedded', and the soldiers themselves not only take trophy pictures with their digital cameras but they also publish them themselves on weblogs. Welcome to the information age where censorship is near impossible, secrets are near impossible to keep, and where concepts of Information Warfare are central to old military strategies dressed up in new costumes like Effects Based Operations.

Information Warfare (IW) as a phrase first began to appear after the Gulf War of 1991. Shortly after the conclusion of this so-called 'first information war'(Campen, 1992), the crisis in former Yugoslavia erupted into a much longer conflict that was in many ways far more significant for the international state system and the emergence of new military doctrines in the post Cold War environment. Desert Storm, as a 'conventional war' between the US-led coalition and Iraq, was to prove atypical of the international crises that characterised the 1990s right down to the undeclared air 'war' between NATO and Serbia over Kosovo in 1999. In the years between, crises in Somalia, Rwanda, Haiti, and within the Balkans seemed to suggest that the New World Order would be characterised more by *intra-state* conflict than by the more familiar inter-state armed conflicts between two or more states. The perceived need of western governments to 'do something' to stop the endless lines of refugees, genocide and ethnic cleansing and the collapse of civil society in failing states eventually prompted the label of 'humanitarian intervention' to supersede traditional concepts of peacekeeping by the international community. Moreover, all this was taking place against what many were describing as a Revolution in Military Affairs (RMA) prompted by advances in technology, especially communications technology, which ranged from improved satellite intelligence gathering capability to the placing of video cameras on the noses of 'smart' weaponry which could hit its target with accuracy unprecedented in military history. However, if such technological wizardry could provide an image (in fact an illusion) of a 'clean war' fought against the Iraqis in Kuwait (Taylor, 1992) the Balkan wars were a constant reminder that 'dirty' conflicts might not be so clinically sanitised or resolved.

Information, or intelligence, has always been important to the military in times of war. Advance knowledge of such things as adversary troop strengths and dispositions, understanding of topography, weather forecasts and insight into enemy psychology of leadership and morale have been essential ingredients of successful war-fighting since the dawn of conflict. In this respect, therefore, the Gulf War of 1991 was not the *first* information war. But, as one of the most one-sided victories for the allied coalition in military history, it highlighted just how important the new computer-based technologies and weapons *systems* had become to war fighting. The liberation of Kuwait was achieved with minimum coalition casualties (less than 150 battle deaths) and, despite all the anti-coalition propaganda, with far fewer Iraqi casualties than is often asserted. Much of the credit for this was put down to the ability of the United States in particular to take 'command and control' of the Iraqi information space, from the destruction of Iraqi anti-aircraft capability on the opening nights of the war to pinpointing precision-guided weapons directly into the Iraqi leadership command infrastructure. Even though, after the war, it came to light that Patriot missiles had rarely been as accurate in their duels with Scud missiles as had been portrayed at the time (Congress, 1992), or that of all the coalition ordinance dropped on the Iraqis only 8% of it had been 'smart', Desert Storm was heralded as a triumph for modern information and communications technologies and as having provided an insight into the future way of warfare.

As part of the usual 'lessons learned' post-conflict analysis conducted by the military, success in the Gulf came to be seen in terms of logistical build-up, fixed and achievable war aims and air superiority, a classic example of Command and Control Warfare (C2W). Over the next few years this concept evolved into C4I (Command, Control, Communications, Computers and Intelligence). But these theories were still being seen as applying to traditional inter-state conflict adapted to the information age. The next publication came in 1993 with Alvin and Heidi Toffler's influential book, *War and Anti-War* (Toffler, and Toffler, 1993). The Tofflers extended earlier theories of theirs concerning societal development through three stages, or waves: first agrarian, followed by industrial and finally into post-industrial or informational waves. They now argued that the particular stage of a society's capacity to wage war reflected the way states undertook their peaceful economic development. As societies such as the United States were by the early 1990s increasingly dependent upon communications and information systems as a source of wealth creation (service and financial industries, money markets, banking etc.), it should come as no great surprise that their military systems should develop in a similar manner. In 'Third Wave' societies, information displaces oil as the lubricant of peace as well as of war. Oil remained important – as the Gulf War demonstrated – but information was moving into a more central, dynamic position in order to achieve national objectives. A country like Malaysia is experiencing all three waves simultaneously.

Writers such as Martin Libicki (1995), John Arquilla and David Ronfeldt (1997) and others began to take up these themes and triggered a flurry of research into what was now being termed information warfare. However, these writers were initially preoccupied with the vulnerabilities now facing Third Wave information societies and their increasing dependence upon communications *systems.* As early as 1991, Winn Schwartau coined the phrase 'electronic Pearl Harbour' and other writers now began to develop a new lexicon of phrases associated with the new thinking. They talked of 'cyberwar', 'infobombers' and hacker warfare. Their emphasis was largely upon computer systems or Computer Network Operations (CNO), and their language was one of protection from attack in an international environment (Computer Network Defence or CND) in which traditional concepts of warfare, of the enemy and of battlefields were obsolete. Now they talked of battle 'spaces', critical information infrastructures, electronic warfare, asymmetric warfare and virtual conflict.

At first, this thinking seemed far-fetched, the stuff of science fiction rather than sound military strategy. However, the experience of IFOR and SFOR in Bosnia between 1995 and 1999 in terms of 'shaping the information space' in support of the mission was to have considerable impact on the development of the IW concepts of the early 1990s and the emergence of Information Operations (IO) thinking in the second half of the decade. IO was to replace IW as the preferred phrase by around 1998 and PSYOPS was brought under its doctrinal umbrella. The agreed US definitions are now as follows:

Information Warfare:
Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Information Operations:
Actions taken to affect adversary information and information systems while defending one's own information and information systems.
(Joint Publication 3-13, 2006).

These definitions are so vague that they are almost meaningless. But they allowed people to interpret IW and IO in just about any way they wanted. They also meant that PSYOPS had to adapt from the traditional 'surrender or die' messages seen in the Gulf War of 1991. In subsequent operations like Provide Comfort (the humanitarian aid to the Kurds in Northern Iraq), Restore Hope (Somalia) and Restore Democracy (Haiti), PSYOPS adapted to Peace Support, Humanitarian and Peace Restoration objectives. A good example of this had been a series of leaflets, posters and broadcasts in support of mine awareness campaigns, but other PSYOPS themes included the use of targeted information to support arms amnesty and food supply campaigns. In a post-conflict situation like post-Dayton Bosnia, PSYOPS adapted to the new kinds of interventions in a manner that was a far cry from the old psychological warfare campaigns of traditional inter-state conflicts. 'In the Bosnia context, where the factions tightly controlled the local media and used them to propagate their self-serving propaganda, IFOR/SFOR needed to circumvent the local media to effectively reach the local audiences' (Siegel, 1998, p.73). For the Public Information/Affairs people, this was an alarming step. 'Although PA officers argued that "shaping the public perceptions" is a PSYOP function, their information does contribute to shaping opinion either directly (through their press conferences) or indirectly (through media reporting of their statements)' (Wentz, 1998).

Discussion of the current challenges

The emergence of IO as a military theory therefore clouded all the issues which had been clear amongst the various military communicators since the Cold War. 9/11 created even more confusion, not least because some planners seemed to have forgotten that the play is not the thing, although IO suggests that the military should indeed play to the camera in a theatre of war where, for example in Iraq after 2003, 'liberation' rather than 'occupation' is the plot, and where military tactics are used to compensate for a lack of long-term political strategy.

What about the spread of democracy to the Middle East? Is not that part of the Bush Doctrine a genuine political strategy? Here is another symptom of the disease – that a fundamental commitment to spreading democracy merely polarises the situation of a so-called war on terror. It certainly gives the West's adversaries who advocate the establishment of a fundamentalist caliphate a common point of reference. This desire to spread western democracy has provided Al Qaeda as a loose network of terrorist groups which had little in common before with a common enemy now. And when the western leader of the war on terror says things like 'you are either with us or against us' or 'there is no neutral ground in the war on terror' this rhetoric which was designed to rally domestic opinion actually serves the interests of the enemy by providing an image of western fundamentalism that can indeed be repackaged as a crusade by western infidels.

This brings us to another symptom of the disease which no spin doctor can cure, namely the tendency to see foreigners as ‘others’ who merely want to become like ‘us’. From an American historical perspective, having broken away from the British Empire and then having built the nation on the philosophy of bring me your tired, your poor and your oppressed, the belief that universal concepts like ‘life, liberty and the pursuit of happiness’ will translate readily to non-democratic societies has proved fundamentally flawed. The triumphalism displayed during the two post Saddam elections in Iraq has had to be tempered by the election of *Hamas* and the subsequent US reaction to the Palestinians has merely reinforced enemy propaganda claims about the hypocrisy and selectivity of the West. The spread of democracy, in other words, has to be on American terms; it has to be a mirror image of ‘our’ democracy. This appears to the recipients of the message as a form of neo-colonialism, another crusade in a thousand year holy war.

Where did this kind of thinking come from? After the so-called triumph of free-market liberal democratic capitalism in the Cold War, there emerged a belief that the New World Order would be sustained by the spread of democracy world-wide. This was because democracies tend not to go to war against other democracies, and thus the potential enemies of democracies were non-democracies or authoritarian regimes. Added to this was the belief after 9/11 that such regimes were also sponsors of terrorism and were thus re-branded, World War Two-style, an ‘axis of evil’. What people did not see, because they neither looked to the past record with post-WW2 Germany and Japan, nor to the far future horizon, was that if you replaced those regimes by force, it would take at least a generation to rebuild not so much the economy of the defeated nation but the psychology of its people. Contrast the pacifist German and Japanese societies of the past with those of today, and you will realise it took 50 years – or two generations – to eliminate the militarist psyche which prevailed half a century ago, supported by their public opinion. But today our short-termist western political leaders did not think that our short-attention spanned public would be able to swallow such a commitment. The lessons of Bosnia were conveniently allowed to drop away from the media agenda. Instead the public ‘moved on’.

IO, to repeat, is a military doctrine designed to assist military commanders in their varied missions in the information age. These missions have been ‘humanitarian’, peacekeeping and even nation-building. Inter-state wars have, in fact, become the exception to the norm. However, terrorism is not war and you cannot fight the ideas which fuel terrorism with kinetic weapons like tanks and bombs and planes. As all the former colonial powers have recognised, counter-terrorism campaigns are as much about ‘hearts and minds’ as they are about killing terrorists. True, the new terrorism sees the terrorists killing themselves in the process of killing as many other people as possible. However, if you wage war against them how does such a war end? Will there be Unconditional Surrender? That is the logic if the policy is not to negotiate, including a peace treaty, with terrorists. Yet Unconditional Surrender is unlikely to be achieved with fanatics who believe that their faith in God is greater than yours and that the end of the world is nigh, so why not accelerate the process? So it is not the Long War; it is Eternal ‘war’.

Unless, that is, the hearts and minds of the real target audience in this war of ideas, namely the unborn whose hearts and minds have yet to be polluted with the hatred and resentment of their parents, are targeted. In other words, this is a generational war for ideas in every way that the Cold War was - except the enemy has not yet got nuclear weapons. The significant 2006 reorganisation in Washington and Fort Bragg of the Public Diplomacy, Strategic Communications and PSYOP machinery may well be the recognition – at last – of the need for a truly integrated long-term propaganda machinery to wage a war of ideas, but one is still left aghast at the impending reduction of *Voice of America* broadcasts.

Perhaps it would be wise to see the creation, or recreation, of the United States Information Agency which would be independent from those well-established turf warriors, the Departments of State and Defence. The jostling for power between State and the Pentagon has been a major barrier to progress in the western information war, and the reasons for this are obvious. When a nation is 'at war' – as the American President reiterated again in the 2006 State of the Union address – it is natural and understandable that the nation's warriors take the front seat and the diplomats take the rear. But in a generational war of ideas, the two key elements to winning are credibility and trust. These take time to create and cultivate, to show potential adversaries what kind of people you really are, that indeed you are not their enemies. In such a struggle, diplomacy should really be in the front seat. But diplomacy is also required for allies and potential allies to form a genuine international coalition in which all nations share a common perception of the common threat. One suspects this is actually happening more in the intelligence community than amongst those NATO partners, for example, who do not share the perception of being 'at war' but who nonetheless understand the threat posed by international terrorist networks.

It is often said that to fight a network you need a network. Whereas we have come a long way in understanding how *Al Qaida* and its affiliates uses the internet, for example, there is still some way to go in increasing the effectiveness of western networks – at least in the field of persuasion. That is the problem with democracies; they find it a long, difficult process to form agreements amongst themselves, especially if their elected politicians only operate in short terms – but it is those very differences which *Al Qaida* propagandists exploit to their own advantage. Compare how slowly the West has been to use the internet with how effectively its enemy has done, culminating with hostage videos or slickly edited DVDs of snipers at work in Iraq or 'martyrdom operations' filmed by terrorist cameramen. The West is indeed losing the information war when many people in the Islamic world believe that the American President is a greater threat to world peace than Osama bin Laden.

Another major issue which has to be confronted is the Islamic Diaspora. The West needs to avoid the 'red under the bed' phenomenon of the Cold War which demonises an 'enemy within'. This both alienates those communities and radicalises certain individuals within them – as Europe's first home grown suicide bombers from Leeds demonstrated only too graphically in London on 7/7. The concept of the *Umma*, or Islamic brotherhood, transcends national boundaries but that does not mean it should be translated into a 'clash of civilisations'. Every racist attack, every piece of graffiti daubed on a mosque, is seized upon by adversaries as a further example that this is precisely what is taking place and thus reinforces the idea of a holy war that needs to be waged against the 'infidel crusaders.'

The military's job may be to go after the 'bad guys' but it is the job of diplomacy and trade to tackle the reasons why some people adopt a terrorist cause – especially those clinging to life on less than a dollar a day throughout the developing world. One way to their hearts and minds is through their stomachs and the rhetoric of 'make poverty history' must be translated into reality if the long war is to be won. That many in the Arab and Muslim world think the way they do – as reflected in unprecedented levels of Anti-American and Anti-Western sentiment – is of course not just down to the mistakes that have been made to date in the information war. Western leaders may have sometimes forgotten that image and reality must go hand in hand if it is to persuade successfully, but they have also avoided serious debate about the reality – or the policy – which it are trying to pursue. The issue is not about presentation. It is about policy. And hence it is about the Bush Doctrine. When *The New York Times* issues an apology for failing to ask the penetrating questions over America's reasons for going into Iraq, it is a sure sign of trouble. It acknowledges in the process that the democratic media have become a lapdog of government rather than a watchdog of democratic debate. If you take the policy of preventive war that was so central to the Bush Doctrine, what you are really accepting is a world as it might be rather a world as it really is. And one person's American Dream becomes another's nightmare, not a universal democratic world where nations are safe from the threat of terrorism. Indeed, this is at the root of what some analysts have called a self-fulfilling prophecy, namely that if there was not a link between Iraq and 9/11, there is now and that for every suicide bomb martyr there are dozens of new recruits to replace him or, indeed, her.

If the West goes to so many lengths to avoid the 'P' word, then it will never get this right. Is the 'P' word: Propaganda, Public Diplomacy, PSYOPS, Public Affairs, or Policy? Partly, it is. Try another 'P' word, namely Palestine. Until the West resolves that issue, no amount of presentation – however skilfully done – can gloss over that festering sore in the minds of the Islamic brotherhood. The West's talk about Strategic Communications and Information Operations will be of no consequence if the policies cause resentment that fuels fanaticism. The West will never be able to sell democracy as a viable, peace-loving political concept. Much has already done much to damage its credibility which may well prove to be like virginity, namely that you can never get it back. But as the baseball-playing Japanese have demonstrated, it is possible to change a national psyche provided there a long-term commitment to the long-term goal and recognise that, to get there, you do not sell a concept, you get people to buy into it. But you can only get them to do that if they recognise that it is in their interests, not yours, to follow that route.

This is what made the young people of Eastern Europe tear down the Berlin Wall. They wanted what the West had because those that had not been brainwashed by decades of communist propaganda hated what was being forced upon them and they desired the opportunities that were being denied to them. They first needed to discover this, which was why satellite television, fax machines, pop music, Radio Free Europe and so on all played their part in the Soviet Union's collapse. To the victors go the spoils, including history written by the victors, and the West has already rewritten the history of the late 1980s and early 1990s as a 'victory' of the West over communism, rather than an internal collapse from within. That interpretation has generated arrogance that this new 'war of ideas' can be won the same way. The West needs to re-think whether it can, whether this war is being fought against the right people, with the right weapons, with the right strategy – or indeed whether there is actually a strategy for 'winning' a long war that perhaps can never be 'won' in terms that has been traditionally understood.

For the challenge is not simply a military one, nor is the solution a military doctrine like Information Operations. In some respects, thinking this way merely makes the problem worse. If IO is at all valuable it is on the battlefield, and it works best at tactical and operational levels. The real problem is at the strategic level where IO should be thought of as a pre-emptive tool. Pre-emptive IO, conducted with a far horizon end-state clearly in mind, and clearly achievable in military, political, economic *and* psychological terms, may not prevent fanatics from conducting future terrorist attacks against vulnerable targets. It never could. But it may well isolate those fanatics from potential supporters who believe, for example, that the American President is the 'Devil in the White House'. In short, what is needed is more propaganda for peace. Only then will persuasion prevail over force.

References

Arquilla, J., Ronfeldt, D. (eds.) (1997) *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, Santa Monica.

Bush, G. (2002) Presidential State of the Union Speech, 29 January 2002. URL: http://merln.ndu.edu/pfiraq/20020129-11.pdf [Accessed August 20, 2006].

Bush, G. (2003) Bush denies Saddam-9/11 link, *ITV.com*, 18 September 2003, URL: http://www.itv.com/news/119359.html [Accessed August 20, 2006].

Campen, A.D (ed.), (1992) *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*, AFCEA International Press, Washington.

Cheney, R. (2002) Vice President Cheney's speech to the Veterans of Foreign Wars, 26 August, 2002. Video available online. URL: http://news.bbc.co.uk/2/hi/middle_east/2218223.stm [Accessed August 20, 2006]

Congress (1992) Performance of the Patriot Missile in the Gulf War, *Report 102-1086 to 102nd Congress*, April 2nd 1992. URL: http://www.radix.net/~jcturner/patriot.html [Accessed August 20, 2006].

Ellul, J. (1965) *Propaganda: The Formation of Men's Attitudes*, Random House. New York.

Foreign Relations (2003) Finding America's Voice: A strategy for reinvigorating American Public Diplomacy, *Report of an Independent Task Force*, Council for Foreign Relations, September 2003.

Freedom Promotion Act (002) The Freedom Promotion Act of 2002, URL: http://wwwa.house.gov/international_relations/107/fpa0617.htm [Accessed August 20, 2006]

Gilmore, G.J. (2002) Strategic Influence Office 'Closed Down,' Says Rumsfeld, URL: http://www.defenselink.mil/news/Feb2002/n02262002_200202263.html [Accessed August, 20, 2006]

Independent(2003) *The Independent on Sunday*, 20 April 2003.

Lasswell, H. (1927) *Propaganda Technique in the World War*, Knopf, New York.

Libicki, M. (1995) *What is Information Warfare?* Centre for Advanced Concepts and Technology, National Defence University, Washington

Joint Publication 3-53 (2003) *Doctrine for Joint Psychological Warfare*, Joint Chiefs of Staff, Washington.

Joint Publication 3-13 (2006) *Information Operations*, Joint Chiefs of Staff, Washington.

Read, J.M. (1942) Atrocity Propaganda, 1914-1919, *Journal of Modern History*, 14(4): 542-543 [December, 1942].

Ross, C. (2002) Interview with C. Ross, *PBS Online Newshour*, 16 January 2002. URL: http://www.pbs.org/newshour/media/public_diplomacy/ross.html [Accessed August 20, 2006].

N. Reeves (1986) *Official British Film Propaganda in the First World War*, Croom Helm, London.

Sanders, M.L., Taylor, P.M. (1982) *British Propaganda in the First World War*, Macmillan, Basingstoke.

Siegel, P.C. (1998) *Target Bosnia: Integrating Information Activities in Peace Operations*, CCRP, Washington,

Storin, M.V. (2002) While America Slept: Coverage of Terrorism, 1993-2001, *Joan Shorenstein Centre on the Press, Politics and Public Policy*, Working Paper No. 2002-7, Spring, 2002.

Taylor, P.M. (1992) *War and the Media: Propaganda and Persuasion in the Gulf War* Manchester University Press, Manchester.

Toffler, A., Toffler, H. (1993) *War and Anti-War: Survival at Dawn of the 21st Century*, Warner Books, London.

Taylor, P.M (1999) *British Propaganda in the Twentieth Century: Selling Democracy*, Edinburgh University Press, Edinburgh.

USA Today (2003) Poll: 70% believe Saddam, 9/11 link, *USA Today*, 9 June 2003. URL: http://www.usatoday.com/news/washington/2003-09-06-poll-iraq_x.htm
[Accessed August 20, 2006].

US House of Reps (2003) Changing Minds Winning Peace, October 2003. URL: http://www.state.gov/documents/organization/24882.pdf [Accessed August 20, 2006].

Wentz, L.K. (1998) *Peace Operations and the Implications for Information Operations: the IFOR experience*, CCRP, Washington.

Zubaida, S (2001) *Islam the People and the States*, I. B. Tauries Publisher, London.

Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques

Jim Yuill[1], Dorothy Denning[2], and Fred Feer[3]

[1]*Computer Science Department*
North Carolina State University, USA,
E-mail: jimyuill@pobox.com

[2]*Department of Defense Analysis*
Naval Postgraduate School, USA,
E-mail: dedennin@nps.edu

[3]*U.S. Army, CIA, RAND, ret.*
E-mail: ffeer@comcast.net

Abstract:

Deception offers one means of hiding things from an adversary. This paper introduces a model for understanding, comparing, and developing methods of deceptive hiding. The model characterizes deceptive hiding in terms of how it defeats the underlying processes that an adversary uses to discover the hidden thing. An adversary's process of discovery can take three forms: direct observation (sensing and recognizing), investigation (evidence collection and hypothesis formation), and learning from other people or agents. Deceptive hiding works by defeating one or more elements of these processes. The model is applied to computer security, and it is also applicable to other domains.

Keywords: *computer security, hiding, denial, deception, operations security*

Introduction

Hiding things from hackers is common practice in computer security. Routinely, systems and files are hidden behind firewalls and access-controls, and data are hidden with encryption. These common forms of hiding typically work by denying information to hackers. Another way to hide things is by using deception. Currently, deception is an emerging and promising means for computer security, as seen with honeypots (Spitzner, 2003). This paper examines the use of deception as a means of hiding things from hackers.

Deceptive hiding can be used in a wide variety of computer security applications. One such application involves hiding information about a network's topology, vulnerabilities, and assets from hacker reconnaissance (for example, scanning). The honeypot *honeyd* for example, intercepts connections to unused network addresses and impersonates computers at those addresses (Spitzner, 2003). Its ruse makes it difficult for hackers to find real computers and to scan the network without being detected.

Deception can be used to hide computer-security devices, including firewalls, intrusion detection systems, keystroke loggers and honeypots. For example, a firewall can send fake ICMP 'host unreachable' messages in response to disallowed packets, making it appear that the firewall, and victim computers behind it, are not on the network.

ISSN 1445-3312 print/ISSN 1445-3347 online

Computer security deception is defined as the actions taken to deliberately mislead hackers and to thereby cause them to take (or not take) specific actions that aid computer security (JDD, 1996). Often, for deceptive hiding, the objective is to cause the hacker to not take a particular action, such as accessing a server.

Furthermore, computer security deception aims to mislead a hacker into a predictable course of action or inaction that can be exploited or otherwise used to advantage (Dewar, 1989). In general, actions that cause the hacker to act dangerously or unpredictably should be avoided. For example, suppose a system administrator hides network logs to prevent hackers from erasing their tracks. If the expected logs are not found, a hacker may erase the entire hard drive, just to be safe. An important aspect of deception planning, therefore, is anticipating such unintended consequences and taking actions to mitigate their effect.

In the context of computer security, things are hidden from an agent, human or computer. The agent whom the thing is hidden from will be referred to as the *target*. The target is a hacker or a hacker's automated agent (for example, a worm). For deception operations, in general, the adversary who is being deceived is referred to as the *deception target*. For deceptive hiding, the target of hiding is also the deception target.

This paper explains how deceptive hiding works in terms of how it misleads, or tricks, a particular target (hacker). However, the deception planner's ultimate purpose is not misleading the target, but improving computer security in some specific way. Deception's trickery can be both alluring and intriguing, making it is easy to lose sight of the deception's ultimate purpose.

The paper describes deceptive hiding through a process model. The model's purpose is to provide a framework for understanding, comparing, and developing methods of deceptive hiding. Although the model is based on general principles and techniques that are domain-independent, the paper focuses on the model's application to computer security. The goal is to help the security professional evaluate, compare, configure, and use existing deceptive hiding techniques (for example, honeyd); and to help explore possibilities when creating new techniques.

The model characterizes methods of deceptive hiding in terms of how they defeat the underlying processes that a target uses to discover the hidden thing. This process is decomposed into three means of discovery: direct observation (sensing and recognizing), investigation (evidence collection and hypothesis formation), and learning from other people or agents. Although the focus is on deceptive hiding, many of the concepts are also relevant to non-deceptive hiding.

The next section introduces the process of deceptive hiding. Subsequent sections describe the three means of discovery and how they are defeated; a final section concludes.

The Process of Deceptive Hiding

Deception has two aspects, hiding and showing. This section first reviews these aspects of deception, and also, the earlier work on deception. It then discusses how deceptive hiding works and the processes involved.

An overview of deception

Deception is a form of perception in which a target is intentionally led to an incorrect perception, through the actions of another (Whaley, 1982) Deception is distinguished from unintentional acts of misrepresentation and from self-induced acts of misrepresentation (self-deception).

Bell and Whaley categorize deceptions as hiding and showing (Bell and Whaley 1982, and Whaley 1982). *Deceptive hiding* conceals or obscures a thing's existence or its attributes in a way that intentionally misleads the target. It is distinguished from *denial*, which may also involve hiding, but without the intent to mislead. Denial simply withholds information from the target. Encryption, which overtly conceals a message but not its existence, is an example. Steganography, on the other hand, which aims to hide the existence of a communication, is deceptive, as it uses a misleading data carrier (for example, text is hidden in the low-order bits of an image file in such manner that the text is not visible to the naked eye).

Deceptive showing makes something that does not exist appear as if it does by portraying one or more of its attributes. For example, after several unsuccessful logins, a computer can continue to prompt for passwords, but ignore them and not permit login. The computer is deceptively showing login prompts.

Hiding and showing are both present in any act of deception (Bell and Whaley, 1982). When showing the false, the truth must also be hidden. When something is hidden, something else is shown instead, even if only implicitly. Further, deceptions are often constructed of multiple ruses, employing both hiding and showing. For example, a honeypot can deceptively impersonate (that is, show) a network server, while deceptively hiding a keystroke logger. When a deception uses both hiding and showing, the deception may be characterized as hiding or showing, according to the planner's primary intent. For instance, a server's banner is modified to display a false model and version number. The banner is showing falsehood, but the primary intent is hiding the server's true model and version from hackers and worms.

Bell and Whaley offer a taxonomy of deceptive techniques based on three ways of hiding: masking, repackaging, and dazzling; and three ways of showing: mimicking, inventing, and decoying (Bell and Whaley, 1982). The taxonomy has been used in both the military and computer security literature (USMC 1989, Julian 2002). The military deception literature also lists common types of battlefield deceptions, examples being camouflage, feints (fake attack-initiation), ruses (tricks designed to deceive), demonstrations (fake force deployment), and displays (the showing of fake military forces or equipment, for example, inflatable tanks) (U.S. Army 1998, Dewar 1989, Fowler and Nesbit 1995). Cohen (1998) and Rowe and Rothstein (2004) have shown how these can be applied to computer network defense. Rowe and Rothstein also give a taxonomy of deception techniques based on semantic cases in computational linguistics such as agent, instrument, location-from, time-at, and purpose. In addition, Rowe has developed a taxonomy for deception in virtual communities (Rowe, 2005). The taxonomy applies primarily to computer misuse, and not to computer security.

The model presented in this paper extends this earlier work by showing how deceptive hiding can be understood in terms of processes, mainly the discovery processes used by a target to acquire information. Particular hiding techniques work by defeating elements of these processes.

An overview of deceptive hiding

Hiding keeps the target from knowing about the hidden thing's existence or its attributes. As a result, the target will be unaware of the thing, certain it does not exist, uncertain of its existence, or left with incomplete or inaccurate information about it. Hiding can prevent discovery of the hidden thing, or it can make discovery more difficult or time consuming.

There are three different ways a target can discover a particular thing:

1) direct observation of the thing,
2) investigation based on evidence of the thing, and
3) learning about the thing from other people or agents.

These three means of discovery comprise the target's *discovery process*. Hiding works by defeating this process, which is driven by two elements: capabilities and a course of action. The target's *discovery capabilities* are defined as the resources, skills, and abilities that the target has for discovery. The *discovery course-of-action* is the way the target carries out the discovery process; it includes how, when and where the target looks for things. This suggests that the target's discovery process can be defeated by affecting either the target's capabilities or the target's course of action. For instance, installing a firewall can ensure a hacker's port scan is not capable of directly observing a computer's servers. Alternatively, deploying an enticing honeypot could divert the hacker's course-of-action so that the port-scans reveal the honeypot rather than the hidden servers.

It is assumed that the target intends to discover the hidden thing. Another way to hide is to affect the target's intentions. For example, to deter network scanning, a company could fire any employee found scanning its intranet. Hiding by altering intentions is not addressed by this paper.

The three discovery processes are now examined in terms of how they work and how they can be defeated through deceptive hiding.

Direct Observation

When hacking a network, much of what the hacker knows about the network is learned by direct observation. For example, a port scan allows the hacker to observe a network's computers and servers. After gaining access to a computer, the hacker can use system utilities to observe the computer's resources, such as files, programs, and running processes; application programs to observe business and user data; and network clients to observe servers and their contents.

After the discovery process is described, hiding is examined to show how it defeats that process.

The discovery process for direct observation

The discovery process for direct observation involves *sensing* and *recognizing*. The process is illustrated in Figure 1 and explained here. The deception target's human sensors (for example, eyes) are used to observe. The target may also rely upon one or more external sensors, such as a network port scanner or packet sniffer. Information flows to and from the sensors over media (for example, network cables, routers, and computer monitors). The hidden thing is observed within the environment in which it resides (for example, a private computer network). After the target receives the sensory input, recognition occurs within the target's brain. Recognition is a cognitive process involving the target's knowledge and understanding. Discovery occurs when the hidden thing is identified (that is, recognized) based on expected patterns.

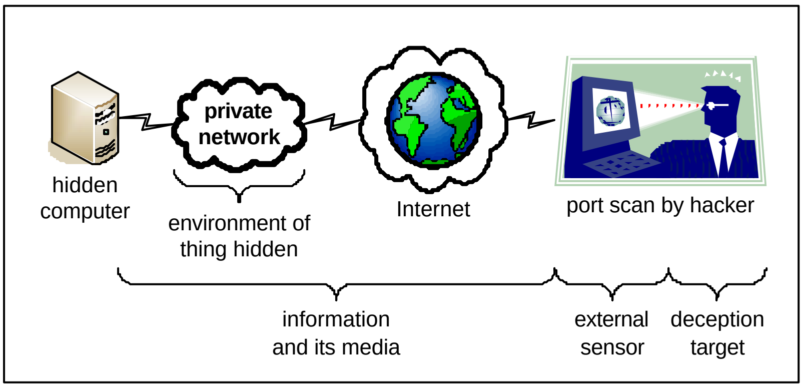

Figure 1 : The process of direct observation, illustrated by a computer-security example

A sensor receives information and then provides images to the target. These images can be conveyed to the target in a variety of ways. For instance, when a target's eyes are used to observe a computer, the image is conveyed visually. When the target observes the computer by using a port scanner as a sensor, the image is conveyed descriptively via text. Typically, sensors work in a deterministic manner, and their operation is based on mechanisms such as software and electronics (for example, the port scanner), or physiology (for example, eyes). Recognition, on the other hand, is much less deterministic than the sensors. The target might miss identifying something even if it is seen, especially if the target does not know what patterns to look for. Recognition depends on knowledge and intelligence, real or artificial.

The target's sensor and recognition capabilities are considered to be distinct elements in the model. In practice, however, both capabilities may be present in a single device. A network intrusion-detection system (NIDS), for example, can have a sensory component consisting of a packet sniffer and a recognition component based on matching packet information against attack signatures or statistical anomalies.

The target can discover things by actively searching for them or through passive observation. Discovery involves bringing the sensors to bear upon the hidden thing. The hidden thing is then distinguished and recognized from within the environment in which it resides.

How hiding defeats direct observation

Hiding defeats direct observation by defeating the targets sensor(s) and/or recognition. The *sensor* is defeated if it does not provide the target with a distinguishable image of the hidden thing. For example, when steganography is used to hide text within a picture, the target's sensors (graphics browser and eyes) cannot distinguish the text data.

Recall that the target's discovery process can be defeated through the target's 1) discovery capabilities or 2) course of action. For direct observation, this means preventing the target's sensor capabilities, or the way the sensor is used, from providing a distinguishable image of the hidden thing. One way to achieve this is by altering an element of the discovery process that is external to the target and the target's sensors. Such elements include the hidden thing's location, appearance or environment, or the information flows to the sensor. For example, placing a firewall between a server and the Internet would alter the information flows between the server (hidden thing) and the hacker's port scanner (sensor), thereby defeating the scanner's capabilities. Alternatively, the hacker's use of the scanner could be defeated by altering the server's location; for example, the server could be placed on a subnet that the hacker is not likely to scan.

Hiding can also be achieved by taking direct action against the target's sensor capabilities or the target's use of the sensor. For example, launching a denial of service attack against the hacker's computer during a port scan could impair use of the port scanner.

Table 1 : Hiding techniques that defeat the target's sensors

Action Type	***Ways to Defeat Sensor*** (sensor does not provide a distinguishable image of the hidden thing)
alter location of hidden thing	place the hidden thing where the target is not likely to observe: • place critical files in obscure directories place the hidden thing where the target's sensors cannot observe: • hide laptop behind NAT (network address translation) device • hide information within a cover medium, using steganography
alter appearance of hidden thing	make the hidden thing not reflect information to sensor: • computer eludes ping scans by not replying to pings make the hidden thing blend in with background: • password file given non-descriptive name, to elude hackers' automated searches for files named 'pass*' alter the hidden thing's appearance, so the target's sensor is not capable of observing it • encrypt message (the target can observe the cipher text, but not the plain text)
alter environment of hidden thing	create noise in environment: • add bogus files to make it harder to find critical ones alter components in environment to prevent access to the hidden thing: • hide network data from sniffers by replacing Ethernet hubs with switches
alter information flows to sensor	alter information needed by sensor: • router drops incoming pings to hide its network's computers from ping scans • delay responses to login attempts so hacker does not have time to guess password add components to communication path • firewall added to prevent certain flows to or from computers on network
diminish target's sensor capabilities	disable or degrade the sensor: • perform a DoS attack against a hacker's port-scanner reduce the target's time available for observation • quickly detect and stop target's reconnaissance, such as port scans
misdirect target's use of sensor	cause the target to observe at the wrong place or time • create a diversion for the hacker

Table 1 summarizes and illustrates the options for defeating sensors. The first column lists the general types of actions outlined above, while the second gives greater specificity and examples. (Subsequent tables in the paper will follow this format.) The table provides the deception planner with a framework for evaluating and developing hiding techniques. The action-types listed in the first column are intended to be exhaustive and mutually exclusive. The body of the table presents a broad, though not exhaustive, collection of common hiding techniques for deception and denial. Some hiding techniques affect multiple elements of the discovery process, so they could be placed in multiple tables or categories within a table.

The target's *recognition process* attempts to identify the hidden thing from among the images provided by sensors. Assuming the sensors provide a distinguishable image of the hidden thing, recognition is defeated if the target is not able to identify the hidden thing from the sensory input. For instance, to hide a virtual private network (VPN) server on a demilitarized zone (DMZ), three honeypot VPN servers could be added to the DMZ. A hacker's port scan reveals all four VPN servers, but the hacker is unable to recognize which is real.

Table 2 : Hiding techniques that defeat the target's recognition

Action Type	***Ways to Defeat Recognition*** (the hidden thing cannot be identified in the sensor's images)
alter location of hidden thing	locate where the target observes, but does not expect the hidden thing: • put sensitive document files in a software application's directory
alter appearance of hidden thing	disguise the hidden thing by making it mimic something expected in environment: • use ports that make a server appear like a workstation to scanners make the hidden thing appear as something the target does not recognize: • use unconventional names for sensitive files
alter environment of hidden thing	make things in the environment resemble the hidden thing: • place a highly valuable workstation on a LAN with many workstations that have low value, but that appear the same to hackers' scans
alter information flows to sensor	generate false information that is received by the sensor, but misleads recognition • *honeyd* thwarts scanning by impersonating computers at unused IP addresses • *nmap*'s decoy port-scan hides the scan's source address by sending many packets with fake source addresses
diminish target's recognition capability	disable or degrade the recognition process: • exhaust the hacker by providing an overwhelming amount of false information reduce target's time available for recognition • stop the hacker before the hacker recognizes critical systems and information prevent target from acquiring the understanding needed to recognize the hidden thing • limit publication of information that could aid hacker
misdirect target's recognition process	cause target to expect something other than the hidden thing • misinform hacker about identity of network elements

The target's recognition process can be defeated through the target's 1) recognition capabilities or 2) course of action. The recognition capabilities are a function of 1) the target's cognitive abilities, skill and experience in identifying the hidden thing from the sensor's image, and 2) the target's available resources, including time. The target's course of action includes how, when and where the target recognizes things, which are all influenced by the target's expectations. For example, a hacker would expect, and more readily recognize, banking-industry security devices on a bank's network than on a typical home network.

Table 2 illustrates how a target's recognition process can be defeated in order to hide. The table's first column is the same as in Table 1. The reason is that recognition is defeated by the same types of actions that are used to defeat sensors. Table 2's second column lists specific hiding techniques applicable to defeating recognition.

Investigation

Investigation is a means of discovery that infers a thing's existence from evidence rather than direct observation. Investigation is used in many domains, for example law enforcement (determining guilt based on evidence) and health care (diagnosing illness from symptoms).

In general, investigation is used to discover a thing that existed in the past when the thing was either not directly observed or a reliable recording of the observation is not available (for example, a computer log, video tape, or witness' testimony). Investigation is also used to discover things that exist in the present, but which cannot be directly observed. Things in the future can be anticipated based on indicators, but cannot be investigated because evidence of them does not exist.

Hackers often use investigation to obtain information about the current state of a victim network's topology, as well as its defences, vulnerabilities, and assets. For example:

- By acquiring a network's computer names, a hacker might be able to deduce which computers are vulnerable (McClure et al., 1999). Computers with names containing 'test' such as 'test-network-gateway,' may be indicative of systems that have not been configured securely.
- A variety of techniques are available for obtaining evidence that reveals firewalls and their access control lists (ACLs) (McClure et al., 1999). Firewalking can reveal which ports are open or blocked by a firewall (Goldsmith and Schiffman, 1998). (Firewalking sends a TCP packet with an IP TTL field set to one hop beyond the firewall. If the reply is the ICMP error message "time to live exceeded in transit", then it is evidence that the TCP port is open.)
- Email sent to a public newsgroup can reveal the internal IP address of a sending computer that is otherwise hidden by a NAT device.

Investigation is an inherent first phase of most network attacks. Deceptive hiding can be used to defeat these and other hacker investigations. When using deceptive hiding for computer security, the hacker is the investigator and deception target. When hiding things from investigation, the investigator is an adversary. Viewing an investigator as an adversary is somewhat unusual, as investigators are normally the 'good guys', for example, policemen and scientists. Of course, when the hacker is hiding things, the cyber cops become the investigators.

The following two sub-sections describe the process of investigation and how that process can be defeated, respectively. The treatment of the investigation process is adapted from David Schum's excellent research on investigation for jurisprudence (Schum, 1999).

The investigation process

Investigation is an iterative process of creating *hypotheses* and acquiring *evidence* about the thing being investigated. Typically, the investigator works with incomplete evidence, so there can be many plausible hypotheses that are consistent with the evidence. At any point during the process, the investigator can either develop new hypotheses based upon the available evidence or search for new evidence to answer questions relating to the investigator's current evidence and hypotheses. As the investigation unfolds, each piece of new evidence reduces the number of possible hypotheses and inspires the creation of more accurate and detailed hypotheses. New evidence suggests new questions and hypotheses, and these in turn drive the collection of further evidence. The information and understanding obtained is cumulative.

There are two types of hypotheses that the investigator develops and works with: discovery hypotheses and collections hypotheses. *Discovery hypotheses* explain that which is being investigated in terms of available evidence, and they culminate in the recognition or discovery of the hidden thing. *Collections hypotheses* explain where additional evidence might be found, and they guide the investigator's search for new evidence. New evidence can be acquired through direct observation (as described earlier) or from other people or agents (as described later). The collected evidence may include false and irrelevant information that misleads the investigator.

Investigations vary in the amount of evidence collected and hypotheses formed. Some are simple and produce immediate results. For example, after breaking into a computer and detecting evidence of a hidden keystroke logger, a hacker could immediately conclude that the computer is a honeypot. Other investigations are more complex, requiring the investigator to combine multiple pieces of evidence acquired over time. Instead of discovering a keystroke logger, the hacker might observe that it is not possible to create outgoing connections and that the computer contains no user data. By observing these conditions over time and considering them together, the hacker deduces the machine is a honeypot.

The process of investigation requires creativity. It also requires deliberate choices. Investigation comes at a cost, so the investigator cannot follow every hypothesis and seek evidence to answer every possible question. The investigator will be limited by available resources (including time), to collect, process, and retain evidence. How the investigation proceeds will depend upon the investigator's resources and decisions about how they are used. If the choices are bad, the investigator will make false hypotheses, collect the wrong evidence, and waste resources on useless paths of investigation.

Evidence often has a temporary existence, which can pose significant problems during the initial investigation. As time progresses, an increasing amount of evidence will no longer be obtainable. For example, log files are eventually erased or destroyed, and peoples' memory fades. The investigator needs to gather and preserve evidence before the opportunity is lost. However, much useful evidence may not be discernable at the beginning of the investigation. The discernment of evidence requires understanding of the case, and the investigator acquires understanding over time. The investigator can reduce the loss of temporarily-available evidence. By making many hypotheses, and very general hypotheses, the investigator can collect a large amount of evidence that is potentially useful. However, the investigator has limited resources for collecting and storing evidence.

Investigation is a necessary first phase of most network attacks. Further, the investigation process is weakest at the beginning of an investigation, as just described. Thus, a hacker's initial network investigation can be a *critical vulnerability*, and relatively easy for defenders to exploit. (In military theory, a critical vulnerability is a specific type of vulnerability. A combatant's vulnerability is a critical vulnerability if it can be exploited to destroy a capability without which the combatant cannot function effectively (USMC, 1997)).

How hiding defeats investigation

The inherent difficulties of investigation can be exploited through deception. If evidence is hidden, the investigator may form false hypotheses, ask erroneous questions, and pursue futile investigation tracks. The investigator may terminate what would have been a fruitful track. In situations where several pieces of evidence are needed to discover a thing, it may suffice to hide some of the evidence in order to prevent discovery. In situations where evidence has a limited lifetime, it may be enough to interfere with the start of the investigation or delay its progress.

The investigation process is defeated if 1) the target does not recognize the hidden thing, or 2) if the target's recognition is made sufficiently uncertain. This can be accomplished by defeating either of the sub-processes that comprise the investigative process: evidence collection and the creation of discovery hypotheses.

The *evidence collection process* includes 1) the target's creation of collections hypotheses and 2) the target's acquisition of information. This process is defeated by preventing the target from obtaining the evidence needed for recognition. Two types of actions can be taken to defeat the target's evidence collection: 1) alter the evidence available in the environment; that is, do not create evidence, hide evidence, or destroy evidence, and 2) weaken the target's evidence-collection process by diminishing the target's capabilities or by misdirecting the target's actions. See Table 3.

The target's evidence collection can be defeated more effectively if the target's search for evidence can be anticipated. There are two common searches for evidence that are especially vulnerable. The first are superficial searches, which result when many things must be examined, and time limitations prohibit a thorough examination. For example, a hacker's network scan may involve examining thousands of computers. To speed up the process, hackers often first perform a superficial ping scan to locate running computers. They then perform a port scan on the running computers. Such superficial examinations can be very vulnerable to deception. Second are predictable searches for evidence performed by computer programs. These searches lack human intelligence. For instance, hackers use open-source vulnerability scanners, and these scanners look for specific types of evidence. Hiding evidence from popular hacker tools can defeat a large portion of the hacker investigations on a network.

The other way to hide from investigation is by defeating the target's creation of discovery hypotheses. However, it is only necessary when the target is able to obtain the evidence needed for recognition. Hiding is accomplished by preventing the target from creating the discovery hypotheses needed for recognition. There are two ways to defeat the creation of discovery hypotheses: 1) ensure the target is not capable of creating the necessary discovery hypotheses, and 2) ensure the target's process of creating discovery hypotheses does not lead the target to recognize the hidden thing. Table 4 elaborates this.

Learning from Other People or Agents

The third way a target can discover something is to learn about it from another entity. This section describes the learning process and how it can be defeated.

Table 3 : Hiding techniques that defeat the target's evidence collection

Action Type	***Ways to Defeat Evidence Collection*** (the necessary evidence is not collected)
block evidence creation	find a way to do things so evidence is not created: • configure outgoing mail server to remove sender's IP address from mail headers
hide evidence	hide evidence that could be acquired by direct observation or learned from other people or agents
destroy evidence	destroy evidence before the target can collect it, either at once or by entropy over time • remove sensitive information from memory and disk after use
diminish target's evidence-collection capabilities	reduce the target's time available for collection • quickly detect and abort hackers before they find critical information • delay the target's evidence collection, so that it exceeds the target's available time
misdirect target's evidence-collection	misdirect the target's collection activities, to keep the target away from necessary evidence; for example, create false evidence that causes the target to look for evidence in the wrong places confuse the target, so the target cannot form the collection or discovery hypotheses needed to obtain necessary evidence; for example, create false evidence that contradicts real evidence reduce the target's perceived reliability of necessary evidence; for example, create false evidence that is of the same type as the real necessary evidence, and allow the target to learn that false evidence has been created

Table 4 : Hiding techniques that defeat the target's creation of discovery hypotheses

Action Type	***Ways to Defeat the Creation of Discovery Hypotheses*** (even if the target has the necessary evidence, the target cannot create the necessary discovery hypotheses)
diminish target's capabilities for creating discovery hypotheses	cause target's capabilities to be insufficient; for example, reduce target's available time
misdirect target's creation of discovery hypotheses	mislead target; for example, create false evidence, or hide true evidence, and thereby cause the target to form incorrect discovery hypotheses confuse the target, so the target cannot form the necessary discovery hypotheses; for example, create false evidence that contradicts real evidence

The learning process

The learning process is a discovery process wherein the target learns of the hidden thing from a *discovery agent*. The discovery agent can be a person or a device with sensor and recognition capabilities, such as a software agent. The agent discovers the hidden thing through its own discovery process, which can be direct observation, investigation, or learning. The agent then reports the discovery, and the report is communicated to the target. The report can be sent directly to the target (for example, via an email), or recorded and placed somewhere accessible to the target (for example, a website). The discovery agent may act autonomously or under the direction of the deception planner or the target. Figure 2 illustrates.

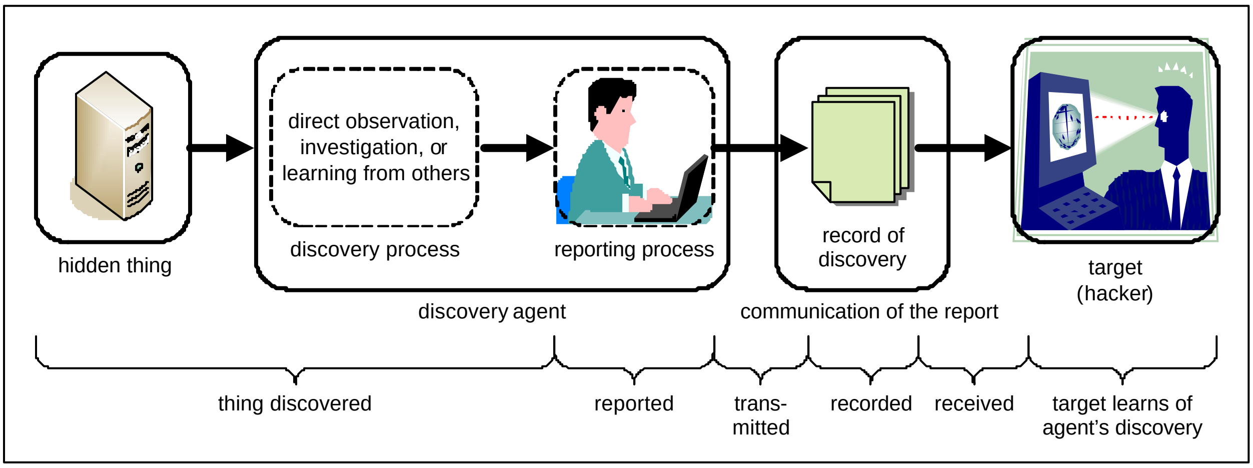

Figure 2 : How the target learns from other‘s, or agents’, discoveries

In practice, the target may learn of a thing through a series of agents. For example, the target learns of the thing from person A, who learned of it from person B, and so on, the first person having acquired it from direct observation or investigation.

Hackers acquire much of their knowledge from others. For instance, through footprinting they learn about a victim's network from publicly available information (McClure et al., 1999). Typical sources include DNS servers, which record the IP addresses and domain names of computers on a network, and company websites, which may contain information about the company's networks. Hackers also learn through distribution lists, chat channels, and other online forums.

How hiding defeats learning

Hiding defeats the learning process by defeating the discovery agent, communication of the report, or the target's recognition. The *discovery agent* is defeated if it does not discover the hidden thing or does not attempt to report it. The *communication of the report* is defeated if the report is not successfully transmitted, recorded, or received by the target (assuming the discovery agent has attempted to communicate the report). The *target's recognition* is defeated if the target does not learn of the hidden thing from the report (assuming the target has received the report). Table 5 elaborates this.

Conclusions

This paper explains deceptive hiding in terms of defeating the target's discovery process. The model includes three means of discovery: direct observation (sensing and recognizing), investigation (evidence collection and hypothesis formation), and learning from other people or agents (discovery by an agent, report communication, and target recognition); for each hiding defeats one or more of the components of the discovery process. This is accomplished by ensuring that: 1) the target is not capable of discovering the hidden thing, or that 2) the target's course-of-action does not lead the target to discover the hidden thing.

The process model offers a conceptual framework for developing new deceptive hiding techniques and for evaluating existing techniques. The model also offers a common frame of reference for collaboration among security professionals. When hiding a particular thing, the deception planner can determine which discovery methods the target is likely to use. For each method, the tables of hiding techniques can be used to consider the possible ways to hide.

Table 5 : Techniques for hiding when the target learns from other's, or agents', discoveries

Action Type	***Ways to Defeat the Discovery Agent*** (the hidden thing is not discovered and reported)
hide thing from discovery agent	hide thing from the agent's direct observation • give unused addresses on a network fake names to hide real computer-names in reverse DNS lookups. hide thing from the agent's investigation
alter discovery agent's reporting process	instruct discovery agents under control of deception planner to omit hidden thing from reports • omit high-valued assets from published network diagrams • omit sensitive network information on public technical-support forums
diminish discovery agent's capabilities for serving target	cause discovery agent to not serve target: • bribe or 'turn' hackers who serve as discovery agents for others • detect and remove a hacker's network sniffers (discovery agents) degrade capabilities of discovery agents: • modify a hacker's sniffers so they garble captured data. The hacker may regard them as too problematic to use on the network. interfere with target's directions to the discovery agent: • install a firewall to block a hacker's access to an installed sniffer
Action Type	***Ways to Defeat Communication of the Report*** (the hidden thing is not successfully communicated)
alter transmission or receipt of report	block the transmission or receipt of the report • configure firewall to drop outgoing ICMP packets, which are used by the hacker tool LOKI to communicate covertly
alter recorded report	falsify or destroy the recorded report • when a hacker's vulnerability scanner (discovery agent) is found running on a computer inside a network, falsify or erase the recorded results.
Action Type	***Ways to Defeat the Target's Recognition*** (the target does not learn of the hidden thing from the report)
affect report	confuse target by causing discovery agent to report things resembling hidden thing • honeyd impersonates many vulnerable computers, causing a hacker's vulnerability scanner to return an overwhelming number of false positives.
diminish target's learning capability	cause the target's learning resources to be insufficient • reduce the target's time available for the report; for example, law enforcement's aggressive pursuit of a hacker causes the hacker to spend more time on evasion and defence, and thus the target has less time for learning about victims' networks.

The hiding model is applicable to both deceptive hiding and non-deceptive hiding (that is, denial). Non-deceptive hiding defeats the target's discovery process, but without misleading the target.

A topic for future research is extending the discovery-process models to deceptive showing. In this case, the discovery process would be manipulated to portray something false. The model might also be extended to deceptions aimed at altering the target's intentions, so that the target no longer attempts to discover the hidden thing. Another topic for future research is developing metrics for evaluating the effectiveness of techniques for hiding (and showing). For computer security, the metrics could be based on those used to evaluate other types of security mechanisms.

References

Bell, J., Whaley, B. (1982) *Cheating and Deception*, Transaction Publishers, New Brunswick, NJ.

Cohen, F. (1998) A Note on the Role of Deception in Information Protection, *Computers & Security*, **17**:483-506.

Dewar, M. (1989) *The Art of Deception in Warfare,* David & Charles, London.

Fowler, C., Nesbit, R. (1995) Tactical Deception in Air-Land Warfare, *Journal of Electronic Defense*, **18**(6):37-44.

Goldsmith, D., Schiffman, M. (1998) Firewalking : A Traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access, URL: http://www.packetfactory.net/projects/firewalk [Accessed: August 30, 2006).

Joint Doctrine Division (1996) *Joint Pub 3-58, Joint Doctrine for Military Deception*, Joint Education and Doctrine Division.

Julian, D. (2002) *Delaying-Type Responses for Use by Software Decoys,* master's degree thesis, Naval Postgraduate School, Monterey, CA.

McClure, S., Scambray, J., and Kurtz, G. (1999) *Hacking Exposed : Network Security Secrets and Solutions,* Osborne/McGraw-Hill, Berkeley.

Rowe, N. (2005) Types of Online Deception, *Encyclopedia of Virtual Communities and Technologies,* Idea Group, Hershey, PA.

Rowe, N. and Rothstein, H. (2004) Two Taxonomies of Deception for Attacks on Information Systems, *Journal of Information Warfare,* **3**(2):28 – 40.

Schum, D. (1999) Marshaling Thoughts and Evidence during Fact Investigation, *South Texas Law Review*, **40**(2): 401-454.

Spitzner, L. (2003) *Honeypots : Tracking Hackers,* Addison Wesley, Boston.

U.S. Army (1988) *FM 90-2 Battlefield Deception*, U.S. Army.

U.S. Marine Corps (1989) *FM 15-6 Strategic and Operational Military Deception: U.S. Marines and the Next Twenty Years,* U.S. Marine Corps.

U.S. Marine Corps (1997) *MCDP 1-3 Tactics*, U.S. Marine Corps.

Whaley, B. (1982) Toward a General Theory of Deception, *Journal of Strategic Studies*, **5**(1):178-192.

Causes and Effects of Perception Errors

L. Brumley[1], C. Kopp[2] and K. Korb[3]

Clayton School of Information Technology,
Monash University, Australia
E-mail: [1]lbrumley@csse.monash.edu.au, [2]carlo@csse.monash.edu.au;
[3]korb@csse.monash.edu.au

Abstract

This paper proposes that both Information Warfare attacks and non-intentional perception errors can be categorised as causes of misperception. The causes of misperception are then analysed in the terms of Boyd's OODA loop model to determine when they cause errors to occur. The OODA loop model is then expanded to produce a theoretical model of the internal process of the Orientation step of the OODA loop. One of these errors is then explained in greater detail with the new model.

Keywords: Information Warfare, OODA loop, perception, misperception, deception, self-deception, perception errors

Introduction

The decision-making processes of biological organisms, machines and organisations all rely upon the availability of information. They continually gather and process information about their surroundings, building and updating a model of the world, which influences their perceptions and decisions. Individuals can gain a competitive advantage by tainting an opponent's model of the world, thereby negatively influencing its decision-making ability. This can be achieved by attacking the opponent's information gathering and processing facilities and its information directly, with Information Warfare attacks. Various cases of perception errors and self-deception (Dixon, 1976; Peck, 1983; Speer, 1970) also show that individuals can inadvertently or deliberately manipulate their model of the world in a detrimental manner. While these manipulations are not caused by a competitor, they do produce the same outcomes as attacks performed by a competitor. As both deliberate attacks and unintentional errors can cause the same effects, they can both be categorised as causes of misperception.

This paper also examines the importance of the correct interpretation and analysis of information to decision-makers. The information interpretation and analysis step of a well known model of the decision-making cycle, the OODA loop model, is examined and an expanded description of this model's information interpretation step is proposed. The model developed is then used to better understand the processes of Orientation and aid the analysis of errors that occur during the Orientation step.

Information Warfare

Information Warfare is defined as the use of offensive and defensive actions against competitors, which both utilise and target information in order to gain an informational advantage (Denning, 1999; Hutchinson & Warren, 2001).

There are many different methods by which offensive Information Warfare attacks may operate. Previous works by Borden (1999) and Kopp (2000) have categorised the various offensive Information Warfare actions into canonical strategies. Both of these categorisations are quite similar, with the main difference between them being that Kopp's work divides Borden's Denial category into Denial by Destruction and Denial by Subversion. The canonical strategies are described below in terms of an attacker and a defender who exchange information via a channel, using Borden's labels first and Kopp's labels in brackets.

1. **Degradation or Destruction (or Denial of Information)**
   Degradation or Destruction attacks aim to deny information to a defender either by flooding the information channel with noise or by altering an object to more closely resemble the channel's background noise.
2. **Corruption (or Deception and Mimicry)**
   In Corruption attacks, the attacker communicates corrupted information to the defender, which mimics a signal that the defender accepts as authentic. The signal is perceived by the defender as authentic and it causes the defender to alter its beliefs to the benefit of the attacker.
3. **Denial [1] (or Disruption and Destruction)**
   During a Denial [1] attack the defender's information receiver is destroyed or disrupted to restrict its information gathering. A disruptive attack temporarily prevents information gathering, while a destructive attack destroys the information receiver.
4. **Denial [2] (or Subversion)**
   A Denial [2] attack induces the defender to perform a self-destructive action or prevents the performance of a beneficial action.
5. **Exploitation**
   Exploitation places a receiver in parallel with the defender, providing the attacker with the same information as the defender. Exploitation is not technically an Information Warfare attack as it does not manipulate the information channel or the receiver; however it has been listed here for completeness.

Information Warfare attacks do not need to be implemented individually, they can also be combined into a series of strategies, which forms a compound strategy (Kopp, 2005a). A compound strategy is a structured network of interrelated Information Warfare attacks, where the combination of attacks shifts the defender to an intended final state.

Decision Cycle Modelling

Various models have been proposed for modelling the decision cycles of individuals and organisations (Neisser, 1976; Norman, 1990; Russell & Norvig, 1995; Boyd, 1996). They all model an individual's sequence of information gathering, decision making and acting behaviours, as feedback loops between the individual and its environment. While all of these models are suitable for representing an individual's decision-making process, Boyd's OODA loop model will be used as it is better known in the Information Warfare domain.

The OODA loop model was initially developed to instruct fighter pilots how to make decisions during aerial combat and later generalised to military strategy. Its name is an acronym of the steps of the loop - Observation, Orientation, Decision and Action. An individual starts in the Observation step gathering new information about its environment. In the Orientation step the newly gathered information is processed and integrated into the individual's model of the world. Next is the Decision step where the individual uses its updated model of the world to decide what it should do. The final step is Action, where the options that were previously selected are performed. The individual's actions will change the state of the world in some way, which the individual can observe in future OODA loop iterations.

During the Observation step the individual uses sensors to gather information about the state of the environment. Sensors may include eyes, ears and noses for biological organisms and switches, scanners, video cameras and barcode readers for machines. Some properties that they may measure include light, temperature, sound, pressure or vibration.

The Orientation step is an important element of the OODA loop, as it is where new information is processed and then integrated into the individual's model of the world. The processing and integration of the information is dependent on the knowledge that already exists inside its model of the world. Boyd states that during the Orientation step an individual combines new information, previous experience, cultural traditions, genetic heritage and analysis and synthesis. As individuals will have different models of the world, it is possible for multiple individuals to observe the same stimulus and develop a different interpretation.

An individual can Decide what actions it should perform after updating its model of the world. There are many methods that individuals may use to choose between possible options; however the OODA loop model places no restrictions on an individual's decision-making method. Possible decision-making methods include rule-based methods, utility-based methods such as Game Theory (Morgenstern & von Neumann 1953) and random selection of options.

Finally, the individual Acts and performs the options it has selected. Actions may include moving, communicating or the manipulating objects in the world. An individual changes the state of the world by acting and these changes can be observed by other individuals. Individuals can fail to perform their selected Actions. Communication fails if the audience cannot understand the message. Individuals may be unable to perform complex physical actions, such as dance steps or athletic movements.

Boyd also indicates that an individual's rate of progression through the OODA loop is important. An individual that decides and acts faster can change the state of the world before its opponent can - which may create differences between the actual world and the opponent's expected world. Boyd (1987a) refers to this behaviour as "operating inside an opponent's OODA loop" (Boyd 1987a, pp. 44-47) and says it will make a faster decision-maker appear to be ambiguous to a slower one. While this important property can be used to produce perception problems for a slower decision maker, it will not be explored here.

Causes of Misperception

Misperception occurs when an individual gathers and analyses information from its environment, before producing a model of the world that does not accurately reflect reality. The individual may not correctly perceive the intentions or actions of others, the existence of objects or the occurrence of events. Misperception may be caused by flawed analysis methods, incorrect information or a combination of these two problems. Misperceptions can be caused by a number of natural errors in the early stages of the perceiver's decision-making cycle. The same perception and analysis errors can also be caused by Information Warfare attacks.

Information Warfare attacks may damage or destroy information receivers, camouflage information so it cannot be perceived or supply corrupt information. Information receivers that have been attacked may provide incorrect information. Information Warfare attacks aim to cause the defender to misperceive or to affect the defender in some way that will cause future misperceptions. An attacker attempts to shape these misperceptions to its benefit. Once a misperception has occurred its effects may be felt for as long as the misperceiving individual retains the incorrect belief.

Information gathering errors

Misperception may first occur during the Observation step, when the individual gathers new information. Due to a perception error the individual is unable to correctly perceive the environment and unknowingly gathers incorrect information. The incorrect information is then used by the misperceiving individual in later steps of its OODA loop, with the individual typically unaware that the information is incorrect. Perception errors are caused by flaws in the individual's information receiver. Eyes and ears are common information receivers for biological individuals, while motion sensors and pressure plates are may be used by electronic or mechanical systems. Flaws may be caused by design limitations of the receiver, natural deterioration of the receiver or the actions of an attacker.

Receiver limitations are flaws in the design of the individual's receiver which have always existed in the individual. Such a flawed receiver typically gathers incorrect information under a certain set of conditions, although in extreme cases it may gather no information at all.

Intentional receiver degradation is caused by a Denial [1] attack that destroys or disables the defender's information receiver. A damaged receiver may gather less information or corrupt the information gathered, while a destroyed receiver will gather no information. By destroying or disabling the information receiver, the attacker has reduced the quality or quantity of information that a defender may gather, however the defender is inherently aware of the attack.

Natural deterioration occurs as the individual uses its information receivers over time. For biological individuals inherited genetic conditions, diseases, accidents and aging are possible causes of receiver deterioration, while electronic or mechanical receivers may suffer from component wear out, accidental damage, or random failure modes (Bazovsky, 1961).

Natural deterioration and Denial [1] attacks both damage a defender's information receiver. While the defender will be aware of the damage to their information receiver, it may be unable to determine whether the damage is due to an attack or a natural failure. Attackers can exploit this ambiguity by disguising their Denial [1] attack as an instance of natural deterioration, to provide a further advantage over the defender.

Information processing errors

The next location where misperception may occur is the Orientation step. When this occurs the individual gathers correct information, but interprets it incorrectly, producing an incorrect model of the world. The incorrect interpretation is caused by biases or flaws in the individual's process. There are many potential flaws, including incorrect assumptions about the world, analysis algorithms that do not operate correctly for all possible inputs or biases that predispose an individual to a particular interpretation of input data. These flaws are part of the individual's model of the world and will remain there until they are removed or replaced.

Some optical illusions (Wade, 1982) are cases of an information processing error, where the brain incorrectly interprets the visual information it has perceived. Biases that are part of the human visual processing system cause these optical illusions, which may cause people to see movement where none exists, hidden objects in an image or even see an image as something it is not.

The flawed analysis methods may have been caused by an earlier Corruption attack, which introduced a new corrupted analysis method, incorrect assumption or other flaw into the defender's model of the world or corrupt an existing one.

Deception

Deception is simply another name for the Corruption Information Warfare strategy and is therefore a potential cause of misperception. A Corruption attack is intended to cause a specialised misperception in the defender that the attacker can benefit from. Deception is typically used in nature either by predators mimicking something that their prey perceives as harmless or by prey mimicking species that their predators will not predate upon. Kopp & Mills (2002) have listed a number of species that use mimicry against others.

A deception attack starts when the attacker decides to deceive the defender. The attacker acts and places the corrupted information into the world, where the defender will perceive it. The defender gathers the corrupted information during its Observation step and analysing the corrupted information during Orientation. If the defender believes the corrupted information is plausible, then it is integrated into its model of the world. By accepting the corrupted information as true, the defender has erroneously corrupted their model of the world. During the Decision step the defender's decisions may be influenced by the corrupted information, which will then affect the defender during its Action step. The defender's future decision-making cycles may be affected by the corrupted information until it is removed.

If the deception attempt fails the defender will not add the corrupted information to its model of the world. Failure occurs if the defender possesses information that disproves the corrupted information or it considers the attacker to be an untrustworthy information source. It may also provoke a response from the defender. If the defender believes that the attacker is intentionally using deception then it may consider the attacker untrustworthy. The defender may also question the veracity of information previously received from the attacker. Haswell (1985) states that an attacker should consider the consequences of failure when planning a deception attempt. Deception should not be attempted if the penalty for failure is too high.

Deception can also be unintentionally caused by miscommunication. In this case, the attacker accidentally corrupts information during its Action step, before communicating it to others. The defender then perceives the corrupted information and acts as it would during an intentional deception attempt. A defender may be unable to distinguish between unintentional miscommunication and intentional deception. Attackers can exploit this uncertainty by camouflaging their deception as an error. Defenders can also incorrectly assume that an unintentional miscommunication is actually an intentional deception attack.

Self-deception

The word self-deception suggests that it is simply a case of self-targeted – or reflexive – deception (Demos, 1960). Self-deception may be more accurately described as an intentional misinterpretation in order to support a favoured, but unrealistic belief (Szabados, 1974). A self-deceiver either possesses an unreasonable belief or desires to change their belief to one that is more desirable. However, this belief is disproved by the correct interpretation of the self-deceiver's available information possesses. The self-deceiver then intentionally misinterprets the information in a manner that supports their desired belief. Self-deception can therefore be considered as a self-targeted Corruption attack, which targets the self-deceiver's information processing methods during the Orientation step.

Andrews (2004) states that self-deception by various American intelligence and security agencies led to the destruction of the World Trade Center. While instances such as this demonstrate the dangers of self-deception, others have argued that it, in some cases, can provide benefits.

Trivers (1976) asserts that self-deception, when used with deception against another, can aid the self-deceiver. A deceiver's behaviour during a deception attempt, such as nervousness or sweaty palms, can reveal their dishonesty. The probability of a successful deception attempt can be increased by preventing behaviour that suggests untruthfulness. According to Trivers, an attacker first uses self-deception to acquire the deceptive belief it wishes to communicate. Since it now accepts the deceptive information as true, it can communicate it to the defender without its behaviour indicating that it is lying. After the deception, the self-deceiver restores the correct belief to its model of the world and takes advantage of the defender's corrupted world model. Here the self-deceiver risks corruption of their own model if the self-deception fails and retaliation from their opponent should the deception fail, in exchange for an increased chance of the deception succeeding. The use of self-deception to aid deception is an instance of multi-channel support for a deception attempt, which is one of Haswell's (1985) seven principles of deception.

Ramachandran (1996) has argued that Triver's explanation of the benefit of self-deception is invalid, as the act of self-deception hides any knowledge of the deception from the self-deceiver. Ramachandran believes that the self-deceiver cannot benefit from the deception attack, as it has no knowledge of it. However this is not always true, as a self-deceiver can benefit from deception without being aware of it. Ramachandran instead proposes that self-deception provides a benefit to individuals, by acting as a defence mechanism that maintains a coherent internal belief structure. This proposal concurs with Cognitive Dissonance theory (Festinger, 1957), which states that contradictory beliefs are dissonant and cause the individual psychological discomfort. Individuals will act to reduce their discomfort, using self-deception to reduce dissonance between their beliefs and thereby reduce their discomfort. This usage of self-deception obtains a corrupted model in exchange for reduced dissonance. Organisational examples of Cognitive Dissonance reduction are commonly seen in cases of Groupthink (Janis, 1982).

A self-deceiver can receive both of these benefits simultaneously, allowing it to reduce its own dissonance and deceive others. The self-deceiver first uses self-deception to reduce its dissonance, which introduces false beliefs into its model of the world. Later the false beliefs are communicated to an opponent, who believes they are true. This deception is unintentional and causes the opponent to behave in a manner that benefits the self-deceiver. This usage of self-deception also combines the drawbacks of the two self-deception methods – the corruption of the model of the world and the potential failure of the deception attempt. This dual-purpose usage of self-deception is a powerful method of perception management, as it allows a self-deceiver to implant the same false belief in itself and then others.

Van Evera (2002) discusses the tendency of organisations to cripple their own self-assessment functions, which leads to a self-deceptive aggrandised assessment of their capabilities. Kopp (2005b) and Hutchinson (2005) discuss how propaganda is used to deceive the target populations of nations, resulting in an incorrect assessment of the nation's actions, intentions and capabilities. In all of these cases, self-deception during self-assessment reduces dissonance caused by evidence of ineffectiveness or failure and permits the deception of others as to the self-deceiver's success.

A common usage of self-deception is to reduce cognitive dissonance and this process will be described. During the Orientation step new gathered information is analysed and found to conflict with the individual's model of the world. As the new information and existing world model are dissonant, the individual experiences discomfort, and desires to reduce it. This can be achieved by manipulating either the new information, the existing model of the world or the world itself. Information is manipulated during the Orientation step, while the world cannot be manipulated until the Action step. Once the dissonance is removed, the information is integrated into the model of the world. The individual then continues through the OODA loop cycle, using the corrupted model of the world as the basis for its Decisions and Actions. This maintains internal cohesion by reducing dissonance for the self-deceiver, at the expense of creating false beliefs in its model of the world.

After the self-deception, the individual may decide that it will communicate its corrupted information to an opponent. This may be due to either an intentional or unintentional attempt to aid deception. The individual communicates the corrupted information to its opponent, who is deceived by it. In a case of unintentional deception, the opponent is influenced to perform some harmful action due to the corrupted information, and the self-deceiver benefits from this without being aware of the deception. In the case of Trivers' self-deception aiding deception, the self-deceiver later removes the corrupted information from its model of the world. Since it is now aware of its deception, it can take advantage of the opponent's error.

Comparison of Misperception Types

A brief comparison of the details of the various misperception types described in earlier sections of this paper is presented in Table 1 for the previously stated assumptions. Here each type of misperception is listed, along with any Information Warfare attacks that may cause it, where it causes an error in the defender's OODA loop, the initiator of the attack that causes the misperception (if there is one) and the potential value and risks to the individual implementing the attack.

Information Gathering Errors were the only misperception type identified that did not occur during the Orientation step. The majority of the misperception types previously discussed cause errors during the Orientation step. It can be seen that there are several methods that affect the Orientation step, which are caused by either Information Warfare attacks or various failures in the individual. This concurs with Boyd's (1987b, p16) declaration that the Orientation step is the *schwerpunkt*, or focal point, of the decision-making cycle.

It can be seen that Gathering and Processing errors may be caused by either Information Warfare attacks or various faults and flaws of the perceiving individual. The individual has either always possessed these faults and flaws or has developed them over time without the influence of an attacker. Self-deception can also cause individuals to develop an incorrect model of the world without any input from an attacker. As these errors also produce the same effects as Information Warfare attacks, it may be difficult for an individual to determine whether or not it is the victim of an attack.

Gathering and Processing errors both produce no benefits for the individual, while self-deception may provide some benefit, with the potential disadvantage of corrupting the individual's model of the world. The individual's opponents typically benefit from the individual's misperceptions; however they can also suffer from them. As stated earlier in the analysis of self-deception, an individual's self-deception may cause them to perform unintentional deception against their opponents. Also self-deception or information gathering and processing errors may cause an individual to act in a manner that is harmful to both it and its opponent. It can be reasoned that since these misperceptions are not initiated by the opponent, the opponent will lack control over them. Due to this lack of control, the opponent should not be exceedingly dependant upon the misperceptions to influence the individual in a manner that benefits the opponent.

Table 1: A Comparison of Misperception Types and their Effects

Misperception Type	**IW Strategy Possibly Used**	**Error Step Location**	**Initiator**	**Potential Value**	**Potential Risks**
Information Gathering Error	Degradation or Destruction, Denial [1]	Observation	Attacker or No one	N/A	Incorrect Information
Information Processing Error	Corruption	Orientation	Attacker or No one	N/A	Incorrect World Model
Deception	Corruption	Orientation	Attacker	Opponent's model corrupted	Opponent Retaliating
Self-Deception aiding Deception	Self-Corruption + Corruption	Orientation	Self	Opponent's model corrupted	Corrupted Model, Angered opponent
Self-Deception reducing Cognitive Dissonance	Self-Corruption	Orientation	Self	Reduced Dissonance	Corrupted Model
Combined Self-Deception	Self-Corruption + Corruption	Orientation	Self	Opponent's model corrupted + Reduced Dissonance	Corrupted Model, Opponent retaliating

Attackers may be able to disguise intentional Corruption and Denial [1] attacks from the defender, by concealing them as unintentional errors or miscommunications. In the case of Denial [1] attacks, there are many potential receiver failures that could be simulated by the attacker. The concealment of attacks allows the attacker to avoid retaliation from a defender. This is especially useful in the case of Denial [1] attacks, as the damaged information receiver is inherently obvious to the defender.

From the analysis, it can be seen that Denial [2] is the only canonical Information Warfare strategy that does not directly cause misperception. This may seem obvious, given that it targets the defender's actions instead of their perceptions. However Denial [2] attacks can indirectly cause misperception, if they cause the defender to perform actions that damage its information gathering or processing apparatus. This will lead to future errors in the defender's Observation and Orientation steps. When Denial [2] is used, it enters the target system with a corruption attack (Kopp, 2005b) and as such enters the target system through the Orientation step, with the self-destructive involuntary behaviour later occurring in the Action step.

The Importance of Orientation

The Orientation step is the major element of the OODA loop model, as it processes newly gathered information and existing knowledge to produce an updated model of the world, which will shape future decisions and actions (Boyd, 1987b, p26). Richards's (2001) representation of Boyd's model describes the Orientation step as a melting pot where new information, previous experience, genetic heritage, cultural traditions and analysis and synthesis methods are combined to somehow update the model of the world. However this process is not described in detail.

The main functions of the Orientation step are to:

1. Recognise known objects, events and relationships, allowing the retrieval and use of existing knowledge linked to those objects,
2. Analyse new information with known processing methods, in order to predict the future state of the world,
3. Assess completion of aims and the development of new aims, based on the expected future world,
4. Determine potential options that allow the individual to achieve its aims and the consequent outcomes of these options.

It is proposed that the Orientation step can be partitioned into four sequential sub-steps that perform these functions. The sub-steps are Identification, Interpretation, Aims Derivation and Options Generation (Figure 1).

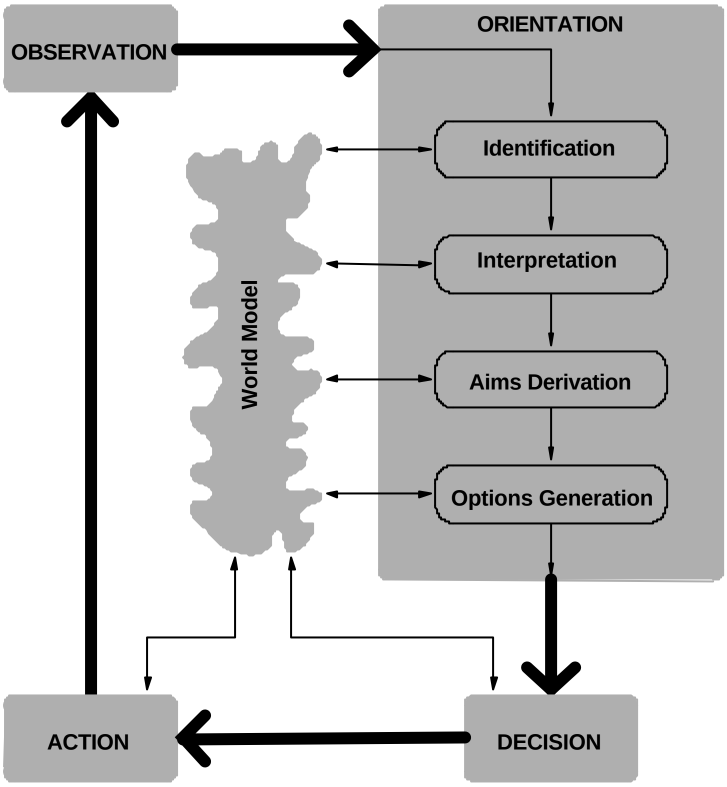

Figure 1: Expanded Orientation step

Orientation starts with an Identification sub-step, where the individual compares the newly gathered information to information that they have already stored. Known objects and events are recognised, while unknown objects and events are marked with placeholders that roughly describe them. If objects or events are unexpected, then they may cause cognitive dissonance in the individual. An unexpected object or event is one that the individual's world model does not predict and could be caused by a previous corruption attack, a lack of knowledge or a previous incorrect interpretation.

The next sub-step is Interpretation where the individual takes the identified and unidentified objects and the existing world model and determines how the world has changed in the past and will change in the future. Information about identified objects - such as their properties, behaviour and capabilities - is retrieved from the world model and used to predict the future (and past) state of the world. Unidentified objects will have some estimated attributes assigned to them, which may be incorrect but can be refined during future perceptions of the object. Learning also occurs here, as new information updates the model of the world. Interpretation is where previous misperceptions will cause errors, as predictions for the past and future will be produced using existing incorrect information or analysis methods.

During the Aims Derivation sub-step the individual uses the updated model of the world to determine whether it is achieving its aims. New aims are also developed to guide the individual's behaviour. An individual's aims can be considered as a set of programmed, higher order aims (such as survival and reproduction) and a lower order set of aims that are derived from them (survival requires avoiding predators and eating food). An updated model of the world is required to remove achieved and impossible aims, update unachieved aims and produce new aims.

Options Generation uses the individual's aims and updated model to produce a number of potential options the individual may pursue and the expected outcomes of each one. Options will be constrained by the individual's knowledge of its own capabilities. Outcomes are produced by the individual predicting what will happen if it implements each option it believes it can perform. The accuracy of an individual's expected outcomes are dependent on its model of the world.

The Decision step compares the produced options and outcomes, assessing the predicted outcomes on some criteria. The outcome that is perceived to be the best is chosen and the option that leads to it is then performed in the Action step. The individual now expects that the future world will match their predictions.

Earlier it was identified that both Corruption attacks and Self-Deception occur during the Orientation step. Since the Orientation step has been partitioned into sub-steps it is now necessary to determine during which sub-steps Corruption and Self-Deception occur.

During a Corruption attack, corrupted information enters the individual's system through Observation and is first examined during Identification. The individual compares elements in the new information against those stored in its memory. This is where the error occurs, as the corrupted information mimics a signal that the individual incorrectly identifies as a valid signal. For example if a decoy vehicle is used in a successful corruption attack, the defender identifies it as a real vehicle. The world model is updated with the erroneous information and it can now affect subsequent iterations of the OODA loop.

The previous definition of self-deception as an intentional misinterpretation indicates that it occurs during the Interpretation sub-step. An individual first collects new information during the Observation step. During the Identification sub-step known objects, events and relationships are identified from the gathered information. Errors do not occur during a self-deceiver's Identification sub-step, however what it has identified may be dissonant with what it expects to find. During Interpretation the new information is analysed to update the model of the world and predict the future state of the world. The interpretation of the new information may disprove a belief that the individual possesses or desires to possess. The desire to possess this belief may be motivated by dissonance reduction. If this occurs, then a self-deceiver will interpret the information again, in an irrational manner that produces evidence that fails to disprove the desired belief and possibly even supports it. The individual updates its model of the world with the revised interpretation of the new information. The model is then used by the Aims Derivation sub-step and the Options Generation sub-step to direct the self-deceiver's future behaviours.

Conclusion

The Orientation step is an important element of the OODA loop, as it is where the individual's model of the world is maintained. Manipulation of the model of the world will affect both current and future decisions and is performed by various types of misperception. Various faults and failures that affect an individual have identical effects to Information Warfare attacks. Attackers can exploit this by disguising their attacks as random failures, to conceal their responsibility for the attack from the defender.

Self-deception is typically used to reduce discomfort caused by dissonance between an individual's model of the world and the real world. However it can also facilitate intentional and unintentional Corruption attacks against others, which will lack the cues that indicate the individual's untruthfulness.

References

Andrews, C. (2004) Belief systems, information warfare, and counter terrorism, *Proceedings of the 5th Australian Information Warfare & Security Conference 2004 (IWAR 2004)*, Perth, Western Australia, pp. 92–99.

Bazovsky, I. (1961) *Reliability Theory and Practice*, Prentice Hall, Engelwood Cliffs, New Jersey.

Borden, A. (1999) What is information warfare?, *Aerospace Power Chronicles, United States Air Force, Air University, Maxwell AFB,* URL: http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html [Accessed August 17, 2005].

Boyd, J. R. (1987a) Strategic game of ? and ?, Slideshow, URL: http://d-n-i.net/boyd/strategic_game.pdf [Accessed September 7, 2006].

Boyd, J. R. (1987b) Organic Design, Slideshow. URL: http://d-n-i.net/boyd/organic_design.pdf [Accessed September 7, 2006].

Boyd, J. R. (1996) The essence of winning and losing, Slideshow, URL: http://www.belisarius.com/modern_business_strategy/boyd/essence/eowl_frameset.htm [Accessed June 17, 2006].

Demos, R. (1960) Lying to oneself, *The Journal of Philosophy,* **57**(18): 588–595.

Denning, D. E. (1999) *Information Warfare and Security,* Addison-Wesley, Boston.

Dixon, N. (1976) *On The Psychology of Military Incompetence*, Jonathon Cape, London.

Festinger, L. (1957) *A Theory of Cognitive Dissonance*, Stanford University Press, Stanford, California.

Haswell, J. (1985) *The Tangled Web*, John Goodchild Publishers, Wendover.

Hutchinson, W. E. (2005) The relationships between western governments, military, and the media during conflicts since 1980, *in* G. Pye & M. Warren (eds), *Proceedings of the 6th Australian Information Warfare & Security Conference 2005 (IWAR 2005)*, Geelong, Victoria, pp. 182–187.

Hutchinson, W. & Warren, M. (2001) Principles of information warfare, *Journal of Information Warfare,* **1**(1): 1–6.

Janis, I. L. (1982) *Groupthink: Psychological studies of policy decisions and fiascoes*, Houghton Mifflin, Boston.

Kopp, C. (2000) Information warfare: A fundamental paradigm of infowar, *Systems: Enterprise Computing Monthly,* Auscom Publishing Pty Ltd, Sydney, NSW, February, 2000, pp. 47–55, URL: http://www.ausairpower.net/OSR-0200.html [Accessed August 17, 2005].

Kopp, C. (2005a) The analysis of compound information warfare strategies, *in* G. Pye & M. Warren (eds), *Proceedings of the 6th Australian Information Warfare & Security Conference 2005 (IWAR 2005),* Geelong, Victoria, pp. 90–97.

Kopp, C. (2005b) Classical deception techniques and perception management vs the four strategies of information warfare, *in* G. Pye & M. Warren (eds), *Proceedings of the 6th Australian Information Warfare & Security Conference 2005 (IWAR 2005),* Geelong, Victoria, pp. 81–89.

Kopp, C. & Mills, B. (2002) Information Warfare and Evolution, *in* W. Hutchinson (ed.), *Proceedings of the 3rd Australian Information Warfare & Security Conference 2002 (IWAR 2002),* pp. 352–360.

Morgenstern, O. & von Neumann, J. (1953) *Theory of Games and Economic Behaviour*, Princeton University Press, Princeton.

Neisser, U. (1976) *Cognition and Reality*, W. H. Freeman, San Francisco.

Norman, D. A. (1990) *The Design of Everyday Things*, Doubleday, New York.

Peck, M. S. (1983) *People of the Lie: the hope for healing human evil*, Simon and Schuster, New York.

Ramachandran, V. S. (1996) The evolutionary biology of self-deception, laughter, dreaming and depression: Some clues from anosognosia, *Medical Hypotheses*, **47**: 347–362.

Richards, C. W. (2001) Boyd's OODA loop, Slideshow, URL: http://www.d-n-i.net/fcs/ppt/boyds_ooda_loop.ppt [Accessed August 15, 2005].

Russell, S. J. & Norvig, P. (1995) *Artificial Intelligence: A modern approach*, Prentice Hall, Englewood Cliffs, New Jersey.

Speer, A. (1970) *Inside the Third Reich: Memoirs by Albert Speer*, Collier Books, New York. Translated by Richard and Clara Winston.

Szabados, B. (1974) Self-deception, *Canadian Journal of Philosophy*, **4**(1): 51–68.

Trivers, R. (1976) *Preface In: The Selfish Gene (Dawkins, R., ed.)*, Oxford University Press, pp. v–vii.

Van Evera, S. (2002) Why states believe foolish ideas: Non-self-evaluation by states and societies, URL: http://web.mit.edu/polisci/research/vanevera/why_states_believe_foolish_ideas.pdf [Accessed August 15, 2005].

Wade, N. (1982) *The Art and Science of Visual Illusions*, Routledge and Kegan Paul, London.

Belgium's intelligence community: new challenges and opportunities

Maarten Vanhorenbeeck

School of Computer and Information Science
Edith Cowan University, Australia
E-mail: mvanhore@student.ecu.edu.au

Abstract

Recently Belgium's intelligence function has been heavily criticized, predominantly regarding its effectiveness and professionalism. Some voices have even gone as far as to propose abolishment of part of the intelligence community. This paper identifies why efficient intelligence gathering is more than ever a requirement for both the Belgian and European leadership. It reviews Belgium's intelligence history and studies the roots of its criticisms. Instead of proposing intelligence 'reform', it identifies important parameters of how contemporary intelligence should be conducted, and how the intelligence services can adapt within the constraints that apply to them.

Keywords*: Intelligence; Belgium; Europe; Intelligence Reform*

The history and constitution of Belgian Intelligence

Belgium's 176 year old intelligence function was finally recognized by law on November 30th 1998. Described in this law on the arrangement of the intelligence- and security-services, are the civilian *Veiligheid Van de Staat* (Dutch) or *Sûreté de l'état* (French), which will hereafter be referred to as the VS; and the military *Algemene Dienst Inlichtingen en Veiligheid* (Dutch) or *Service Général du Renseignement et de la Sécurité* (French), hereafter referred to as the ADIV (FOD Justitie, 1998a).

Summarized, the responsibilities of the VS are described as acquiring, analyzing and processing intelligence on activities that could jeopardize internal and external security of the state and the scientific and economic potential of the nation. It also deals with investigations pertaining to security clearances and dignitary protection. It resorts mainly under the Ministry of Justice, though the Ministry of Interior Affairs does have some use of its services.
Its Military counterpart, the ADIV, acquires, analyzes and processes intelligence on activities that could violate national territory or the security of Belgian subjects abroad. It also protects military secrets, personnel and installations.

This law does not differentiate between the gathering of data - as raw source material - and the production of intelligence – it specifies the *gathering of intelligence*. Identified by a government committee, this issue was not considered significant (Kamer, 1997). Police law also assigns certain intelligence functions to the police departments as long as they directly apply to policing tasks. They are however not considered intelligence services.

A third group, the *Coordination Service for Threat Analysis* or CODA was instated in July 2006 with as goal to perform evaluation of emerging threats. By law, the intelligence and police services, as well as the Federal Public Services of Finance, Transportation, Interior Affairs and Foreign Affairs are obliged to provide it with all information they acquire related to terrorism or extremism (FOD Justitie, 2006). The CODA replaces the Anti-terrorism Group AGG which had more limited sources of information.

ISSN 1445-3312 print/ISSN 1445-3347 online

A fourth institution related to intelligence is the supervisory *Permanent Committee for the Control of the Intelligence Services* or *Comité I*. This organization was signed into law on July 18th, 1991 and can either out of its own initiative or by request of the Chamber of People's Representatives, Senate or a number of defined Ministries, initiate investigations and review the operations of the intelligence services (Senate, 2006).

While this technical view represents the services as they are today, it would be invalid to reflect on their current place in society without having a brief look at their extensive history. The civilian intelligence function was founded in 1830 as the department of Public Security. While its duties were defined as to maintain internal security, it mainly concentrated on investigating foreigners on Belgian soil. Through signing of the Belgian constitution in 1831, the department as a separate entity was shut down and merged into the Interior Affairs department. Subsequently, in 1832, it was moved to the Justice department. (FOD Justitie, 1998b)

In 1840, shortly after Pierre-Joseph Proudhon's novel *What is property* and the subsequent rise of anarchist ideology (Woodcock, 1962), both anarchism and socialism became important challenges for the young intelligence service. The reality of this threat became clear with an attempted invasion by Belgian workers from Paris (Van Opstal, 2006), the so-called Risquons-Tout incident.

The First World War led directly to the establishment of a military intelligence service. This is where a complex organizational mix of the intelligence services starts - during the Second World War the Public Security department was also merged into the Defense department structure. During the occupation of Belgium its intelligence services operated from London and focused on maintaining contact between resistance groups and the government-in-exile.

As of the end of the Second World War, two separate intelligence functions had emerged – one military, resorting under the department of Defence, and one civilian, resorting under the department of Justice. Simultaneously, intelligence services worldwide became more focused on the threat emanating from the Communist front and the Eastern Block countries.

In the 1980s and 1990s terrorism took the place of the Cold War as the priority issue. In Belgium, the *Cellules Communistes Combattantes* executed fourteen bombings in 1984 and 1985. At the end of the 1990s, the GIA or *Groupement Islamique Armée* was the country's first confrontation with militant Islam.

Simultaneously, Belgium's intelligence services received bad press due to their involvement in Operation Gladio – the existence of CIA and NATO stay-behind armies charged with countering communism in Europe. These were publicly linked to acts of terrorism in Italy, significantly impacting public perception of the services. This scandal led to the 1991 founding of an oversight organization, the Comité I. (Comité I, 2006b, 2006c). This organization then identified the need for the 1998 framework legislation that defines the intelligence services today.

Voices of criticism

Criticism of the Belgian intelligence machinery can usually be attributed to one of two causes: either the intelligence target selection or an operation gone awry. Target selection is defined per the legal framework of 1998. A disputed regulation put forward in this law is the requirement on Belgian intelligence to analyse activities that could jeopardize internal security of the state. While this sounds like a perfectly reasonable requirement, it has a negative connotation quite specific to Belgium.

Belgium, a federal state, consists of the separate regions Brussels-Capital, Flanders and Wallonia. In addition, three communities are divided on language boundaries: French, Dutch and German. Particularly in Flanders, there is significant interest in splitting off from the rest of Belgium to form an independent European state. A number of mainstream political parties support this message, such as the *Nieuw-Vlaamse Alliantie* and the *Vlaams Belang*. While a democratic process, these parties could be identified as a potential target for intelligence gathering. Regardless of whether they have or have not been targeted, this argument has been used in public to label the intelligence services as undemocratic.

This situation was exacerbated in 2003, when a press article revealed that the VS had identified Soetkin Collier, the singer of a band selected for the Eurovision Song Contest, as being of extreme right ideology. The investigation also claimed she had a strong belief in Flemish independence (Seront, 2003). This incident led to the singer being banned from participating.

During a review investigation by the Comité I, the information gathered on the artist was found to be at least partially factual, though the type of communication done by the VS was not considered in line with the threat posed. In addition, the press leak did not originate with the VS (Comité I, 2004). It did open the service up to additional negative press coverage

A second type of criticism deals with those operations that did not go as planned. Two very recent examples are the escape of Turkish citizen Fehriye Erdal, suspected and later convicted of involvement with a terrorist organization, and the supposed smuggling of an isostatic press to Iran. Both incidents were brought to press in 2006, leading to the resignation of the then head of the VS.

As in most cases, truth behind these events was much more complex, and in both cases responsibility was to be shared between the VS and other parties. The Comité I published reports that indicated limited responsibility of the Veiligheid van de Staat in both affairs (Comité I, 2006b, 2006c). Nevertheless, the issue had in the meanwhile contributed to the deteriorating view of the intelligence service.

As is so often the case where a federal service needs to operate within the constituency of feuding political complexes, official criticism was not far away. Johan Vande Lanotte, head of the SP.A party (previously known as *Socialistische Partij – Anders*, which means Socialist Party – Different) proposed full-scale abolishment of the VS and its merger into the police services (VRT, 2006a); Ludwig Vandenhove, an SP.A colleague, proposed placing the VS under the jurisdiction of Interior Affairs instead of the Justice department (VRT, 2006b).

Operating the intelligence machinery

Defining intelligence is not an easy undertaking. After careful consideration, Michael Warner defined it as “secret, state activity to understand or influence foreign entities” (Warner, 2002, p. 7). Much can be said of this, and many may feel that there is no need for *secrecy* or the achievement of active *influence*, or perhaps even doubt whether state actors need to be involved.

A definition that may not be intended as such, but seems more appropriate to today's environment is put forward by Robert M. Clark. He defines it as being "about reducing uncertainty in conflict" (Clark, 2004, p. 26). This phrase implies that everyone can make decisions – intelligence merely enables a leader to reduce uncertainty regarding their outcome. Where information is sourced from, being secret, public or grey sources is less important. It allows for intelligence in business decision making or a social context.

Whilst intelligence is used continuously, those organizations most successful at exploiting it have processes that define its gathering and exploitation. One of such processes is the five phase intelligence cycle (Joint Chiefs of Staff, 2000):

This complete cycle can take place within one organization, or can take place by linkage to other organizations. In large intelligence machinery such as the UK for example, the Joint Intelligence Committee can direct the Government Communications Headquarters (GCHQ) to gather signals intelligence and the Secret Intelligence Service (SIS) to collect human intelligence from abroad. It then processes, analyses and disseminates this information to decision makers. Until recently, this complexity was missing from the Belgian system. The establishment of CODA now allows for such assessments. The VS and ADIV can thus operate as single source intelligence collection agencies, while CODA functions as an all-source analysis institution.

Limitations imposed on Belgian Intelligence

Budgetary constraints

National planned expenditures for the VS in 2007 are 21.6 million euros, compared to 15.3 million euros in 2004 (Kamer, 2005). Press reports indicate the service has some 500 employees in manpower (Herremans, 2006). Expenditure for ADIV is considered a whole part of the defence budget and not published. The VS budget is dwarfed by that of the *Algemene Inlichtingen- en Veiligheidsdienst* or AIVD, its equivalent in the Netherlands: in 2004 they expended 87.5 million euros (AIVD, 2004).

This budgetary discrepancy cannot be explained on the grounds of country sizing. While it would be perfectly normal if Belgium's social security expenditure is small compared to that of the Netherlands – Belgium has 10 million inhabitants, while the Netherlands has 16 million – this does not apply to intelligence, mainly due to changes in how threats need to be assessed.

Assessing threat levels

The old methodologies of intelligence analysis, being the use of trends & patterns and frequency analysis have been shown to be less applicable to the contemporary threat environment (Segell, 2005). Military invasion can often be identified by the gathering of troops on the border, but significant troop movements do not apply to attacks executed by non-state actors such as Al-Qaeda. The amount of tools available to forecast this type of attack is limited.

As such, Segell notes that the use of a third methodology is becoming preferred: probability analysis. This consists of "determination of the probability of a terrorist event based upon the risk analysis of latent threat and target vulnerability" (Segell, 2005, p. 229). The activity significantly differs from the other methodologies: not only in its approach, but also regarding how it should be resourced. In essence, infiltrating a terrorist group to acquire information requires good sources, not necessarily large teams. With probability analysis, assessments need to be made of potential terrorist targets. This requires detailed risk assessment, an expensive proposition.

If Belgium and the Netherlands are compared from this perspective, the amount of inhabitants becomes much less important. The Netherlands is a strategically important nation – hosting amongst others the International Criminal Court in The Hague; but this applies perhaps even more to Belgium which hosts the headquarters of both NATO and the European Union. In addition, Belgium is a significant transfer point of goods – with transport company DHL's European distribution centre in Brussels - and finances – being the home to international clearing houses SWIFT and Euroclear.

It is interesting to take note of the fact that some foreign intelligence services are adjusting to these new requirements. The Dutch AIVD reported that it had conducted security scans of the computer networks of ministries and regional security authorities. In addition, they had identified *vital products and sectors* within the Netherlands and had assisted them in performing risk assessments (AIVD, 2005).

From the yearly review report of the Comité I, it becomes clear that Belgium has not yet gone through such paradigm shift. The 1998 law provides for protection of the scientific or economic potential of the nation, and should enable the organization to perform such probability analysis. However, a great deal of political discussion is still preventing its actual implementation (Comité I, 2006a).

An alternative view on sizing

Friedman argues that excessive size of intelligence machinery has its toll on its efficiency (Friedman, 2006). The value of information, and subsequently of the intelligence product, is often very dependent on time. An organization in which intelligence needs to pass through many layers before reaching the consumer may prove obsolete.

In addition, while information systems can assist in identifying anomalies and patterns, identification of them as a threat or benign event is a human endeavour. Threats hidden in highly fragmented and individual components analysed by individual analysts without a view from the top are unlikely to be identified. This becomes more important with the recent change from symmetric to asymmetric threats: intelligence components were organized to work with limited numbers of large data blocks, such as troop movements. Distribution of these within an organization was relatively easy. With asymmetric threats, in which the adversary's approach is of a different, usually smaller, scale, analysis and synthesis of smaller data blocks becomes the norm.

Legal framework

There is still plenty of discussion regarding the VS' investigative powers. The current law specifies that information needs to be obtained either from other government departments, by inquiring with commercial organizations or through human sources.

Wiretaps, for example, long one of the basic instruments in the toolkit of intelligence services, are still out of their reach. Such actions need to be executed by police services, who are allowed to perform telephone taps under existing penalty code, provided that it concerns serious crime, and all other investigate methods have proven insufficient (FOD Justitie, 1995).

In 2004, Minister of Justice Onkelinx announced she would be issuing a proposal to allow the VS to perform wiretaps as well. Recent discussions in the Chamber of People's Representatives show it has not yet been approved and is being merged into new laws regarding data retention (Kamer, 2004). Due to this added complexity it is unlikely to qualify for prompt approval.

Constraints of movement

The civilian intelligence service VS is not authorized to conduct operations abroad. While this limitation does not apply to the military service ADIV, these activities are usually restricted to the military context and could be expected to be in direct support of planning and execution of operations by either the Belgian armed forces or its partners.

Obviously the lack of a foreign intelligence service such as the British Secret Intelligence Service, Australian Secret Intelligence Service and French *Direction Générale de la Sécurité Extérieure* (DGSE) places Belgium at a disadvantage compared to its neighbours. The perception of foreign spying does however not resonate with the view that Belgium extols of being a neutral country. The limited and mostly negative perception of the services by Belgian citizens combined with funding constraints make it highly unlikely these types of operations would be added to the intelligence portfolio.

The limitation on wiretaps mentioned earlier logically restricts the amount of information gathering that can be performed. It makes it unlikely that attention is currently being paid to Communications Intelligence (COMINT) and Signals Intelligence (SIGINT). The ADIV, however, often operates under foreign law. Belgium does have a law that allows foreign officials to conduct wiretaps on its soil (FOD Justitie, 2004). Presuming that the ADIV operates in countries with similar laws, this is an indication that COMINT development may have arisen organically within the service.

Public perception

Criticism by the political leadership has already been reviewed in more detail. Those same issues naturally also impact public perception. An initial step to improve this situation was a public exposition on the VS' 175 year service, organized in 2005. Further action would be useful to move the service away from the fringes and into society.

It can be questioned whether the amount of secrecy employed is in line with the organization's goal. While the organization releases relatively less information through its website than its British counterpart MI5, names of new intelligence analysts - by definition in the process of acquiring security clearances - are published in the official daily *Staatsblad* or Bulletin of Acts (FOD Justitie, 2003). This poses unnecessary risk to these employees as well as to the information they are cleared to access.

Creatively adjusting focus

It would be outside the scope of this paper to advocate intelligence reform. This term is too often used to describe cosmetic changes to process instead of creating an open culture of improvement that can dynamically adjust itself to changing requirements. After reform, an intelligence system usually settles into its new situation – only to be shaken on its foundations by an unpredictable event some years later. Instead, intelligence organizations should concentrate on continuous identification of new requirements. The organization should actively advocate its new profile instead of passively being subjected to it.

Rather, creatively adjusting the intelligence services' focus will be our main starting point. Such adjustments would take into account current requirements, limitations and constraints of the services and how these can be overcome

Actively tapping into open source intelligence

To some in the business this may read as merely effectively leveraging the power of the internet. Steele (2006, p. 522) however puts it this way: "Most of the relevant useful information is not secret. Unfortunately, it is also not online, and, regarding the rest of the world, not in English".

This is an extremely accurate statement. With the expansion of technology and especially the internet, the value of secrets is quickly eroding. At the famous Nevada military test site Area 51, mountains surrounding the facilities were gradually closed off over the years to prevent people from viewing the base. The availability of high resolution commercial satellite imagery of Area 51 in 2000 however, changed the picture drastically (Terraserver, 2006). As the images were made using a Russian satellite, there was also little awareness with the US military of this potential disclosure.

Looking further into Steele's statement, it is also important to note that indeed, not all open source intelligence is "online" or "on the internet" (Steele, 2006, p.522). This has its repercussions for intelligence gathering. It may be good to use current media advertising techniques as a starting point to ponder further on reality and clarify this statement.

With the rise of new media, there has been a shift from the use of demographic profiles in advertising, that segment the population by parameters such as age, to psychographic profiles that take into account interests of a certain group. While in the past, people advertised on BBC One because it attracted a large young audience, it is now possible to advertise on the Sci-Fi channel. The audience may be smaller, but if our goal is to sell a Star Trek DVD it is more likely to induce a purchase.

Communities built around such psychographic profiles, often termed interest groups, have always existed in the physical realm and are the obvious targets for human intelligence. These communities underlie society and can often provide significant intelligence. Examples are groupings of innovative small businesses, or religious groups concentrated around a church or mosque. In general, intelligence services acquire information from these groups not so much by infiltration, but by engaging sources already active within that community.

As such, an important source of information that appears to be underexploited is the use of cooperation as an information channel. The Dutch AIVD mentions in its yearly report that they provide security information to companies and reach out to business sectors that could be the target of foreign intelligence services (AIVD, 2006). Through these informal contacts, incident information can also flow back into the intelligence machinery.

Effectively leveraging the power of commercial organizations

Improving the protection of vital sectors of society is an important part of protecting Belgium's economic potential. Mentioned earlier was the Dutch approach of performing security scans of the internet infrastructure of public parts of the critical infrastructure. Within the current budget, the VS may not have the opportunity to provide similar services. The idea should be considered of allowing commercial organizations to become certified by the VS to provide these services. They could then be allowed to perform these functions instead.

More of a good thing for Europe

European intelligence integration

In the future, intelligence operations within Europe will likely become more integrated. For some time, cooperation has been seen as a way of alleviating financial constraints. Generally considered the most evolved SIGINT system in the world is the UKUSA agreement, in which the USA, United Kingdom, as well as Australia, New Zealand and Canada each perform signals intelligence within their respective region and exchange valuable information. The launch of a satellite is prohibitively expensive for many smaller nations, leading to natural cooperation. In 1995 France launched the Helios 1A military imagery intelligence satellite with financial assistance from Italy and Spain (Nomikos, 2005 & Schmitt, 2005). All three countries are entitled to shared use of the infrastructure.

Current European Union plans to integrate intelligence are fragmented. The European Commission recently allocated 7 million euros to launch a pilot counterterrorism project. A shared facility for information and crisis management will be established, followed by a critical infrastructure protection program (European Commission, 2005). This in addition to four major intelligence centralization activities that are already ongoing (Müller-Wille, 2004):

- INTDIV, the coordinating intelligence body of the European Military Staff;
- The SATCEN, or European Union Satellite Centre was established on July 20th, 2001 and is based in Torrejon, Spain. It performs imagery analysis based on material commercially acquired or provided by member states;
- The SITCEN, or Joint Situation Centre which is composed of seven seconded analysts and issues situation and threat assessments. Its information is acquired predominantly through a number of national agencies, combined with information from European military cooperation;
- Europol, the European central police organization.

With such centralization underway, is there still a need to invest effort into Belgian intelligence? While the number of initiatives is impressive, the efforts in getting to true integration are not. There are a number of reasons for this, but mutual distrust is most likely one of the more important ones. This actually makes sense: interests of different countries within the EU may in some cases be different. An example: in 2005, France was benefactor to 27.9% of Algeria's US$ 22.53 billion imports, while Germany contributed by 6.2% (CIA, 2006). Obviously both countries would have a distinct foreign policy approach to Algeria and intelligence collection requirements would differ.

There is also a different philosophy underlying many of the intelligence services. In 1991, Pierre Marion, the head of France's GDSE announced on television that under his direction, GDSE had embarked on a program of commercial espionage (Lacayo, 1991). Other countries may limit their activities to more defensive strategies.

The recent terror attacks in the US, UK and Spain have however led to an increase in intelligence cooperation across the board. This has for example resulted in a diversity of information sharing laws in the field of aviation (European Commission, 2006).

In comparison to the past, where financial reasons were at the root of cooperation, currently skills are a dominant reason for cooperation. Belgian's VS, for one, has little to no foreign intelligence except where acquired through partner organizations. Due to its legislative framework, it is limited to gathering intelligence within the country. While this may be useful in countering some forms of terrorism, such as typical right-wing Belgian groups, it does not always apply to the types of terrorism recently experienced.

As border customs control is rare, it is now possible to enter the country from France, Germany or the UK with little to no effort and without inspection. Actual planning and organization of an attack can easily take place by foreign groups that have entered the country solely for observation purposes. Prior to conducting an attack, members may even never have entered the country. This adds to the complexity of the phenomenon and especially to how an intelligence service contained within its borders can prepare for it. Cooperation no longer is a mere luxury, it is vital to the mission of the VS.

Centralization, or at least effective distribution of intelligence material would lead to a significant increase in the quality of intelligence available to European decision makers. Each country could contribute its own specialty analysis. Belgium has a number of such unique selling propositions for its intelligence material:

Acquired versus native languages
Most intelligence services employ linguists, either to analyse information acquired from foreign sources or ethnic groups within their constituency. Review of the recruitment websites of Britain's MI5 security service and the Dutch AIVD shows a particular interest for Arabic as well as certain Indo-European languages such as Urdu and Pashto. These can be classified as *acquired languages:* not native to the service, agents fluent in them are recruited to analyse intelligence items in that specific language. Presumably, these agents are brought into specific investigations when required.

As part of its 2003 recruitment campaign, the VS encouraged those with a degree in Arabic Studies to apply (SELOR, 2003), indicating a similar school of thought. In addition, the Belgian VS has two languages which will hereafter be referred to as *native languages*, being Dutch and French. Belgium has three official languages, with Dutch (60%) and French (40%) being the most common tongues. While a wide range of Belgians are fluently bi- or even tri-lingual, upon recruitment into the VS, analysts are trained in the second language.

This is more important than it looks at first instance. Prime in intelligence are those people conducting it. While systems, procedures and technologies can support the intelligence process, in the end people are its discriminating factor. Preventing the millennium bombing at LAX was not so much a *terrorism list* of suspicious people, but the bright perception of a customs officer on the Canadian border (Burton, 2006). The question may be why some people have this insight, and some do not.

It would be outside the scope of this paper to review thinking and analysis theory, but techniques such as lateral thinking (De Bono, 1968) and inventive problem solving could help explain. A useful contribution is that "the source of a good idea is usually a combination of knowledge of the literature and practices in a subfield, specific theories and principles, common sense and the researcher's own phenomenology." (Sjöberg, 2003, p. 5). One requirement for a good idea, as such, is the exposure to many different others. There is no reason to believe this would not apply to intelligence as well.

Officers within the VS have the ability to natively assimilate and consider information – and ideas - emerging from two different language groups. One language group is predominantly

European and covers data from two highly economically active countries; the other is spoken throughout Africa, the Middle East and South-Western Europe. Exploited to its maximal potential, this allows analysts to operate more effectively than in single-language services.

Access to ethnic groups
Belgium’s colonial history led to the establishment of Sabena, its national airline. It was one of the first airlines to build a large African network. While the company folded in 2001, its successor SN Brussels Airlines maintained the busiest African routes.

With this appeared a large immigration route to the European Community. Despite the country being surrounded by other Western European countries, and as such having limited overland immigration, it quickly became host to a variety of cultures. A 2000 investigation by the federal public service in charge of employment indicated large scale naturalization of previous citizens of Morocco, Yugoslavia, Algeria, Democratic Republic of Congo, Tunisia and Poland (FOD Werkgelegenheid & Arbeidsmarkt, 2003).

Conclusion

Belgium’s intelligence services have a rich history that unfortunately in some respects tainted their image. The validity of their independent existence has recently been questioned. Due to the secrecy of the services it is often difficult to respond to such concerns. Some of the criticism may have roots in historical political feuds instead of being truly constructive. Belgian intelligence machinery was recently expanded with an all-source agency that provides improved coordination in the analysis of current threats. However, the single-source collection agencies, especially the civilian service VS suffer from significant constraints, such as the prohibition of wiretaps, that limit their effectiveness.

Financially, Belgium’s resources do not match those of neighboring countries. Nevertheless, the threat is similar to or even exceeds that of its partners. As such, Belgium would benefit significantly from increased cooperation across European intelligence services. While progress is being made, differing interests are likely to prevent complete integration in the near future. In the meanwhile, the Belgian VS should not be subjected to cosmetic ‘intelligence reform’ but should focus on changes that allow it to do more with less: efficient exploitation of open sources by improving bidirectional communication with society, improving openness and incubating a ‘will to cooperate’ amongst its constituency.

With political assistance it could also jumpstart its mission to protect the scientific and economic potential and collaborate with commercial organizations to this respect. Finally, it should cultivate its unique selling propositions to prepare for full-fledged European integration in the future and to increase its value as an intelligence partner.

References

AIVD (2005) *Annual report 2004 – General Intelligence and Security Service,* AIVD, Den Haag.

AIVD (2006) *Annual report 2005 - General Intelligence and Security Service,* AIVD, Den Haag.

Burton, F. (2006) *Beware of 'Kramer': Tradecraft and the New Jihadists.* Stratfor Premium. Stratfor Inc, Houston.

CIA (2006) Algeria. *CIA World Factbook*. URL: https://www.cia.gov/cia/publications/factbook/geos/ag.html [Accessed September 8, 2006]

Clark, M. (2004) *Intelligence Analysis: A Target-Centric Approach*. CQ Press, Washington.

Comité I (2004) *Het toezichtsonderzoek en de klacht inzake Mevr,* Soetkin Collier. Activiteitenverslag 2003, Comité I, Brussels.

Comité I (2006a). *History*. Comité I, Brussels. URL: http://www.comiteri.be/index_en.html [Accessed: September 4, 2006]

Comité I (2006b) *Toezichtsonderzoek naar de wijze waarop de veiligheid van de staat haar toezichtsopdracht t.o.v. Mevrouw F. Erdal heeft uitgevoerd,* Comité I, Brussels.

Comité I (2006c) Toezichtsonderzoek naar de wijze waarop de firma EPSI eventueel door de inlichtingendiensten werd gevolgd in het kader van de strijd tegen de proliferatie. *Activiteitenverslag 2005,* Comité I, Brussels.

De Bono, E. (1968) *The 5 day course in thinking*, Penguin Press, London.

European Commission (2005) *Commission allocates 7 million euros for a "pilot project" in the field of prevention, preparedness and response to terrorist attacks,* Media Release, European Commission, September 21, 2005. European Commission, Brussels.

European Commission (2006). *Commission Activities in the Fight against Terrorism.* Media release, European Commission, September 11, 2006. European Commission, Brussels.

FOD Justitie (1995) Wet ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en –telecommunicatie, *Belgisch Staatsblad,* Bestuur van het Belgisch Staatsblad, Brussels.

FOD Justitie (1998a) Wet houdende regeling van de inlichtingen- en veiligheidsdienst. URL: http://www.ejustice.just.fgov.be [Accessed September 13, 2006]

FOD Justitie (1998b) Historiek van het Departement. URL: http://staatsblad.be/nl_htm/organisation/info_historiek/I980006N.htm [Accessed September 8, 2006]

FOD Justitie (2003) SELOR – Selectiebureau van de federale overheid, *Belgisch Staatsblad van 12 November 2003.* Bestuur van het Belgisch Staatsblad, Brussels.

FOD Justitie (2004) Wet betreffende de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90ter van het Wetboek van strafvordering. *Belgisch Staatsblad van 24 December 2004.* Bestuur van het Belgische Staatsblad, Brussels.

FOD Justitie (2006) Wet betreffende de analyse van de dreiging. URL: http://staatsblad.be/nl_htm/organisation/info_historiek/I980006N.htm [Accessed September 12, 2006]

FOD Werkgelegenheid & Arbeidsmarkt (2003) *De Immigratie in België: Aantallen, stromen en arbeidsmarkt. Rapport 2001,* May 2003, Algemene Directie Werkgelegenheid en Arbeidsmarkt, Brussels.

Friedman, G. (2006) *The Intelligence Problem*, Stratfor Premium, Stratfor Inc, Houston.

Herremans, M. (2006). Staatsveiligheid ten prooi aan malaise, *De Standaard,* March 18, 2006, Vlaamse Uitgeversmaatschappij, Groot-Bijgaarden.

Joint Chiefs of Staff (2000) *Doctrine for Intelligence Support to Joint Operations*. Department of Defense, Washington DC.

Kamer (1997) *Wetsontwerp houdende regeling van de inlichting- en veiligheidsdiensten. Verslag namens de verenigde commissies voor de landsverdediging en voor de justitie,* October 8, 1997, Belgische kamer van volksvertegenwoordigers, Brussels.

Kamer (2004) *Beknopt verslag: Commissie voor de justitie*, Monday, July 5, 2004. Belgische Kamer van Volksvertegenwoordigers, Brussels.

Kamer (2005) *Verantwoording van de Algemene Uitgavenbegroting voor het begrotingsjaar 2006,* November 9, 2005, Belgische Kamer van Volksvertegenwoordigers, Brussels.

Lacayo, R. (1991) Intelligence: Crisis in Spooksville, *Time Magazine*, **138**(12):16, Time Inc, New York.

Müller-Wille, B. (2004) Building a European Intelligence Community in response to terrorism, *European Security Review*, **22**:3-4, April 2004. International Security Information Service, Brussels.

Nomikos, J. M. (2005) A European Union Intelligence Service for Confronting Terrorism, *International Journal of Intelligence and Counterintelligence*, **18**(2):191-203. Taylor & Francis, Philadelphia.

Schmitt, B. (2005) *Armaments cooperation in Europe*. Institute for Security Studies. URL: http://www.iss-eu.org/esdp/07-bsarms.pdf [Accessed September 20, 2006]

Segell, G. (2005) Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004. *International Journal of Intelligence and Counterintelligence*, **18**(2):221-238. Taylor & Francis, Philadelphia.

SELOR (2003) *Selectiereglement. Analisten (M/V) Veiligheid van de Staat*, SELOR, Brussels.

Senate (2006) Vast comité van toezicht op de inlichtingen- en veiligheidsdiensten (Vast Comité I). Senaat, Brussels. URL:
http://www.senate.be/nominations/comite%20I/index_nl.html [Accessed September 7, 2006]

Seront, F. (2003) Le passé néonazi de la chanteuse belge à l'Eurovision! *La Dernière Heure.* February 19, 2003. La Dernière Heure, Brussels.

Sjöberg, L. (2003) Good and not-so-good ideas in research. A tutorial in idea assessment and generation. *VEST: Journal for Science and Technology Studies*, **16**(2):33-68. Society for Vest, Oslo.

Steele, R. D. (2006) Peacekeeping Intelligence and Information Peacekeeping. *International Journal of Intelligence and Counterintelligence*, **19**(3):519-537, Taylor & Francis, Philadelphia.

Terraserver (2006). About Terraserver.com. URL: http://www.terraserver.com/aboutus/aboutus.asp [Accessed September 9, 2006]

Van Opstal (2006) Thesis: België beeft. Politieke misdrijven voor de Assisenhoven van Antwerpen en Brabant (1830-1849). URL: http://www.ethesis.net/politieke_misdrijven/politieke_misdrijven.htm [Accessed September 15, 2006]

VRT (2006a) De staatsveiligheid moet veranderen. *VRT Nieuws: Terzake*. March 9, 2006 [video recording]. VRT, Brussels.

VRT (2006b) Paars heeft Staatsveiligheid kapot gemaakt, *VRT Nieuws: De Zevende Dag*. March 5, 2006 [video recording], VRT, Brussels.

Warner, M. (2002) Wanted: A definition of “intelligence”, *Studies in Intelligence*. **46**(3):7, Center for the Study of Intelligence, Washington, DC.

Woodcock, G. (1962) *Anarchism: A History of Libertarian Ideas and Movements*, World Publishing, Cleveland, OH.