UNISCI Discussion Papers

COVERT ACTION AND ITS NECESSITY IN 21ST CENTURY COUNTER-TERRORISM

AUTHOR:[1]

GUSTAVO DÍAZ
UNISCI

KAROV MORAVE

1. The Shortcomings of Passive Intelligence

It can be said without doubt that today counter-terrorism has risen to become the greatest of priorities in terms of national security. Evidence of this is former Director of Central Intelligence (DCI) Porter J. Goss's recent testimony to the US Senate Armed Services Committee that the global war on terrorism has become today's dominant intelligence priority, with fundamental changes being made to the United States Intelligence Community to provide counter-terrorism and war-fighter support. These include the redirection of people and collection systems, as well as rapidly expanding programs, budgets, and capabilities.[2] An important element of this counter-terrorism war will inevitably be covert action (CA). Counter-terrorism though is neither a chess game against a single enemy, nor an attempt at completing a jigsaw puzzle, unless one accepts that the picture is fragmentary and dispersed, with many pieces that fit nowhere.[3] Today non-state actors with menacing intentions are also able to utilise technological developments as well as the ease in trans-national flows to their benefit. This has certainly been the case with non-state actors that adhere to ideologies of aggressive Islamic extremism. The boundaries between state and non-state security threats have also become increasingly blurred as certain states provide direct or indirect support to such terrorist entities.[4]

It can be said that intelligence in its traditional sense is information and information gathering, a passive practice; no-one gets hurt by it, at least not directly. Some nation-states though view CA as a necessary tool in national security affairs, and therefore see it as a form of intelligence. CA is a unique method for implementing national security policy, as it differs strikingly from passive intelligence, which is essentially the collection and delivery of

[1] *Las opiniones expresadas en estos artículos son propias de sus autores. Estos artículos no reflejan necesariamente la opinión de UNISCI.* The views expressed in these articles are those of the authors. These articles do not necessarily reflect the views of UNISCI.
[2] Steiner, James E.: "Restoring the Red Line Between Intelligence and Policy on Covert Action", *International Journal of Intelligence and Counterintelligence* 19 (2006), p.159
[3] "Counter-Terrorism, Information Technology and Intelligence Change", *Intelligence and National Security* 18, No. 4 (Winter 2003), p. 43. Published in Security Monitor (London: RUSI 2002).
[4] Mandel, *Deadly Transfers and the Global Playground: Translational Security Threats in a Disorderly World,* p. 77.

analyzed information to those formulating and implementing policy. In sum, CA is all about making things happen, while intelligence in its traditional sense consists of making the right decisions about what may happen.[5] CA covers a broad range of diverse activities, from propaganda and subversion to the training and funding of foreign intelligence and security services. The activities themselves are not necessarily secret or clandestine, but the role of the nation-state engaged in such activities must be disguised so as to provide for plausible deniability. This separates CA from diplomacy and the use of conventional military force, as covert action is employed when a country seeks to accomplish a national security goal without its involvement being recognised. CA actions also inevitably raise moral and ethical issues for nation-states in their conduct of foreign and domestic policy.[6] To truly understand the meaning of covert action for democracies though, one must first look at its various uses in the past.

2. Covert Action and Democracies

For many observers, and especially for critics, secret intervention is synonymous with intelligence and loomed large in Cold War debates about the legitimacy and morality of intelligence organisations and their activities. Since September 11, Washington's agenda for taking the offensive to the United States' enemies has rekindled such arguments. The shock of mass violence witnessed in 9/11 has forced a shift towards this new thinking, as the US had previously been content with a reactive approach to terrorism. It was believed that the terrorists that carried out the 9/11 atrocities belonged to a new generation of terrorism, far more insidious, owing mainly to technological empowerment. Active approaches to such a threat would no longer suffice. CA was seen as an essential element of this active approach. Though it has been this new approach by the US that has re-invigorated discussions on CA, the topic of CA in general is not limited to the US alone. It must be noted that the conceptions of CA can markedly differ between nation-states, particularly those that are democratic and non-democratic, but in this instance the focus will be placed on the meaning of CA for the US, as it is the nation-state most threatened by modern Islamist terrorism. To truly get an understanding of what CA really means for the US, one must first explore in depth the various uses and understandings of it through recent history. Only after this has been done can an analysis of the role of CA be made within the broader realm of intelligence and security affairs.

The more prominent definitions of CA are predominantly American, dating back to the celebrated 1948 National Security directive 10/2 which authorised the CIA to engage in: propaganda, economic warfare, preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures, subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-Communist elements in threatened countries of the free world. More recent US government statements cover most of these activities though some of the language has altered (notably the demise of 'subversion'). In US law CA became defined as: 'an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the government will not be apparent or acknowledged publicly, but does not include… traditional counter-intelligence…

[5] Steiner, *op. cit.,* p. 163.
[6] Herman Michael: "Ethics and Intelligence after September 2001", *Intelligence and National Security* 19, No. 2 (Summer 2004), p. 350.

diplomatic… military… (or) law enforcement activities'.[7] One commonly accepted aspect of these definitions is that they refer to actions abroad.

We know about CA in the same way that we learn about other intelligence activities, through authorised and unauthorised disclosure: memoirs, journalism, defectors, archives, whistle-blowers and judicial investigation. The veracity and integrity of these sources may differ, though there are generic questions to be posed about the agendas and intentions of those who provide us with information about CA.[8] One question is whether we know more about CA than intelligence gathering and analysis. A second is whether we know more about certain kinds of CA than others, especially the more dramatic. Some covert operations have been easier to discover because they failed. For many governments the concept of plausible deniability has been integral to the activity, therefore one must consider the possibility that we may be learning more about unsuccessful operations than successful ones, and that when we are learning of secret interventions from unreliable sources, we may in fact be the target of disinformation or propaganda

A lack of transparency in these types of operations makes democratic accountability difficult, and correspondingly affects the level of public support and consent for such ventures. Citizens expect that intelligence sector activities will protect and support liberal democracy rather than undermine it. Although secrecy is a necessary condition of the work, intelligence professionals are expected by the national citizenry to be accountable, act in the public interest, and in conformance with a society's moral values. Lacking a direct means to confirm that this is so, the public tends to suspect that what is secret must be perverse. This is especially true in the case of foreign intelligence collection and CA, where the purpose and moral criteria for specific activities is poorly understood and rarely articulated. Democratic government in theory is expected to rest on openness and participation, rule of law, privacy, and mutual trust, conditions with which the requirements and practices of intelligence are often at variance. Nevertheless, an explicit statement of the ethical principles that guide decisions in intelligence 'monopolies' could help to enhance public trust in the work of intelligence services. This is especially important following the findings of the Hutton and Butler Reports in the United Kingdom; the Joint Congressional Inquiry in the United States; and the Flood Commission in Australia, over the role of intelligence in the Allied decision to intervene militarily in Iraq in 2003.[9] Security, the state's obligation to defend its territorial integrity and the freedoms and safety of its citizens, was claimed to be such an absolute value by President Bush following the events of 11 September 2001. In such a setting, new balances will have to be struck between extended intelligence coverage on the one hand, and citizens´

[7] Intelligence Authorization Act, Fiscal Year 1991, P.L. 102–88, 14 August 1991; Shulsky, Abram (1993), *Silent Warfare: Understanding the World of Intelligence,* London, Brassey's, p. 84. The CIA's definition is: 'An operation designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the sponsoring power; it may include political, economic, propaganda, or paramilitary activities.' CIA (1995): *CIA, Consumer's Guide to Intelligence,* Washington DC, CIA, p. 38, quoted in Rudgers, David: 'The Origins of CA', *Journal of Contemporary History* 35, No. 2 (2000), p. 249.

[8] Scott, Len: "Secret Intelligence, CA and Clandestine Diplomacy", *Intelligence and National Security* 19, No. 2 (Summer 2004) p. 322.

[9] United States. Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001. *Report of the U.S. House Permanent Select Committee on Intelligence and the US Senate Select Committee on Intelligence*, (December 2002). Senate–House Report No. 107–792, Report No. 107–351. Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, 20 July 2004. The Rt. Hon. The Lord Butler of Brockwell, *Review of Intelligence on Weapons of Mass Destruction, House of Commons 898*, 14 July 2004. Lord Hutton, *Report of the Inquiry into the Circumstances Surrounding the Death of Dr. David Kelly CMG, House of Commons*, 28 January 2004.

privacy on the other. Governments and their citizens will therefore have to decide what, if any, sacrifices must be made for the sake of security from terrorist threats.

3. Old Lessons and New Challenges

CA today faces new challenges which can only be dealt with after first comprehending the relevant lessons of history. The role of CA in the international context is undoubtedly a crucial one. It has been used with regularity in recent history, yet not all of these operations are publicly known. Nevertheless, the numerous openly known successful and unsuccessful CA operations conducted particularly during the Cold War, provide an excellent analytical treasure trove for the understanding of CA in the international setting. The very fact that details of CA operations have been leaked also poses challenges to the conduct of similar operations for the present day. The information age has made the conditions for plausible deniability, an essential element of CA, an even more difficult endeavour for governments engaged in the use of such operations. These realities force governments as well as intelligence and security establishments to acknowledge that absolute secrecy and total information control may well be an impossible task. Operating within such an environment forces governments to conduct CA with greater sensitivity to the electorate, as the national citizenry are more likely to become aware of such actions, through unauthorised leaks. In the past governments believed that secret operations would remain exactly that, secret, or at the very least not leaked whilst they were in power, thereby allowing them to place less of an emphasis on the potential public reaction to the unveiling of CA operations. This new heightened level of sensitivity to the public, limits governments in their selection of CA options, which, depending upon various factors, can be potentially advantageous or disadvantageous to national security interests. Only when these broader CA lessons and challenges are understood can its use in a counter-terrorism context then be analysed. Counter-terrorism has without doubt, in parallel to the threat of Islamist terrorism, risen to the top of the intelligence and security agenda of national governments, and it is essential that CA evolves from its Cold War form into an asset that can be invaluable in the counter-terrorism wars of the 21st century.

The main emphasis of studies on CA has often been on intelligence's observable international effects; in crude terms, whether it has been good or bad for international society, using the commonsense yardsticks of whether it has promoted or discouraged responsible government behaviour, good inter-state relationships, the minimisation of tension, co-operation for internationally valuable purposes, and the avoidance of war. At the height of the Cold War CA was justified by the US as a quiet option and as a tool for fighting the Soviet Union in the absence of conventional military combat, to be used where diplomacy was insufficient and force was inappropriate. Enveloped in secrecy, few Americans were aware of most CA programs; one prominent example being that Washington's role in supporting Afghan fighters against the Soviet Union was not unveiled until well after combat ended. For critics of such operations, Western CA undermined the legitimacy of Western (especially US) intelligence if not indeed Western foreign policy (particularly US) during the Cold War. For the supporters of such activities, CA represented (usually) discreet forms of intervention that obviated more violent methods. The US in particular has always considered CA a useful adjunct to military force during wartime, yet the various instances of failure in such operations have resulted in negative consequences.

The list of unsuccessful CA activities**,** which has altered both public and bureaucratic perceptions on the wisdom of CA, is unfortunately long. Despite an embarrassing failure in a paramilitary operation in Indonesia in 1958 and the 1961 Bay of Pigs fiasco, the CIA's CA capability remained relatively free from exposure troubles until 1967, when a series of articles by Ramparts magazine exposed a major portion of the CIA's CA assets; the cultural and propaganda resources around the Congress for Cultural Freedom, including media outlets such as the London-based Encounter magazine and Forum World Features Service, and youth and student activities involving the US National Student Association and the World Assembly of Youth. These exposés were quickly followed by an 'outing' of Radio Free Europe, Radio Liberty, and the Free Europe Foundation as CIA-controlled assets. As a result, Congress removed Radio Free Europe and Radio Liberty from CIA's control in 1972 and funded it overtly, establishing a Board of International Broadcasting (later changed to the Broadcasting Board of Governors). The 1980s and 1990s saw even more disclosures of CA operations. Major paramilitary operations such as those in Angola, Nicaragua, and Afghanistan were impossible to keep secret. Indeed, Congress insisted on debating such 'covert' assistance in open sessions. Bob Woodward's book, Veil: The Secret Wars of the CIA, published in 1987, disclosed dozens of previously unpublicised or little publicised CA operations during the presidency of Ronald Reagan.[10] Professors Ernest May and Roy Godson, both esteemed intelligence scholars, spoke for many when they concluded that keeping CA operations secret was almost impossible, given the current rulebook.[11]

The issue of secrecy in CA is an essential one, as plausible deniability can be listed as one of the core element for such operations, but it is now arguably harder than ever for governments anywhere to keep secrets for long; most of such secrets leak out sooner or later.[12] In the years after the Cold War ended, commentators could argue that in an increasingly open world, intelligence's emphasis would shift away from collection and towards analysis, and that there would be more emphasis on 'intelligence-as-information', drawing on more open source material, and less on 'intelligence-as-secrets'.[13] In fact, some have argued that CA secrecy is a thing of the past.[14] Total operations security in the information age is made increasingly difficult, as a vast multitude of sources exist through which classified material can be anonymously leaked. Furthermore, no amount of vetting and counterintelligence will guarantee that such leaks will be absolutely prevented, though they can be reduced if such actions are implemented appropriately. Though intelligence and security organisations can take measures to reduce the volume of leaks, it would be unrealistic to expect that details of all CA operations will remain secret until appropriately declassified. Evidence of this is that articles and books on a long list of identified CA operations, sometimes complete with CIA codenames, have appeared in the news media. Major daily newspapers such as The Washington Post, The Washington Times, The New York Times, and The Los Angeles Times all have reporters who specialise in covering the intelligence community, and regularly report on CIA activities. There is therefore no reason to believe that the current President or his successors will eschew what both former Secretary of State Henry A. Kissinger and CA specialist, the late Theodore Shackley, termed 'the middle option', even

[10] Woodward, Bob (1988): *Veil: The Secret Wars of the CIA, 1981–1987,* New York, Pocket Books.
[11] Godson, Roy; Kerr, Richard and May, Ernest: (1992) *CA in the 1990s*, Working Group on Intelligence Reform, Washington, D.C.
[12] Herman, Michael: "Ethics and Intelligence after September 2001", *Intelligence and National Security* 19, No.2, (Summer 2004), p. 350.
[13] Hurrell Andrew: "There Are No Rules (George W. Bush), International Order after September 11", *International Relations* 16, (August 2002).
[14] Wettering L. Frederick, "[C]overt Action: The Disappearing 'C'", *International Journal of Intelligence and Counter-Intelligence* 16 (2003), p. 562.

if some instances of CA are now essentially 'overt-CA'.[15] This new reality will inevitably have far-reaching consequences for the conduct of CA in a counter-terrorism context.

As the United States and its allies consider themselves in semi-perpetual war against terrorism, and preventive action in counter-proliferation and counter-terrorism (in overt and covert policy) becomes increasingly prevalent, the implications for CA will be profound. The United States' current mood shows little aversion to using force, and overt action is less constrained by domestic opposition or international restraint. The major role played by American CA forces in the global war on terrorism is both huge and public. In the Cold War, intelligence was helping governments to avoid war; now it is actively involved in fighting one, seeking to save lives and defend national security in the most literal sense, in an asymmetrical contest whose nature gives it a special importance. Whatever reservations were expressed about the US declaration of a 'war on terrorism', the wartime metaphor fits intelligence's current status rather well. As a result of this reality, intelligence budgets are increasing everywhere, and hardly a day passes by without its appearance in the news.[16] It is important to note though, that despite being an intelligence superpower, the United States cannot meet all its counter-terrorist requirements by itself. Almost every nation is able to supply some unique intelligence on global terrorism, from local records and local human and technical sources. The United States accordingly developed a set of new or deeper counter-terrorist relationships, and Britain followed suit. The main change has been the dramatic increase in intelligence's own importance after September 11, 2001. A trend in that direction had begun earlier; after intelligence budgets had been reduced as part of the peace dividend at the end of the Cold War, they were already being restored to cope not only with terrorism but also with the requirements of the 1990s for support of multi-lateral and international peace enforcement and humanitarian operations, and for intelligence on WMD proliferation, sanctions evasion, drug trafficking and the other emerging targets of the decade. Governments were already adapting themselves to what seemed an increasingly unstable world, and to the information revolution within it, both in relation to the information available and in governments' ability to collect and process it. Intelligence as a whole was growing again and was no longer quite such a deniable activity. Nevertheless, before September 11, it was still not seen as a defence against an overarching and common threat. International terrorism and other threats in the 90s were still seen as peripheral ones, slightly remote, though this has now undoubtedly changed.

The nation-states that are now threatened by global terrorism have a mutual interest in cooperating with each other. The problems of counter-terrorist intelligence cannot simply be eliminated through financial means. The success of counter-terrorism depends on a new level of intelligence cooperation, in effect the creation of a new international counter-terrorist intelligence community.[17] For instance, in the realm of human intelligence there are severe limits to what larger nation-states can do to expand their own collection, but such capabilities can be improved by developing better liaisons with foreign intelligence services. Similar considerations apply to some technical sources, but effective intelligence liaison relations require the right form of political support. It must be noted though that the greater the number of countries that are involved with CA, the greater the likelihood of classified details being

[15] Wettering, *op. cit.,* p. 570.
[16] Herman, Michael: "Ethics and Intelligence after September 2001", *Intelligence and National Security* 19, No. 2 (Summer 2004), p. 347.
[17] Herman, Michael (2001), *Intelligence Services in the Information Age,* London, Frank Cass, p. 230.

leaked. In addition, intelligence will also need new approaches in meeting terrorist threats, as the old structures of the cold war are today ill-adapted for this new kind of war.[18]

The 'offensive hunt' strategy that will be necessary for 21st Century intelligence, will involve methods which were not the norm prior to September 11, 2001. This new approach to counter-terrorism will involve not only hunting down and, if need be, killing terrorists but also, where necessary, ignoring local sensitivities and the operating rules of local intelligence and security services. Recent actions in locations such as Afghanistan, Pakistan and Europe are examples of this new strategy or offensive hunt, where CA will be a fundamental part of intelligence activities.[19] The magnitude of the global terrorist threat requires in response such new, aggressive and unorthodox tactics.[20] As the commission on the 9-11 terror attacks pointed out, for the US in particular, CA has been and will be a fundamental tool for its intelligence and security agencies in combating terrorism.[21] Furthermore, this new offensive approach will require radical steps in changing internal security structures, as in the absence of such changes the US, as well as other nation-states, will continue to remain vulnerable to further attacks against their interests.[22]

4. The Information Age Terrorist

The terrorist attacks of 11 September 2001 have given rise to what can almost be called a tidal wave of literature trying to understand the surprise attack on the American mainland. In lethality terms alone, the September 11 attacks were without precedent.[23] It not only showed a level of patience and detailed planning rarely seen among other terrorist movements, but the hijackers stunned the world with their determination to kill themselves as well as their victims. Suicide attacks differ from other terrorist operations precisely because the perpetrator's own death is a requirement for the attack's success.[24] Catastrophic terrorism, as that committed on 9/11, like wars, may accelerate dangerous economic, political, and social change. Terrorist organisations such as Al-Qaeda also embrace far more amorphous religious aims and wrap themselves in less-cohesive organizational entities, with a more-diffuse structure and membership. In addition, they use amateurs to a far greater extent than in the past. These organisations are inspired by religion and their members are seen as religious fanatics, seeking weapons of mass destruction to kill as many people as possible, with their victims selected indiscriminately. Contrary to popular belief suicide terrorists are also not exclusively derived from the ranks of the mentally unstable, economically bereft, or abject, isolated loners.[25] Finally, it would be wise not to overestimate, as some have, the degree to

[18] Herman, Michael: "Counter-Terrorism, Information Technology and Intelligence Change", *Intelligence &National Security* 18, No.4 (Winter 2003), p. 42.
[19] Cogan Charles, "Hunters not Gatherers: Intelligence in the 21st Century", *Intelligence and National Security* 18, No. 2 (Summer 2004), p. 316.
[20] Akin, William: "The Secret War", *Los Angeles Times*, 27 October 2002.
[21] Commission on the 9-11 terror attacks, Intelligence Policy, Staff Statement No.7. "In Mach 2001, National Security Adviser Rice tasked DCI George Tenet to draw up a new document on CA authorities for Afghanistan".
[22] Cogan, Charles: "Hunters not Gatherers: Intelligence in the 21st Century", *Intelligence and National Security* 18, No. 2 (Summer 2004), p. 319.
[23] Hoffman, Bruce: "Rethinking Terrorism and Counter-terrorism Since 9/11", *Studies in Conflict & Terrorism,* 25 (2002), p. 303.
[24] Schweitzer, Yoram: "Suicide Terrorism: Development and Main Characteristics," *The International Policy Institute for Counter-Terrorism at the Interdisciplinary Centre Herzliya*, Countering Suicide Terrorism: An International Conference, Jerusalem and Hewlett (2001), pp. 76.
[25] Hoffman, *op. cit.,* p. 305.

which puritanical organisations such as Al Qaeda are at the same time 'modern' and comfortable with 'modern methods'.[26]

In the late 20th century the lethality of terrorist attacks gradually increased as terrorists motivated by ethnic hatreds or religious fanaticism revealed themselves to be demonstrably less constrained and more inclined to carry-out large scale indiscriminate attacks. A number of reasons account for terrorism's increased lethality. The overall rise during the past 20 years of terrorism motivated by a religious imperative, encapsulates the confluence of new adversaries, motivations and tactics affecting terrorism patterns today. Religion is today a significant force behind terrorism's escalating lethality, and the proliferation of amateurs taking part in terrorist acts has also contributed to terrorism's increasing lethality. Though Religion and fanaticism are said to be the main motivators for the terrorists of today, earlier forms of terrorism can also be characterised by political motivations, such as nationalism and extreme left-wing ideologies that were in fact religious in nature. The IRA for example, had an almost exclusive Catholic membership.[27] In fact the nexus between religious motivation and violence is reflected in the fact that while previous secular, nationalist terrorist organizations understood that 'wanton violence' could be politically counter-productive[28], the apocalyptic world-views of the religiously motivated terrorist hamper the articulation of a plausible political agenda, and this contributes to an absence of constrained violence.[29]

Terrorists have also profited from past experiences and have become more adept at killing. Not only are their weapons becoming smaller, more sophisticated and deadlier, but terrorists may also have greater access to these weapons through their alliances with various states. Such acts of violence have become accessible to anyone with a grievance, an agenda, a purpose, or a combination of all the above. It is important to note though that with the growth of amateurs engaged in such operations, the sophistication and operational competence of terrorists is also increasing, as the new generation of terrorist learns from its predecessors, becoming smarter, tougher and more difficult to eliminate. The actions and weapons of this new form of terrorism aims to inflict as much damage as possible by killing many innocents civilians, but it should be asked whether the terrorists have in fact changed or whether the world in which they operate has altered. The reality seems to point to a change in both the terrorist and the surrounding environment, since when the means become available, terrorist violence will also inevitably become more extreme. It is also true that the number of terrorist victims has been on the rise for at least two decades, which does not overlap with the rise of this new generation of terrorism. In that sense, the use of weapons of mass destruction is not an inherent feature of this new form of terrorism and certainly does not constitute a trend. An important lesson here is not to disregard an adversary's apparent lack of technological or operational sophistication and thereby be lulled into a false sense of security. The sophistication of terrorist weapons will continue to be in their simplicity, and as a result it will be almost impossible to protect all possible targets, and to deter terrorists completely, as any security hurdles placed in their path will not stop them from striking, but likely only displace the threat onto softer targets. The populations and governments of Western countries are particularly vulnerable to this new generation of terrorism, as they rely almost entirely on national critical information structures (NCII) consisting of government and corporate computer servers, telecommunications facilities and Internet services provides. Terrorists will continue to use what they know will work, but the possible combination of terror and WMD

[26] Tan, Andrew and Ramakrishna, Kumar (2002): *The New Terrorism*, Eastern Universities Press, p. 4.
[27] Duyvesteyn Isabelle, "How new is the new terrorism", *Studies in Conflict & Terrorism* 27, (2004) p. 443.
[28] Meter, Berger L.: "Picking Up the Pieces: What can we learn from- and about 9/11", *Foreign Affairs* 81, No. 2 (March-April 2002), p. 172.
[29] Simon, Steven and Benjamin, Daniel: "The Terror", *Survival* 43, No. 4 (Winter 2002), p. 5.

will continue the greatest worry for national security services for many more years to come. Today's terrorist though continues to use predominantly the same weaponry as the traditional terrorist. The increased lethality of terrorists can also be explained not only by a gradual increase in the effectiveness of the means in today's world, but more importantly by the inherent necessity in terrorist actions to strike harder to achieve the same required effects. There appears to be a pattern that suggests that at least some terrorists have come to believe that public and government attention is no longer as readily obtained as it once was. To their minds, both the public and media have become increasingly inured or desensitized to the continuing spiral of terrorist violence, therefore they justify increased lethality to achieve effects similar to or greater than those in the past. The terrorist continues to require the media as a spectator, as the immediate effect that is still aimed for in nearly all terrorist attacks is geared towards achieving maximum surprise and publicity.

Terrorism today also displays both signs of change and continuity. New adversaries with new motivations and new rationales have appeared in recent years to challenge some of the most basic assumptions about terrorists and terrorism.[30] Particularly, the pyramidal, hierarchical, organisational structures that were dominant among terrorist organizations during the 1970s and 1980s have been put aside for far more amorphous, indistinct, and broader movements.[31] The networked nature of terrorist organisations such as Al Qaeda can be largely attributed to the revolution in computing, telecommunications, and data transference capabilities, commonly referred to as the information revolution. It is fundamentally an asymmetric method through which a weaker actor seeks to obtain its ends by breaking the will of a stronger power. It is also commonly regarded that terrorism organisations are Darwinian in that they tend to learn from their predecessors. They are thus evolutionary in character and are ever mutating in order to adapt to the changing security landscape.[32] Terrorist networks have been shown to incur seventy percent attrition rates and still maintain operational capabilities. Decentralized command structures also make difficult the strategic targeting of networks, because classical military thought assumes that 'hostile will' resides not in the population at large but in the leadership.[33] Particularly problematic is the fact that Islamist terrorist organisations such as Al Qaeda have no lack of sympathetic supporters in whom succour might be found. Regardless of the loss of its professional cadre, such organisations have an abundance of amateurs, walk-ins, and sympathetic organisations form which to pull human, monetary, and ideological resources. Islamist terrorist movements in particular are today also seen to have less easily defined aims or identified objectives; some are motivated by unswerving hostility toward the West in general and the United States in particular or a desire for revenge and retaliation that is frequently fuelled by compelling religious imperatives and justifications rather than abstract political ideologies. A distinction should also be drawn between the short-term and long-term goals of terrorism. Short-term goals, to the terrorists, seem highly attainable, that is, provocation, publicity, and hurting the enemy. Long term goals are often less clear and their achievability is often judged to be unrealistic by all but the terrorists. Given this mixed picture of terrorist patterns and trends and the inherent uncertainty in attempting to predict future terrorist behaviour, what can or should be done to counter effectively the terrorist threats of today and the future?

[30] Hoffman, Bruce: "Change and Continuity in Terrorism", *Studies in Conflict & Terrorism* 24 (2001), p. 420.
[31] *Op. cit.,* p. 417.
[32] Hoffman, Inside Terrorism, *op. cit.,* p. 179.
[33] Szafranski, Richard: "A Theory of Information in Warfare", *Airpower Journal* (Spring 1995), p. 2.

5. Opening the CA Toolbox

CA by its very nature is a most valuable tool in the exercise of intelligence warfare. The multitude of weapons available, varying within various thresholds of risk, if wisely used in an integrated manner, can greatly increase the likelihood of success in meeting intelligence and policy objectives. It is for this reason that the most sophisticated of global intelligence and security organisations have used and continue to use its potential powers within the context of a nation-state's foreign policy. Whilst CA has always remained a controversial practice within the realm of international affairs, it continues to be used with great frequency.[34] In an international legal sense the lines of demarcation between acceptable and unacceptable intervention can be hazy, as texts approved by the United Nations on the use of CA represent compromise formulations that are open to multiple interpretations.[35] Crucially, the lines of demarcation between legal an illegal CA must be made as clear as possible within intelligence and security apparatuses, so as to prevent confusion or disarray in determining the planning or authorisation of such activities. Many of the tools of CA discussed here (Psychological warfare, information warfare, political CA, economic CA and paramilitary activities) have been used from the dawn of warfare, although in a less sophisticated manner than is attainable today. Indeed Sun Tzu's 'Art of War' dedicates an entire section to 'The Use of Spies', expounding their value in deception and assassination operations. However, to measurably increase its likelihood of success, the tools of CA must be used in a coordinated manner; this would be greatly facilitated by ensuring the existence of a CA centre in which national CA capabilities of a nation-state can be used effectively.[36] On an international level the creation of joint CA centres may also be worth taking into consideration, for the purposes of utilising the CA capabilities of allied nation-states. Additionally, it must be understood that whilst CA is essentially an offensive form of intelligence, it is the defensive side of intelligence (collection and analysis) that will ultimately determine whether CA operations will be successful or not. It is this form of intelligence that establishes when and how CA should be used for particular targets, as well as aiding in the understanding of its short and long-term impacts. While mistakes and misjudgements will continue to occur as long as human beings remain fallible, governments contemplating covert intervention ought at a minimum, to know enough about the culture and values of a target to make informed judgments about its politics and history, thus being able to calculate the likely consequences of the kinds of intervention contemplated.[37] This level of understanding requires greater attention by decision makers to the recommendations of intelligence analysts, covert-action specialists and outside academic experts.

5.1. Psychological Warfare

Perhaps the most valuable of tools in the war against the terrorist adversary is psychological warfare (PSYWAR). PSYWAR or strategic psychological operations (PSYOP) can be most accurately described by using the US Department of Defense's definition: 'The planned use of propaganda and other psychological actions having the primary purpose of influencing the

[34] Reiter, Dan (2002), *Democracies at War*, Princeton, Princeton University Press, pp. 162.
[35] Lock K. Johnson, "On Drawing a Bright Line for Covert Operations", *American Journal of International Law*, Vol. 86 (1992), pp. 287.
[36] Hulnick, Arthur S. (1999): *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*. Westport, Praeger, p. 83.
[37] Beitz, Charles R.: "Covert Intervention as a Moral Problem", *Ethics and International Affairs*, Vol. 3 (1989), p. 49.

opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives.'[38]

Propaganda can be set into four basic categories: conversionary propaganda, which aims at changing the emotional or practical allegiance of individuals from one group to another; divisive propaganda, which is designed to separate component subgroups of the target population; consolidation propaganda, which is directed toward civilian populations in areas occupied by an armed force and strives to ensure compliance with the policies of the occupying force; and counterpropaganda, which refutes specific points or themes of the enemy's propaganda.[39]

To increase the probable desire outcomes of PSYOP, intelligence collection and analysis, or defensive intelligence, must first succeed in gathering as much intelligence as possible on the terrorist targets or 'audience' and the environments in which they operate. Only when this has been done can appropriate PSYOP be developed in response to a threat. This then crucially allows for each audience group for PSYOP to be addressed in terms appropriate to its situation. It is also at this point that a combination of the four aforementioned propaganda categories can be utilised.

A) Conversionary Propaganda

When dealing with a terrorist adversary that holds deeply rooted ideological beliefs, one is highly unlikely to convert such targets entirely away from their convictions, as one cannot effectively attack with logic that which is not logical.[40] A more appropriate response would be the development of PSYOP that influences moderation in a terrorist, with a minimum aim of getting the target to abandon violence in the pursuit of its goals. In dealing with members of Islamist terrorist organisations, Britain's Secret Intelligence Service (SIS) has pursued such an approach. In 2005, public knowledge of plans by SIS officers to pose as 'moderate' Islamists online, forced the Foreign and Commonwealth Office to publicly to publicly deny the further pursuit of such PSYOP.[41]

Preventing individuals from becoming terrorists in the first place is a far more complex affair, involving sociological and economic developments that would move beyond the scope of this paper. Nonetheless, dismantling the breeding grounds of terrorism should be seen as an issue of utmost importance, as a greater number of terrorists will inevitably further complicate intelligence and security matters.

B) Divisive Propaganda

In instances where there may exist a number of loosely allied terrorist organisations, divisive propaganda can be utilised to create and further develop fractures between such entities. If

[38] Joint Chiefs of Staff: "Doctrine for Joint Psychological Operations", *Joint Publication 3-53*, 5 September 2003.
[39] Gilmore, Allison B. (1998), *Psychological Warfare against the Japanese Army in the Southwest Pacific*. Lincoln, University of Nebraska Press, p. 100.
[40] Lerner, Daniel (1949): *Sykewar: Psychological Warfare against Germany, D-Day to VE-Day*. New York, George W. Stewart, p. 173.
[41] Bright, Martin: "MI6 plan to infiltrate extremists", *The Observer*, 4 September 2005.

successful such PSYOP strategies can weaken alliances, and thus the overall threat posed by it.[42] Furthermore, differences can be encouraged to such an extent that terrorist organisations begin to turn against one another. The problems associated with such a strategy lie in the possibility that the ultimate victors of such an internal war may pose a greater overall threat due to its homogenous nature. In addition, such divisive propaganda may not be favourable in instances where warring terrorist factions and their use of violence could heavily undermine national security and overall policy objectives to a greater extent than if they had peacefully coexisted with one another.

C) Consolidation Propaganda

Consolidation propaganda in its use against terrorism can dissuade terrorists by emphasising the negative consequences of pursuing such a course of action. The overwhelming potential force and powers of government resources can force adversaries into doubting the likelihood of success in facing a far superior opponent. By sowing such doubt into the minds of terrorist adversaries one increases the likelihood of terrorist organisations curbing or reducing their own plans and activities, as terrorists and their sympathisers are more likely to be ripe for absorbing new ideas if the futility of fighting on can be made more apparent.[43] Similar PSYOP strategies can be used to decrease the likelihood of terrorist sympathisers and deter the possibility of aid being given by such persons to terrorists and their organisations. In addition, the effective exploitation of dissensions between terrorists and probable recruits from a population can substantially weaken terrorist entities.[44]

D) Counterpropaganda

Crucial to discrediting terrorist adversaries is to refute through PSYOP all propaganda emanating from such entities. It will ultimately be the targets of such terrorist propaganda that must be targeted by such PSYOP, as this will directly aim to reduce the likelihood of sympathy for terrorists and their cause. The cover for such PSYOP must also be sourced in a form that will deflect prejudices that the target audience may hold. Counterpropaganda plans must also be considered with caution as merely recognising and contradicting terrorist propaganda may in fact provide further publicity for the ideas. Negating or ignoring terrorist propaganda with a positive line of propaganda may be of greater value under such circumstances.[45]

5.2. Deception

Deception, as a form of CA, can be used within the realm of PSYWAR and outside of it. Deception aims to deliberately induce misperception in another. Deception is a deliberate

[42] Davies, Philip H. (2004): *MI6 and the Machinery of Spying*, London, Frank Cass, p. 298.
[43] Lerner, Daniel, (1949): *Sykewar: Psychological Warfare against Germany, D-Day to VE-Day*. New York, George W. Stewart, p. 174.
[44] Taylor, Philip M. (1997), *Global Communications, International Affairs and the Media since 1945,* London, Routledge, p. 82.
[45] Leeman, Richard W. (1991): *The Rhetoric of Terrorism and Counter-Terrorism*. New York, Greenwood Press, p. 111.

enterprise; it is not the result of chance, nor the by-product of another endeavour. Deception can be defined as information designed to manipulate the behaviour of others by inducing them to accept a false or distorted presentation of their environment - physical, social, or political.[46] In its use against terrorism deception can be used to manipulate the thought processes of terrorists leading to misperceptions that can impede or curb their activities.

5.3. Information Warfare

The increasing use of advance technology by terrorist adversaries provides opportunities for information operations (IO) to be used in countering its potential benefits. IO can be described as the integrated employment of electronic warfare, computer network operations, PSYOP, deception and operations security.[47] Exploiting weaknesses in terrorist information structures ensures that terrorist recruitment planning and operational activities are all negatively affected. In such IO operations assessments will have to be made so as to ensure that the benefits of sabotaging a target will outweigh the benefits of any valuable information that could be gathered by allowing its continued operation. Deciding between continued surveillance or termination of a target is often a difficulty in intelligence and security matters, as the pursuit of intelligence through surveillance may result in points of no return being crossed that strengthen terrorist adversaries and their likelihood of carrying out an attack. Nonetheless, such critical decisions will also have to be made in the context of IO.

5.4. Political CA

Political CA can be used for the same purposes as those possible for PSYOP. Through recruited agents or non-official cover (NOC) intelligence officers that have infiltrated terrorist organisations, discord can be created within or between terrorist organisations so as to impede their activities.[48] Creating or actively supporting existing entities that pursue moderate and peaceful forms of broader terrorist goals can also hinder the growth and strength of terrorist adversaries. In addition, it is vital that where necessary, financial and logistical support be given to the intelligence and security apparatuses of allied nation-states involved in combating terrorism.

5.5. Economic CA

Economic CA will also have to be used in conjunction with political CA in order to finance moderate and counter-extremist ideologies. In order to avoid existing negative prejudices, the cover for such financing may have to be developed so as to be seen as a favourable and acceptable resource, thereby protecting and enhancing the overall position of the financial receiver.[49] For the purposes of obstructing terrorist financing, the financial activities of financiers and terrorists must be aggressively pursued and identified so as to be frozen and

[46] Gerwehr, Scott and Glenn, Russell W. (2000): *The Art of Darkness: Deception and Urban Operations*. Santa Monica, RAND, p. 15.
[47] Joint Chiefs of Staff: "Information Operations", *Joint Publication 3-13,* 13 February 2006.
[48] Marks, Ron: "Keep an Eye on the Ball; Intelligence Director Faces Certain Challenges", *The Washington Times*, 17 August 2004
[49] Marchetti, Victor and Marks, John D. (1974): *The CIA and the Cult of Intelligence*. New York, Dell, p. 72.

shut down when necessary.[50] Furthermore, for the intention of developing mistrust and discord within terrorist networks, capital from accounts can be partially seized.

5.6. Targeted Killings (Paramilitary Activities)

The targeted killing of key terrorist targets, despite being the most controversial of all CA possibilities, is nevertheless given serious consideration by some modern democracies within the context of counter-terrorism. When apprehending a high profile terrorist is made operationally problematic and the individual's existence strengthens the likelihood of an attack, for security purposes there remains few choices but to take into serious consideration the possibility of using a targeted killing to eliminate the relevant terrorist. Modern democracies have been highly sensitive to such courses of action, therefore it can be said that a greater effort by governments seeking to use such CA activities must be made to put forth the arguments in support of them. In addition, governments must emphasise that targeted killings will only be used as a weapon of last resort and only when sufficient evidence exists for such operations to proceed. Modern democracies such as the US and Israel have been known to carry out such methods of CA in the context of counter-terrorism. Most recently, the US's Central Intelligence Agency (CIA) has been actively utilising unmanned airborne systems (UAS) for the assassination of Islamist terrorists. In 2002 six suspected members of the al-Qaeda network were killed by a Hellfire missile fired from an RQ-1 Predator drone in Yemen.[51] Israel pursued a policy of assassinations soon after the 1972 Munich Olympic massacre to send a message not only to those who participated in the Munich massacre, but also to those considering future terrorist attacks. In order to carry out this task, Mossad activated its assassination unit, known as the kidon - Hebrew for 'bayonet.' Kidon teams have been responsible for a number of high profile assassinations, including Dr. Gerald Bull, designer of the Iraqi supergun, and Nasser Issa, also known as 'The Engineer', a master bomb-maker for Hamas.[52] The 'Wrath of God' operation, as it was called, had been successful in terms of both eliminating those the Israelis had deemed responsible as well as reducing the frequency and magnitude of terrorist attacks in the short term.[53] It must be noted though that such targeted killings may create martyrs that can be useful for terrorist propaganda and recruitment purposes. Furthermore, such a CA weapon eliminates a target that may hold information of value for counter-terrorism purposes. In the analysis preceding such operations, a critical issue that must be also considered is whether the replacement for an assassinated terrorist will increase the overall threat of terrorism from the relevant terrorist entities. Although in a far different context, similar analyses were made by British intelligence in World War II when plans for the assassination of Adolf Hitler (Operation Foxley) were aborted. The conclusion had been made that as leader, Hitler was leading the Germans to almost certain defeat and that a more competent replacement would have reversed this process.[54] Finally, a professional operational capability for such operations will be vital so as to prevent any mishaps from occurring in the course of such operations.

[50] Whittaker, David J. (2004): *Terrorists and Terrorism in the Contemporary World,* New York, Routledge, p. 134.
[51] David, Steven R. "Israel's Policy of Targeted Killing", *Ethics and International Affairs*, Vol. 17 (2003), p. 1.
[52] Hunter, Thomas B.: "Wrath of God: The Israeli Response to the 1972 Munich Olympic Massacre", *Journal of Counter-Terrorism & Security International,* Vol. 7, No. 4 (2001), p. 14.
[53] Byman, Daniel: "Do Targeted Killings Work?", *Foreign Affairs*, Vol. 85, No. 2 (2006), p. 102.
[54] Hosmer, Stephen T. (2001), Operations against Enemy Leaders. Santa Monica, RAND, p. 32.

5.7. The Risk of Failure

CA may fail for many of the same reasons that other elements of intelligence may fail. Its requirement for a clear set of objectives, an accurate understanding of the conditions in which it will take place and how the objectives will have been achieved, are all subject to fallible human interpretation.[55] Yet what separates this arm of intelligence from all others is its use of third parties. The use of such groups outside the direct control of intelligence organisations is essential in maintaining deniability.[56] They have been commonly used in CA operations that have aimed to exert political and economic influence on foreign territories. Such exertion of influence can be done through foreign structural and agential means, examples being: paramilitary groups, political organisations and those generally aiding the foreign intelligence organisation in achieving its objectives.[57] The use of such third parties produces a host of problems that may lead to intelligence failures. With regards to secrecy third parties are not obliged to respect the rules that the personnel of an intelligence organisation will have to abide by, nor will they have gone through any vigorous and extensive screening process to ensure a certain degree of reliability and trustworthiness.[58] This dependence on third parties can also be identified in the use of psychological warfare, as such actions put the onus on a third party target to believe what it is being told.[59] One hundred percent accuracy is the only margin of safety in preventing intelligence failures and one that is innately out of reach for any national security apparatus, intelligence being no exception. It is important to note though that as with most endeavours, intelligence and security organisations that refuse to risk failure in CA operations will in great likelihood become ineffective.

6. Offence is the Best Defence

In facing the modern terrorist adversary, defensive or passive intelligence can be of limited utility. Intelligence in the traditional sense of collection and analysis may occasionally help government and its institutions in curbing terrorist intentions, but the law of odds determines that it will only be a matter of time before a catastrophic attack is carried out. Terrorists have increasingly been gaining access to ever more powerful weapons of death and destruction, a reality which nation-states have previously not had to deal with. It is inevitable that this trend will continue, and that terrorists will in the future gain the potential for acquiring ever more hazardous weapons. In addition, terrorist organisations, such as those that are Islamist in nature, are actively engaged in acquiring new recruits to bolster their capabilities. These recruits are increasingly joining such terrorist organisations from widely differing backgrounds, which continues to make any form of profiling largely ineffective. Those threatened by such terrorists therefore cannot hope to effectively gain the upper hand by simply standing idly by and observing an ever expanding army of terrorist recruits that are falling prey to terrorist propaganda. Even the greatest amount of investment in intelligence collection and analysis alone will fail to adequately protect citizens from the scourge of terrorism. Citizens understandably do not wish to give up many of their rights and freedoms to simply aid the task of counter-terrorism, therefore working beneath a haze of normality as just another citizen, allows terrorists to pose an increasingly insidious threat. The very rights

[55] Shulsky, *op. cit.,* p.84.
[56] Wettering, *op. cit.,* pp.562
[57] *Ibid.,* p. 562.
[58] Gunter, Michael M.: "The Iraqi Opposition and the Failure of U.S. Intelligence", *International Journal of Intelligence and Counter Intelligence* 12, No. 2 (2002), p. 144.
[59] Shulsky, *op. cit.,* p. 93.

and privacy laws offered by democratic nation-states create highly attractive environments within which to operate by terrorists, thus making democracies more vulnerable to terrorism. A greater effort must therefore be made by national governments to communicate to the public the nature of the terrorist threat and the measures that will be necessary in order to combat it. By doing so, governments are less likely to face public outrage in the probable event that details of surveillance, data mining or other such operations are leaked. Furthermore, this would offer a measure of legal stability to national intelligence and security organisations, to prevent them from having to go through difficult adaptations to endless cycles of legal amendments, such as those experienced by the US intelligence community, that continuously seek to restrict or expand their powers. Just as governments have a responsibility to keep soldiers suitably equipped in battlefields, they must ensure that intelligence officers are adequately empowered to pursue the goals with which they have been tasked.

The modern day information revolution has allowed terrorists to benefit from the advancements in a global multi-billion dollar technology industry. These same technologies have allowed terrorists to evolve their hierarchical structures into decentralised forms that complicate the work of intelligence and security organisations seeking to eliminate the threat of terrorist organisations. In such an environment of trans-national terrorism, simply defending one's homeland will not suffice, as passive intelligence or law-enforcement style strategies simply do not have the capability to deal effectively with present day and future terrorism. Terrorism and the threat of terrorism must be identified, wherever it may exist and be eradicated, as nation-states will have to go further than mere containment if they are to gain the upper hand on such an enemy. As an offensive or active weapon, CA will be an invaluable tool in the present and future intelligence wars of nation-states against technologically and hierarchically empowered terrorists. CA activities such as PSYOP, Deception, IO, Political CA, Economic CA and targeted killings are all valuable weapons in the counter-terrorism arsenal of nation-states. Greater emphasis must also be placed on the development of centres or joint centres specialising in the development, planning and execution of CA in an integrated manner, as it can only be in such an environment that the full potential of CA can be utilised.

One thing that is certain is that for as long as there will be humans, there will exist men and women willing to use terrorist strategies in support of a cause. For the security of present and future generations we must now ensure that forceful approaches are developed and taken through CA to counteract such ill intentions.