CRITICAL ISSUES IN CONTEMPORARY COUNTER-INTELLIGENCE

Kaveh Moravej [1]
Manchester University

Gustavo Díaz [2]
UNISCI / Universidad Complutense de Madrid

Abstract:
The world of counter-intelligence is one in which truth, lies and deception converge in perhaps the most sophisticated manner. As a result of this reality, intelligence organisations are forced to take extensive measures to ensure that the right people are employed and that in the event of a breach, damage is limited. In attempting to weave their way through this intricate maze in a most effective manner, a balance must be struck between security and operational effectiveness. Counter-intelligence can be defined as intelligence gathered about an adversary's intelligence activities and capabilities to unmask and inhibit adversarial intelligence operations and capabilities. This can involve various types of action to prevent or neutralise hostile intelligence successes against national interests.

Keywords: Intelligence, counter-intelligence.

Resumen:
El mundo de la contrainteligencia (CI) es en el que probablemente se entrelaza de una manera más sofisticada la verdad, la mentira y el engaño (deception). *Como resultado los distintos servicios de inteligencia se ven forzados a tomar medidas que aseguren que las personas correctas son utilizadas para según que puesto y que en caso de fisura el daño sea el menor posible. Para conseguir la mayor efectividad es fundamental encontrar la relación correcta entre seguridad y efectividad operacional. Si entendemos CI como la información recogida sobre las actividades de inteligencia del adversario y la capacidad de desenmascarar y neutralizar es esfuerzos. Esto pude incluir distintas acciones encaminadas a prevenir y neutralizar actividades que atenten contra la seguridad nacional.*

Palabras clave: *Inteligencia, contrainteligencia.*

[1] Kaveh Moravej is a Ph.D. Candidate at the University of Manchester, and holds a M.A. in Intelligence and Security Studies, University of Salford. His main research interests are intelligence services.
Address: School of Languages, Linguistics, and Cultures, The University of Manchester, Manchester M13 9PL, United Kingdom. *E-mail:* kaveh@moravej.com.
[2] Gustavo Díaz Matey is a Research Fellow at UNISCI, Complutense University of Madrid, and holds a M.A. in Intelligence and Security Studies, University of Salford. His main research interests are international security and intelligence.
Address: Departamento de Estudios Internacionales, Facultad de Ciencias Políticas y Sociología, UCM, Campus de Somosaguas, 28223 Madrid, Spain. *E-mail:* G.DiazMatey@pgt.salford.ac.uk.

Introduction

James Jesus Angleton, former head of CIA counter-intelligence, once famously described counter-intelligence as a 'wilderness of mirrors'. This phrase, borrowed from T. S. Eliot, aptly describes the infinite complexity of the field. In this mirrored world of distortion, attempting to understand and gain the upper hand on an adversary can be an excruciatingly difficult and complex task.[3] The world of counter-intelligence is one in which truth, lies and deception commingle in perhaps the most sophisticated manner. As a result of this reality, intelligence organisations are forced to take extensive measures to ensure that the right people are employed and that in the event of a breach, damage is limited. In attempting to weave their way through this intricate maze in a most effective manner, a balance must be struck between security and operational effectiveness. Too much security can indeed be a bad thing. In the event of unreasonably draconian security measures the best potential employees may be turned away, the morale of employees may be negatively impacted, and the restricted flow of information may hinder the work of intelligence analysts and case officers. The world of counter-intelligence is not simply defensive though, as its use in an offensive manner can paralyse an adversary in indecision and paranoia, forcing the adversarial intelligence organisation to crumble from within. Technological developments have also brought about challenges for those tasked with maintaining the cover of intelligence employees. In a world in which mere internet searches can accurately reveal the identities of hundreds of intelligence employees, new approaches are required to ensure the safety and security of such personnel.[4] To begin to understand how this crucial equilibrium between security and operational effectiveness can be acquired, one must first accurately understand the true meaning of counter-intelligence.[5]

1. What is Counter-Intelligence?

Counter-intelligence can be defined as intelligence gathered about an adversary's intelligence activities and capabilities to unmask and inhibit adversarial intelligence operations and capabilities.[6] This can involve various types of action to prevent or neutralise hostile intelligence successes against national interests, such as the production of knowledge concerning the plans, operations, and capabilities of those organisations intent upon subversive activities. The term is used here in a broad sense, to include espionage, sabotage and other related actions.[7] Counter-intelligence is also often the most arcane and organisationally fragmented, the least doctrinally clarified, and legally, and thus politically, the most sensitive intelligence activity. It provides information upon which military commanders and civilian agency managers should base their decisions upon regarding security measures. Beyond this authority, which effectively is to protect intelligence, not to provide general security to outside organisations, Intelligence Community officials have only the power of persuasion when it comes to security measures in non-intelligence organisations. One should emphasise though that it may sound a bit illogical to call counter-intelligence a type of intelligence, particularly if we think of intelligence as knowledge, and counter-intelligence as an activity or organisation (or part of an organisation) acting against forces

[3] Phrase from: Eliot, T. S. (2003): *The Waste Land and Other Poems,* Penguin Books; quoted by Martin, David C. (1980): *Wilderness of Mirrors,* Harper Collins.
[4] Crewdson, John: "Internet Blows CIA Cover", *Chicago Tribune*, 12 March 2006.
[5] Kalaris, George and Mc Coy, Leonard: "Counter-intelligence for the 90s", *International Journal of Intelligence and Counter-intelligence*, Vol. 2, No. 2 (1987), p. 179.
[6] Odom, William E. (2003): *Fixing Intelligence*, New Haven / London, Yale University Press.
[7] Activities defined in *U.S Federal Statutes*, Chapter 115, Title 18, U.S Code.

seeking knowledge. Indeed the first thing we must do is to differentiate between counter-intelligence information (knowledge) and counter-intelligence measures (activity) and the allocation of personnel to these duties (organisation).[8] In this sense, the activity of counter-intelligence is the production of knowledge, and as with all the intelligence, this knowledge is not produced for the counter-intelligence organisation alone, but ultimately for other elements of the state. One should also distinguish between counter-intelligence activities and security measures, as security measures are defensive in nature, applied as protection against the elements which counter-intelligence seeks knowledge of.[9]

Specifically as organisation, counter-intelligence consists of personnel, along with their organised skills and methods, as well as their organised fields of data, that produce counter-intelligence knowledge. Counter-intelligence can also involve offensive measures, with deception operations being one such example. Deception operations, like security measures, are command and management functions, and not solely counter-intelligence or intelligence functions. Just as tactical intelligence supports military combat operations, counter-intelligence must support deception operations.[10] Another doctrinal boundary lies between counter-intelligence and 'arrest authority'. Once an espionage agent is detected, by definition a crime is also detected. Law enforcement officials must arrest that person if it is decided to neutralise his activities. The key point with regard to this boundary is that counter-intelligence organisations need not have arrest authority. If one sought to adhere to the doctrinal principle, then one would keep counter-intelligence organisations separate from law enforcement responsibilities, including arrest authority.[11] To be effective, counter-intelligence must also involve taking advantage of signals and imagery intelligence to discover hostile entities. In addition, counter-intelligence operations must also learn about the capabilities and targeting of hostile signals and imagery intelligence. This broader approach is often termed 'multidisciplinary counter-intelligence'.[12]

In specifically observing the U.S. interpretation of counter-intelligence one can find that it is defined by President Reagan's Executive Order 12333, which is still in force, as both 'information gathered' and 'activities conducted' in order to 'protect against espionage, other intelligence activities, sabotage or assassination conducted on behalf of foreign powers, organisations or persons, or international terrorist activities but not including personnel, physical documents or communications security'.[13] From the U.S. intelligence perspective, there are therefore four basic functions of counter-intelligence.

(I) Collection of information on foreign intelligence and security services and their activities through open and clandestine sources.

(II) The evaluation of defectors.

---

[8] Classification taken form Kent, Sherman, (1949): *Intelligence for American World Policy*, Princeton NY, p. xi.
[9] *Dictionary of U.S Military Terms of Joint Usage, Military Regulations*. U.S. Army Regulation, pp. 310-25, at http://www.fas.org/irp/doddir/army/ar310-25.pdf, pp.56.
[10] Dear, Ian C.B (1996): *Sabotage & Subversion: Stories form the files of the OSS and SOE*, Cassell Military Paperbacks.
[11] Odom, *op cit.*
[12] U.S. Department of Defense: *Counter-intelligence (CI) Directive,* No. 5240.2, 22 May 1997; see also: "Counter-intelligence, Psy-war, and Unconventional Warfare", at http://faculty.ncwc.edu/toconnor/427/427lect09.htm
[13] *Executive Order 12333*, United States Intelligence Activities, 4 December 1981, at http://www.tscm.com/EO12333.html.

(III) Research and analysis concerning the structure, personnel, and operations of foreign intelligence and security services.

(IV) Operations for the purpose of disrupting and neutralising intelligence and security services engaging in activities hostile to the national interest.

Of course it must be stressed that like the definition of intelligence, there are various interpretations of what counter-intelligence specifically involves, both within a given country, and outside of it. This paper will therefore address some of the above functions, but will also deal with the wider and more critical issues of the day relevant to the field of counter-intelligence.

2. The Functions of Counter-Intelligence

2.1. Protecting secrets

The first responsibility of counter-intelligence is to protect information. Two aspects relating to this function are: First, physical security, which involves keeping classified information away from those who are not authorised to have access to it, and secondly, making sure that the people who are made aware of restricted information protect that information. The most obvious physical security measures involve the keeping of foreign intelligence officers and their agents away from classified information by denying them access or proximity, and preventing unauthorised personnel from walking off with such information.[14]

2.2. Vetting - The First Line of Defence

The protection of acquired knowledge is a vital function of any intelligence organisation, yet no amount of extensive security and stringent assessment checks will guarantee that an employee will observe the rules. It would also be logical to assume that if a person has access to any piece of information then it can in all likelihood be compromised. In holding the responsibility of protecting their knowledge, intelligence organisations are faced with two dilemmas in their selection of employees. Firstly, the instruments of psychological and behavioural measurement hold accuracy rates that are below 100%, allowing individuals who may pose a security threat to be cleared for employment.[15] Secondly, attempting to create a profiling system that identifies future betrayers would be an imperfect process leading to the allocation of resources towards the wrongfully suspected rather than those well trained in evading detection.[16] Given the complexity and importance of this problem it seems somewhat surprising that so little scientifically grounded paradigms exist for the detection and prevention of such espionage methods.[17]

[14] Wettering, Frederick L.: "Counter-intelligence: The broken Triad", *International Journal of Intelligence and counter-intelligence*, No. 13 (2000), p. 268.
[15] Sarbin, Theodore R., Carney, Ralph M. and Eoyang, Carson (eds.) (1994): *Citizen Espionage: Studies in Trust and Betrayal*, Westport, CT, Praeger, p. 70.
[16] Sarbin, *op cit*., p. 70.
[17] Weltring, *op cit*., p. 270.

Drawing upon psychological models would be the most rational method of detecting betrayers, as it offers us the chance to identify psychological abnormalities.[18] Whilst physical actions may identify a betrayer and prevent the continuing compromise of knowledge, it is the prevention of such an intelligence failure that should be our primary concern and for this we must turn to psychology.

The psychological paradigm essentially makes the assumption that those who are actively compromising information or liable to betray secrets, are likely to differ in a measurable, reliable, and distinct way from those people who are not likely[4]. Moreover, there exists the assumption that an underlying characteristic, not yet identified, is related to the likelihood of an actor to engage in betrayal. If this characteristic can be identified and measured reliably, those who score below a scientifically established threshold can be denied access to the most critical and sensitive positions of an intelligence organisation[5]. Until such a system comes to fruition though, intelligence failures in this field will be a likely occurrence. The most common occurrences of betrayal have been linked to money, ideology, coercion and ego, all of which are extremely problematic to measure scientifically[6]. Other psychological factors in bringing out betrayal can be disaffection, vindictiveness and whimsy, all of which are again impossible to accurately measure with today's scientific and psychological capabilities. The complex nature of such traits also reduces the likelihood of scientific means ever being developed to fully screen out personnel that may in future betray secrets.

The British method (Developed Vetting) of clearing employees for intelligence and security work, is also prone to failure. Developed Vetting (DV), the most comprehensive form of security vetting in the UK, is a process that involves paper references and interviews with referees (e.g. social, employment, education). The referees will normally be people who have known the applicant over a significant period their life (excluding blood relatives). They will be asked to describe the applicant's way of life, attitudes, abilities etc. Applicants are also interviewed and asked to produce a passport, birth certificate and any other relevant documents. During this process (and often towards the end) and with the permission of the applicant, the applicant's current employer is also contacted by the relevant intelligence and security organisation. The process in its entirety usually takes 3-4 months. One distinctive element of the British clearance process that sets it apart from the US is that the applicant must have at least one parent that is a British citizen.[19] This in all likelihood is a hopeful attempt that the applicant will be psychologically less prone to betraying the nationality of a parent. There are of course no known figures (if they at all exist) to judge the efficacy of such a policy, but it would be realistic to assume that the U.S. also places a higher level of security risk on an applicant that does not have at least one parent that is a U.S. citizen. U.S. intelligence employees with familial ties to non-U.S. Citizens have also been known to be rebuked on a regular basis by their employers for their contacts with foreign national relatives. Furthermore, an applicant that is married to or living with a person who is not a British or U.S. citizen remains eligible for employment at the discretion of the potential employer.

Marriage to, or co-habitation with a person who is not a British or U.S. citizen after being hired, may in some circumstances result in withdrawal of security clearances and transfer to another department (effectively a demotion), or upon refusal of a transfer, dismissal.

It can be deduced from these realities therefore that from the perspective of the relevant intelligence and security organisations, the racial and ethnic diversity of the British and U.S.

[18] Sarbin, *op cit*., p. 71.
[19] Quinn, Ben: "Muslim Pc Barred from Guarding Blair", *Daily Telegraph*, 8 November 2006.

populations is looked upon both as a great strength and a threat. In the British case it is made clear that even British citizens (without a British parent) are to be viewed as untrustworthy.[20] Indeed similar regulations are in place throughout the British Military (with greater trust placed in Commonwealth citizens), in contrast to the U.S. Military which accepts all U.S. citizens.[21] Determining which route is 'safer' from a counter-intelligence point of view is not immediately obvious, but what is likely is that the inequitable nature of the British regulations, effectively creating a second class of British citizen, is prone to turning away many of the most able and sought after potential applicants, such as those of Arab descent. In such an instance U.S. Intelligence is far better placed to recruit the best candidates, particularly owing to the ethnic diversity of its population and large pool of immigrants. Of course by recruiting such applicants, U.S. Intelligence organisations may also be placing themselves at greater risk from a counter-intelligence standpoint. It would be logical therefore to reason that the best form of recruitment would be one accepting all national citizens of the country, yet deciding who is to be trusted with sensitive information on a case by case basis. Indeed, owing to CIA security worries that job candidates with foreign ties could leak sensitive information, candidates with foreign links would usually have to endure long waits as the agency investigated their families and friends. Post 9/11 these extensive checks were reviewed. Porter Goss, the DCI at the time, whilst concerned about possible security breaches, understood that lengthy checks were costing the agency valuable recruits.[22] Goss also made clear that he was more worried about terrorists killing people than "a terrorist reading a top-secret report". In today's global political climate it is essential that intelligence and security organisations reach out to those particularly of Arab and Chinese descent as it will be people of such backgrounds who will be able to deal with the most critical security challenges of the day. Those of European ethnicities may have been able to operate within Soviet borders without standing out a great deal, but to have similar expectations within the Middle and Far eastern regions would be unrealistic. From an intelligence and security perspective the ethnic diversity of populations like that of Britain and particularly the U.S., should be looked upon as an invaluable asset in gaining a competitive advantage in the world of intelligence warfare.

2.3. Internal Checks and Reviews

In addition to ensuring that new employees will not pose a security risk, as part of the counter-intelligence process, already hired personnel will also be subject to reviews every few years. The dates of such reviews can also be brought forward if there is reason to believe that any particular individual may be violating standard security procedures. Employees can be flagged as security risks for various reasons, such as attempts to access information not relevant to their area of focus and irregular psychological behaviour. One of the methods used to reduce the likelihood of unauthorised access is compartmentation, although such a method can also have the negative effect of restricting the flow of information, particularly in cases where information may be required from numerous areas of focus.[23] In addition, creating an environment where everyone is a suspect can also negatively impact the morale of employees.

[20] Intelligence and Security Committee, *Annual Report 2005-06,* 1 July 2006.
[21] Bender, Bryan: "Military Considers Recruiting Foreigners", *The Boston Globe,* 26 December 2006.
[22] Diamnond, John "It's no Secret: CIA Scouting for Recruits", *USA Today*, 22 November 2005.
[23] Hulnick, Arthur (1999): *Fixing the Spy Machine,* Westport, Praeger.

2.4. TSCM[24]

Technical security countermeasures (TSCM) are a collection of technical efforts to detect the technical penetrations of facilities by foreign intelligence services to collect intelligence. The best-known are electronic audio listening devices, or bugs.[25]

TSCM measures usually involve trained technicians who, using both sophisticated electronic and x-ray devices, as well as painstaking physical examination, 'sweep' an area to discover any such devices. TSCM simply has far too few resources dedicated to it compared to the breadth of the attacks. Sweeps, even of highly-threatened facilities, are made too infrequently. Encryption of communications is also an often used counter-intelligence tool, but like sweep teams, is not used nearly enough to secure information. Part of the problem relates to the sheer volume of communications involved in, for example, a military deployment. Within democracies, another part of the problem is the cultural trait of avoiding any counter-intelligence procedure that is too intrusive or value-conflicting.[26]

3. Frustrating Foreign Intelligence Operations

A major function of counter-intelligence is clearly to frustrate the efforts of foreign intelligence operatives in stealing sensitive information. Essential parts of any counter-intelligence effort are good record-keeping and the sharing of information among agencies. Record-keeping is at the heart of any counter-intelligence program, but the single most effective counter-intelligence technique used to suppress foreign spying is the expulsion or denial of entry to suspected foreign intelligence officers.[27] The positive outcomes though as a result of such actions are generally short-term. Most intelligence personnel operate with the protection of diplomatic status, or 'official cover', as it is known within the intelligence community. One may wonder if expulsions with publicity and visa denials are so successful, why are they not used more often? The answer is twofold: first, the foreign governments always retaliate, although not always proportionately. More importantly, such expulsions seriously damage relations with the state whose suspect diplomats have just been expelled. Important bilateral and multilateral agreements, as well as trade relations - the basic elements of diplomacy and state-to-state relations - are put at risk. Mutual hostilities increase as a result, and diplomatic 'hawks' are encouraged. This being so, presidents, prime ministers, and especially foreign ministries almost always oppose such expulsions.[28]

Almost anywhere in the world, the potential amount of counter-intelligence is vast, and produced for the national interest, both within the country and in all the foreign areas to which a country's interests extend. Information concerning the activities of foreign intelligence security services comes from a variety of sources. In the case of closed societies, open source material is limited. Information about friendly services may come from liaison and training arrangements.[29] Liaison with allied services also provides information about the activities of

[24] *TSCI - Technical Surveillience Countermeasures Handbook,* Technical Security Consultants Inc., http://www.dbugman.com/handbook/index.html
[25] Wettering, *op cit*., p. 276.
[26] *Ibid*. p. 277.
[27] Richelson, Jeffrey T. (1999): *The U.S. Intelligence Community*, USA, Boulder, Westview.
[28] Wettering, *op cit*., p. 280.
[29] Schweitzer, Peter (1993): *Friendly Spies: How America's Allies are using Economic Espionage*, NY Monthly Press.

hostile services.[30] Two types of human sources may provide useful information. The first is the individual that holds an official position within a hostile service. This individual may agree to provide information for ideological or financial reasons or as the result of coercion or blackmail, which might be based on evidence of sexual or financial misbehaviour. Beyond human sources, technical collection also provides data of value for counter-intelligence. Intercepted communications from within a country or to embassies overseas can reveal either the activities of the internal security service or the intelligence activities of the foreign intelligence service. Satellite imagery is decidedly less useful than human sources, open sources, or signals intelligence in providing information about most activities of foreign intelligence services. It can, however, provide information on the precise location and layout of intelligence and security service complexes.[31]

3.1. Using Physical Surveillance

Physical surveillance, the most common technique of counter-intelligence worldwide, can be very labour intensive and tedious. Positive results are also few and far between. Physical surveillance can be divided into three parts: static surveillance, mobile surveillance, and electronic and other surveillance.

A) Static Surveillance

Static or fixed-point surveillance is observation of a place, perhaps a suspect's residence, or a 'choke-point', where suspects regularly have to pass, or, more commonly, the chancery building of a foreign embassy whose personnel include intelligence officers. Such surveillance has three purposes: to alert a mobile surveillance team when a subject exits or passes by so that the team might pick the suspect up; to chronicle a suspect's movement and/or visitors; and to attempt to identify would-be agents walking into a foreign embassy to volunteer their services.

The third purpose, catching prospective enemy agents and intelligence officers is, frankly, not well-served. Static surveillance has a very narrow window of usefulness to counter-intelligence, and is therefore better suited to watching suspects and catching low-level would-be adversaries than to ensnare heretofore undiscovered real enemies coming in off the street.

B) Mobile Surveillance

Mobile surveillance can be done in many ways: on foot, cycle, vehicle, and aircraft. This type of surveillance, very common worldwide, is designed for two purposes: to intimidate and discourage a suspect from undertaking an illegal act relating to espionage, and catching the suspect in the act of undertaking some aspect of espionage.

[30] Johnson, Loch K. (2002): *Bombs, Bugs, Drugs, and Thugs*, New York, New York University Press.
[31] Richelson, *op. cit.,* p. 238.

C) Electronic and Other Surveillance

Electronic surveillance by means of telephone taps (teltaps) or electronic listening devices (bugs), and other forms of surveillance, such as 'mail-covers' (intercepts), serve to frustrate foreign intelligence officers by identifying their contacts, and either subsequently blocking their communications or enabling them to be converted to 'double agents'. Electronic devices also assist mobile surveillance with such tools as 'beacons' which broadcast the location of a vehicle or item. These special surveillance tools are very useful to counter-intelligence. Teltaps and bugs can serve other purposes bedsides discovering contacts or tracing the movements of suspects. In terms of frustrating espionage efforts, the utility of electronic and other devices is limited, and presupposes that foreign intelligence officers will meet a real or would-be enemy contact in the country.

The most effective sources for identification purposes are the defecting foreign intelligence officers and the agents themselves. The second most effective is the decryption of coded messages, primarily electronic. The third most effective are intelligence efforts to acquire this information, including attempts to recruit foreign agents who have such knowledge. A fourth is through double agents. Double agents are individuals who fall into either of two categories: (a) foreign espionage agents who have been discovered and subsequently agree to work for their counter-intelligence captors to avoid penalties; (b) or 'dangles', controlled sources who are used as bait in front of a foreign intelligence officer, often by directly volunteering to work for them, in the hope that the officer will take the bait and attempt to recruit the dangle. From such agents a counter-intelligence officer hopes to learn the identity, methods of operation, and surveillance equipment provided by the intelligence service to 'their' agent. The effort also offers an opportunity preoccupy the other side's officers, keeping them occupied and without time to chase valid target. Lastly, it offers opportunities for disinformation.

4. Counter-Intelligence and the Internet

The rapid growth and usage of the internet has brought about new challenges for those engaged in the conduct of counter-intelligence. The vast volume of information available on the internet, directly accessible and cached from previous years, provides foreign intelligence agencies as well any determined individual, with the opportunity to discover classified information through various means. Indeed, one newspaper went as far as creating a directory of more than 2,600 CIA employees, 50 internal agency telephone numbers and the locations of some two dozen secret CIA facilities around the United States, simply by searching a commercial online data service.[32] The information acquired included the names of clandestine CIA operatives assigned to U.S. embassies, covert mailing addresses used by some of those operatives, and the 'cover names' used by several members of the CIA's paramilitary Special Activities Division.[33] Home addresses and telephone numbers of CIA headquarters employees were also available for a price, as were those of some CIA officers operating overseas posing as business executives or using other 'non-official cover'.[34] The data was acquired from sources such as telephone listings, real estate transactions, voting records, legal judgments, property tax records, bankruptcies and business incorporation papers. It would be logical

[32] Crewdson, John: "Internet Blows CIA Cover", *Chicago Tribune*, 12 March 2006.
[33] Crewdson, John: "Data Mining Easy as Using Credit Card", *Chicago Tribune*, 11 March 2006.
[34] *Ibid.*

therefore to accept that an organisation far superior in resources would be able to identify via the internet a far greater number of supposedly classified details.

Whereas the internet is all about the rapid and free distribution of information, an intelligence and security organisation seeks to restrict and make difficult the access of their information. Government, particularly in the United States may seek to restrict freely available databases of personal information by toughening lax privacy laws, but such actions would also make difficult the work of intelligence and security organisations, as well as certain private sector corporations, by eliminating the availability of certain information crucial to their operations. In such a scenario therefore, it is crucial that those engaged in operational security rapidly adapt to the information age. Of course it must be said that rapid changes in the workings of public sector organisations is often an unrealistic expectation, but nevertheless, particularly in the instances where the lives of intelligence officers could be at risk, adequate measures must be taken to ensure that the identification of classified information becomes an impossibility on the internet. To determine precisely what measures must be taken would move beyond the scope of this paper, but several crucial elements of such counter-intelligence activities will undoubtedly be an in depth knowledge of the Internet's infrastructure and the methods in which information on it is accumulated and stored.

It must be said that to place all responsibility for the cover of intelligence employees on the intelligence employer would be unrealistic, as employees must all ensure that away from work appropriate security measures are always taken. Many employees of intelligence and security organisations, particularly elder generations will most likely not have the technological knowledge or ability required to ensure high levels of data security. Foreign intelligence organisations, such as that of China, have highly skilled employees that are more than capable of attacking and breaching the electronic security of even the most security conscious.[35] On numerous occasions it has been revealed that electronic attacks from China (code-named Titan Rain) have successfully breached the networks of the Department of Defence and other US agencies.[36] Private defence contractors have also been the victims of such attacks. With the threat of computer intrusions on the rise generally among Internet users, U.S. government officials have made no secret that their systems, like commercial and household ones, are subject to attack. As the Pentagon has more computers than any other agency, approximately 5 million worldwide, it is the most exposed to foreign as well as domestic hackers.[37] Pentagon statistics have shown that more attempts to scan Defence Department systems come from China, which has 119 million Internet users, than from any other country. The number of attempted intrusions from all sources identified by the Pentagon in 2004 totalled about 79,000, up from about 54,000 in 2003.[38] Of those, hackers succeeded in gaining access to a Defence Department computer in about 1,300 cases.[39] Similarly concerning is that the People's Liberation Army (PLA) now sees computer network operations as critical to seizing the initiative in establishing electromagnetic dominance early in a conflict that would lead to increased effectiveness in battle. In addition, one recent DoD report notes that "The PLA has likely established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics to protect friendly computer systems and networks".[40] In the same report it is also noted that the PLA has increased the role of CNO [computer network operations] in its military exercises and that whilst the PLA's

[35] McElroy, Damien: "China Aims Spy Network at Trade Secrets in Europe", *Daily Telegraph*, 3 July 2005.
[36] Graham, Bradley: "Hackers Attack Via Chinese Website", *Washington Post*, 25 August 2005.
[37] Solomon, Jay: "FBI Sees Big Threat from Chinese Spies", *The Wall Street Journal*, 12 August 2005.
[38] Graham, Bradley: "Hackers Attack Via Chinese Website", *Washington Post*, 25 August 2005.
[39] *Ibid.*
[40] Rogin, Josh: "DOD: China Fielding Cyber Attack Units", *Federal Computer Week,* 25 May 2006.

initial training efforts have focused on increasing the proficiency in defensive measures, their more recent exercises have incorporated offensive operations, primarily as first strikes against enemy networks.

5. Foreign Intelligence Agencies

The greatest foreign intelligence threat today facing democratic nation states, is that of Chinese and Russian foreign intelligence organisations. The former remains an authoritarian nation-state whilst the latter continues today as a semi-authoritarian nation-state. Though the Cold War has long been over, both countries still perceive many democracies, both within their own regions and outside of it, as their strategic competitors. Though economic relations remain largely positive between the U.S. and China, the U.S. Department of Defense (DOD.) has made clear through its 2006 annual report to Congress that it considers the People's Republic of China a military and security threat. China's economy has been growing at a rate of at least 10 percent for each of the past 10 years, providing the country's military with the needed funds for modernization. The combination of a vibrant centralized economy, growing military and increasingly fervent nationalism have transformed China into what many DOD. officials view as a fascist state. [41]

Russia has also displayed through its actions that it considers the democratisation of its surrounding countries a threat. As Europe and North America have largely been the backers of such democratic movements, Russia has also considered many of the nation-states within these regions as strategic threats. Whilst not overtly hostile therefore, both Russia and China view countries such as the U.S. and UK as adversaries. This reality has led to a covert war where both Russian and Chinese foreign intelligence agencies are actively operating against the interests of various foreign countries that they perceive as being adversarial.

5.1. China

China is stepping up its overt and covert efforts to gather intelligence and technology in the world, and their activities have boosted the Chinese regime's plans to rapidly produce advanced-weapons systems.[42] It has been said that developments that would normally take 10 years to develop take China two or three. The Chinese have become highly effective collectors of secrets and military-related information. Chinese foreign intelligence operations have been mostly focused in areas such as command and control. In the military field, the rapid development of the Chinese navy can be in part attributed to some of the research and development information collected in the U.S..[43] The Chinese intelligence services use a variety of methods to collect intelligence on foreign soil, including traditional intelligence operations targeting U.S. government agencies and defence contractors. Additionally, China make use of the hundreds of thousands of Chinese visitors, students and other non-professionals to gather valuable data, most of it considered 'open source', or unclassified information. This asymmetrical, unofficial presence is further strengthened by as many as 3,200 Chinese front companies, many run by groups linked to the Chinese military; set up to covertly obtain information, equipment and technology.

[41] Johnson, *op cit.*
[42] Hill, John: "Defections Reveal Extent of China's Espionage Operations", *Chicago Tribune*, 11 October 2005.
[43] Caldwell, Oliver J. (1972): *A Secret War: Americans in China*, Carbondde, Southern Illinois University Press.

As a result of this massive numerical presence, the problem of Chinese intelligence operations is a daunting one.

The three main Chinese government units that run intelligence operations are the Ministry of State Security, the military intelligence department of the People's Liberation Army and a small group known as the Liaison Office of the General Political Department of the Chinese Army.[44] China in fact gathers most of its important information not from intelligence officers but from unwitting American visitors to China, from both the U.S. government and the private sector. Due to their more indiscreet nature, many of these individuals easily disclose information sought by the Chinese. The model that China has for its intelligence, in general, is to collect a small amount of information from a large amount of people.[45]

Exacerbating this problem is the fact that since 1985, there have been only six major intelligence defectors from China's spy services, and information about Chinese activities and methods is limited.

5.2. Russia

As with all states that require a system of intelligence gathering beyond their borders, Russia has been no exception. Russia retained its foreign intelligence apparatus after the collapse of the Soviet Union, creating the *Sluzhba Vneshney Razvedki Rossii* (SVR) from the KGB's former First Chief Directorate. Russia's foreign intelligence capabilities owe much to the KGB, particularly as the counter-intelligence sections of most foreign intelligence agencies proved to be no match for the KGB. Many of the KGB's efforts duped even organisations such as the FBI and CIA.[46] Indeed in one well-known incident, an atmosphere of such paranoia had been created within the CIA that a bona fide Soviet defector was imprisoned. The KGB's successors seem to have continued from where their predecessors left off, with Russia's foreign intelligence service having to frequently refute accusations against it by the security services of countries such as the U.S. and Britain. These security services have claimed that the SVR's activities in the United States and the EU, including its recently admitted members, have reached Cold War levels.[47]

In particular, Britain's MI5 has warned government departments that Russia has resumed Cold War spying methods in Britain.[48] This was revealed in a confidential document that was circulated in response to an increase in the activities of Russian intelligence officers.

The document warned that Russian intelligence officers were travelling widely throughout Britain and posing a 'substantial' threat. MI5 claimed that these activities were related to attempts by Russia at collecting classified information about Britain's military capabilities and its defence industry. It was also believed that Russia was interested in the activities of Chechen asylum seekers and their associates. The SVR is believed to have about 18 offices in Britain while the *Glavnoje Razvedyvatelnoye Upravleniye,* GRU (military

[44] Eftimiades Nicholas (1994): *Chinese Intelligence Operations,* Annapolis, Md, Naval Institute Press, p. 29.
[45] *Ibid,* p. 28. See also: Loeb, Vernon: "Chinese Spy Methods Limit Bid to Find Truth, Officials Say," *Washington Post*, 21 March 1999, p. A24.
[46] Andrew, Chistopher and Gordesvsky, Oleg (1990): *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*, London, Hoder and Stoughton, p. 381.
[47] Fidler, Stephen: "Moscow Steps Up Spying in UK", *Financial Times*, 20 November 2006.
[48] *Ibid.*

intelligence) is said to have 14 - all in the guise of official Russian organisations, with diplomatic status. The SVR is divided into three specialist fields: gaining intelligence on political issues, matters of security, and technology, such as military and commercial secrets. The GRU concentrates on running agents and focuses more on Britain's nuclear and military capabilities.

6. U.S. Counter-Intelligence

It is reasonable that if the United States is running espionage operations against other countries, those same countries may be spying on the United States. Of course, from the U.S. perspective, if the United States is carrying out espionage, it is considered necessary for reasons of national security. If, however, other countries run espionage operations against the United States, they are seen to be acting improperly, violating international law, and must be stopped. This, of course, is the standard way of thinking for all nation-states, and not simply the U.S. Counter-intelligence (CI) – the business of catching enemy spies – has long been a part of the intelligence world and has deep roots in the United States.[49]

Every year thousands of people apply for jobs in American intelligence, and only a relative handful are asked to take the next step, which is to send in a detailed background form. From this handful, only a selected few are invited to Washington for interviews and many who reach this stage fail to pass the polygraph test or other hurdle in the hiring process. A prospective penetration would probably fail to pass the security screening, although there are a few cases where security checks have failed. Most of these cases involved employees already on board, rather than new hires. Thus, it seems unlikely that there would be a payoff for an intelligence service trying to penetrate American intelligence by using this strategy.[50] The more probable way to infiltrate an intelligence service is to recruit an agent who is already a member of the target service. Most professional intelligence officers would, however, recognise immediately that they were being targeted and would not fall for the ploy unless their superiors decided to have the intelligence target pretend to go along with the recruitment to see what develops. Although this works in fictional espionage stories, it is unlikely to be productive in reality. Other efforts to penetrate a hostile intelligence service involve defectors or 'walks-ins', intelligence officers who seek to flee their own country or to work for a foreign service. The evaluation and debriefing of defectors is also another important aspect of counter-intelligence operations.[51]

For the purposes of research and analysis it is fundamental to both intelligence and counter-intelligence missions that there exist a store of knowledge concerning the personalities, past operations, structure, and activities of other nations´ intelligence and security services.[52] Only with such knowledge can positive intelligence collection operations be planned and conducted effectively. Likewise, only with such knowledge can effective penetration and disruption and neutralisation activities be conducted. The neutralisation of the activities of hostile intelligence services can be accomplished by various means. Penetrations of a hostile service can be used not only to gather information but to damage the service's

[49] Johnson, Loch K., *op cit.,* p. 78.
[50] Douglas, Hugh (1999): *Jacobite Spy Wars: Moles, Rogues and Treachery*, Phoenix Mill, Sutton.
[51] Herrington, Stuart A. (1999): *Traitors among U.S.: Inside the spy Cather´s World*, Novato, C.A., Presidio Press
[52] Eisendrath, Craig R. (ed.) (1999): *National Insecurity: U.S intell after the Cold War,* Philadelphia, Temple University Press.

operations. A second method of neutralising a hostile intelligence service is by passing information to a third country that will lead that country to take action against the officers and agents of the hostile service. On other occasions the recipient of the information may itself be a hostile state. Another method of neutralization entails running double agents. Double agent operations often are initiated after a member of the armed forces or government employee reports an approach made by a foreign intelligence officer.[53]

7. The Co-Operative Gamble

The counter-intelligence demands of adversarial, asymmetric intelligence liaison are extraordinarily high. In sum, when democracies engage in adversarial liaison with the intelligence services of hostile powers, special risks are usually involved. An adversary interested in tactical bartering will likely seek to use the intelligence relationship to further its own ends; its 'sources' must therefore be treated as suspect. Moreover, any exposure of the 'devil's bargain' could bring serious domestic or international political fallout unless threat levels are publicly perceived as very high.[54] When engaging in a bilateral relationship, experienced intelligence services 'run the traps' to make sure that there are no unknown beneficiaries involved that might make the arrangement effectively multiparty. This basic counter-intelligence effort may get short shrift if needs are pressing and time short, as in the months following the terrorist attacks of 9/11.[55]

Because of the sensitivities involved, intelligence services are usually reluctant to make public the success arising form close cooperation. In some counter-intelligence cases, however, where services are less reluctant to talk publicly and where open discussion of the cases is sometimes possible after the cases are closed, more information is available.[56] The most common and important form of cooperation is information sharing, but economic factors also play an important role in encouraging co-operation. Costs though are not the only limitation on a nation's ability to fashion an extensive intelligence network. Particular skills are also required and can take a long time to refine. Geography is important, too. No state, not even those with a long history of intelligence activity, have all the requisite resources for perfect or even near-perfect global coverage. A final reason- but unspoken- reason for intelligence liaison is that it may enable a country to spy on its own partner. The intelligence services of other nations, even friendly ones, may for instance still be used for the purpose of stealing technology or economic data for the advancement of their economic interests. Nation-states have also traditionally been lenient with foreign intelligence officers operating on their soil, and tougher on their own citizens that may be working for another country. [57] However useful in some respects, intelligence liaison inevitably engenders an attitude of ambivalence in both parties. Ambivalence characterizes liaison partnerships for yet another reason: concern that the allied intelligence service may have been penetrated by a common adversary. While understanding and enjoying the benefits of sharing, both sides are careful to protect both their own intelligence sources (the names and locations of agents) and methods (the specifics of

[53] Hulnick, *op cit*., p. 158.
[54] Wirtz, James J.: "Constraints on Intelligence Collaboration: The Domestic Dimension", *International Journal of Intelligence and Counter-intelligence,* Vol. 6, No. 1 (Spring 1993), pp. 85-99.
[55] Wannall, W. Raymond: "Undermining Counter-intelligence Capability", *International Journal of Intelligence and Counter-intelligence*, Vol. 15 (2002), p. 328.
[56] Hulnick, Arthur S.: "Intelligence Cooperation in the post-Cold War Era: A new Game Plan", *International Journal of Intelligence and Counter-intelligence,* Vol. 5, No. 4 (1992), p. 457.
[57] Johnson, *op cit.,* p. 79.

their most advanced espionage techniques). The most important reason for countries to share their intelligence information is the threat felt by the sharing partners with respect to a common adversary and a belief that by combining their resources, both parties may better understand the dangers they face (even if the threat assessment of both parties does not always prove entirely congruent). Threats and the perception of their imminence inevitably change with time.[58] Since the end of the Cold War, international organisations, particularly the United Nations and the North Atlantic Treaty Organisation, have also played an important part in US foreign policy. The UN has received less information from the U.S. intelligence community over the years than has NATO, although according to the Aspin-Brown commission, the United States still provides most of the information the UN uses to support its activities.

When UN and NATO missions overlap, as they did in Bosnia in the early 1990s, the intelligence community provides one level of classified information to NATO participants and a less detailed version to UN participants.

8. Problems and Solutions

Major concerns in counter-intelligence relate to how organisational responsibilities adversely affect professional skills and institutional culture, as well as the fragmentation that leaves large gaps in the Intelligence Community's overall counter-intelligence coverage. Law enforcement techniques that work against criminals seldom work against intelligence officers and agents. In the U.S., the F.B.I. predominately uses three methods against criminals: telephone taps, informers in criminal circles, and heavy-handed interrogations. Intelligence officers/agents and terrorists have motivations and goals that differ dramatically from those of criminals. Intelligence officers and agents are normally well financed by their governments, and terrorists may often have wealthy non-state organisations behind them. Foreign intelligence officers tend to be better educated and trained for years in espionage techniques, thereby being very able at evading detection. Managers of terrorist operations are also adept at executing their plans.

Counter-intelligence relations between separate agencies can often be conflict-ridden. The solutions to both of these problems are responses to (i) organisational incompatibilities between law enforcement and counter-intelligence operations, and (ii) fragmentation in counter-intelligence coverage. The need to resolve these issues are good enough reason for the creation of a national counter-intelligence service. For the purpose of brevity, it can be referred to by the acronym NCIS. Such an organisation must have coordinating authority over all counter-intelligence operations within Intelligence Community components. The national manager for counter-intelligence must also be given responsibilities for providing support to all departments and agencies at the national level. The national manager for counter-intelligence must also maintain a comprehensive picture of all relevant counter-intelligence targeting of foreign intelligence services. Finally, the NCIS must ensure that it has available the record of all counter-intelligence cases as possible sources for instructional material.

United States counter-intelligence is functional but not defective. Its triad of three essential functions are: protecting secrets, frustrating attempts by foreign intelligence services

[58] *Ibid*., p. 78.

to acquire those secrets, and catching Americans who spy for foreign intelligence services. Counter-intelligence is not being effectively conducted by U.S counter-intelligence agencies today. In fact, it has rarely been effectively conducted.

CIA officers tend to put other activities under the rubric of counter-intelligence. One adequate response would be the protection of intelligence collection operations by tightening up tradecraft and vetting sources more carefully. (CIA operations officers like to split counter-intelligence into 'offensive' measures, primarily recruitment and double agent operations, and 'defensive' measures, such as surveillance of personnel.

The relevant prevailing law in the U.S. is based primarily on the 1917 Espionage Act (now 18 US Code 794) which requires that four elements be proven before as espionage conviction can occur: The accused person must (1) knowingly communicate or deliver to (2) a foreign entity (3) material related to national security with (4) intent to injure the United States, for the advantage of the foreign entity, or for personal gain. For a counter-intelligence service, attempting to develop and prove all four parts, absent a confession or catching the suspect 'in the act', is an extraordinarily difficult task.[59]

Even when all four elements appear to have been developed, the government faces the additional problem of the right of 'discovery'. This threat of exposure of secret information obtained by the defence under discovery motions is termed 'greymail'. In 1980, Congress, at the urging of the counter-intelligence community, provided some relief from greymail by passing the Classified Information Procedures Act (CIPA), which allows the government to present the material ex parte and in camera to the judge, that is, secretly, without the defence present.[60] But this does not relieve the government from giving the defence classified information that is directly relevant, and fear of exposure of this information still constrains counter-intelligence agencies and government prosecutors.

President Clinton, in presidential Decision Document 24, reshuffled and renamed several counter-intelligence coordinating committees. Notably, after each major intelligence scandal, counter-intelligence coordination improves between agencies, but rarely lasts.[61] Some of the reforms have also improved inter-agency communication, but basic bureaucratic behaviour consistently precludes developing an efficient counter-intelligence system. As a result, an examination of its component parts shows U.S. counter-intelligence to be indeed broken. Bureaucratic rivalries and operational realities show that a truly effective U.S. counter-intelligence program cannot be brought about without a sea change in American political attitudes.[62]

Conclusion

After terrorism, the greatest threats to national security are undoubtedly the activities of foreign intelligence organisations. Within the U.S. alone, intelligence officers and agents from

[59] *U.S. Espionage Act*, (15 June 1917), at http://www.firstworldwar.com/source/espionageact.htm. Ammended to: 18 USC 793, 794. Also see: http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html.
[60] Classified Information Procedures Act PL 96-456, at http://www.fas.org/irp/offdocs/laws/pl096456.htm
[61] *Presidential Decision Directive on U.S. counter-intelligence effectiveness,* at http://www.fas.org/irp/offdocs/pdd24.htm
[62] Wettering, *op cit*., p. 265.

more than 140 (of 191) nations are operating and attempting to acquire sensitive U.S. defence and commercial information, using both traditional and new intelligence tradecraft.[63] Further complicating the task of counter-intelligence, foreign intelligence services are deviating from the traditional practice of placing operatives under official cover in their embassies, consulates or trade missions. Instead, they are tasking defence attaches, émigrés or visiting students, businessmen, scientists and researchers to respond to specific information requests or exploit 'targets of opportunity' that they come across, with a key target at present being advanced technologies. Foreign intelligence officers and agents recruit company insiders, form joint ventures and even engage in 'dumpster diving' for discarded data, resulting in billions of dollars being lost to hostile economic intelligence activities.[64] Whilst the counter-intelligence elements of organisations such as the F.B.I. and MI5 can respond simply by increasing the number of people working in these fields, due to the sheer scale of the problem, it would be impossible to expect all of their activities to be successful. The increasing financial and operational focus of intelligence and security services on terrorism, has allowed for a favourable environment to blossom for hostile foreign intelligence services. Security services are undoubtedly overstretched dealing with terrorism alone, and therefore it comes as no surprise that the foreign intelligence services of countries such as Russia and China have increased their activities within countries such as the U.S. and U.K. Further exacerbating this counter-intelligence dilemma are the various shortcomings of counter-intelligence practices. In an environment in which less of a focus has been placed on counter-intelligence, it is therefore of even greater importance that counter-intelligence practices be made as efficient as possible in achieving their objectives in a favourable manner. To view counter-intelligence simply in terms of its core objectives would be wrong, as it is essential that a balance be struck between security and operational effectiveness. Draconian counter-intelligence measures may unnecessarily screen out valuable, talented and much needed intelligence officers, or make inefficient, at the risk of national security, the flow of information within and between intelligence and security services. One of the steps towards alleviating the difficult demands of counter-intelligence would be an emphasis on joint activities with foreign intelligence services. This once again places an emphasis on the flow of information, but national counter-intelligence bodies would be rightfully cautious in assessing to the fullest the sensitivity of the information that is being shared. As has been demonstrated on many occasions, no foreign intelligence or security service can place its full trust in the loyalty or reliability of another country. Even the closest of allies, despite their outward and explicit denial, will inevitably seek to acquire information on one another through their respective intelligence and security apparatuses. This therefore further complicates the task of counter-intelligence, whilst at the same time providing the potential for valuable benefits. Another element of contemporary counter-intelligence that cannot be ignored is the information revolution. Those tasked with protecting the cover of intelligence employees can no longer follow the practices used during the Cold War. Doing so will lead to instances in which the identities of hundreds of intelligence and security personnel can be identified via the Internet. Notably, the failure in fully understanding modern day technological hurdles, played an important part in the Italian authorities being able to accurately trace the locations and activities of several CIA operatives that had had been working on the most sensitive of missions in Italy.[65] Innovative solutions and a re-think of traditional methods will be required to maintain effective cover and stealth in a 21st century operational environment. In sum, if the problems of contemporary counter-intelligence are to be dealt with, it is critical that those

[63] House Judiciary Subcommittee on Immigration, Border Security & Claims: *Hearing on Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage,* (September 15, 2005).
[64] Federal Bureau of Investigation, *Focus on Economic Espionage,* in: http://www.fbi.gov/hq/ci/economic.htm
[65] Whitlock, Craig, "Italians Detail Lavish CIA Operation", *Washington Post*, 26 June 2005.

responsible for ensuring national security rapidly respond to the shortcomings of their present day efforts. Too great of a focus on terrorism at the price of neglecting other critical threats, as is the case today, can indeed be a bad thing.