Geneva Centre for the Democratic Control of Armed Forces (DCAF)

Occasional Paper – №16

Fighting the Pre-eminent Threats with Intelligence-led Operations

Fred Schreier

GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF ARMED FORCES (DCAF)

OCCASIONAL PAPER – №16

Fighting the Pre-eminent Threats with Intelligence-led Operations

Fred Schreier

ISBN 978-92-9222-099-0

DCAF Occasional Papers are detailed, theoretical studies on core issues of Security Sector Governance. DCAF Occasional Papers can be downloaded free of charge from the DCAF website at www.dcaf.ch/publications

Table of Contents

List of Abbreviations and Acronyms 3

Introduction 5

1. The Pre-eminent Threats 6

1.1 The Risks and Threats of Transnational Organised Crime 7
1.2 The Risks and Threats of the Proliferation of WMD 16
1.3 The Risks and Threats of Transnational Terrorism 25

2. What Is Intelligence? 47

2.1 How Is Intelligence Produced? 49
2.2 What Types of Intelligence Services Are There? 52
2.3 What Are the Problems for, and the Limits of, Intelligence? 54
2.4 Why Is Intelligence Important for Fighting the Pre-Eminent Threats? 57

3. The Application of Intelligence and the Contributions of Intelligence-led Operations to Fighting the Pre-eminent Threats 60

3.1 Intelligence-led Policing 60
3.2 Criminal Intelligence Analysis 66
3.3 Intelligence-led Counter-trafficking 67
3.4 The Contributions of Intelligence-led Operations to the Fight Against the Pre-eminent Threats 74
3.5 New Ways of Combating Organised Crime 88

4. Patterns and Problems of Intelligence Cooperation 90

4.1 Intelligence and Law Enforcement Cooperation 90
4.2 Cooperation With and Within the EU 92

5. Intelligence-led Operations and Democratic Oversight 102

5.1 The Need for Tighter Democratic Control, Supervision and Oversight 102
5.2 The Problems Accruing to Democratic Control, Oversight and Accountability 104
5.3 Clear Redefinition of Accountability 107
5.4 Executive Control and Supervision 109
5.5 Reinforcing the Checking Mechanisms Outside the Executive 111
5.6 Improved Complaints Mechanisms 112

6. Key Recommendations 113

7. Select Bibliography 117

List of Abbreviations and Acronyms

BTWC	Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons
BW	Biological Weapon
CBNR	Chemical, Biological, Nuclear and Radiological
CCTV	Closed Circuit Television
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CNE	Computer Network Exploitation
COMINT	Communications Intelligence
CRYPINT	Cryptology Intelligence
DDoS	Distributed Denial-of-Service
DNA	Deoxyribonucleic acid containing genetic instructions
ECHR	European Court of Human Rights
ECIM	European Criminal Intelligence Model
ELINT	Electronic Intelligence
EMP	Electro-Magnetic Pulse
EU	European Union
Eurojust	European Investigation and Prosecutorial Cooperation Mechanism
Europol	European Police Office
EUSC	EU Satellite Centre
FATF	Financial Action Task Force of the OECD
FISINT	Foreign Instrumentation Signals Intelligence
GCHQ	Government Communications Headquarters of the UK
GPS	Global Positioning System
HERF	High-Energy Radio Frequency
HEU	Highly enriched uranium
HPM	High-Power Microwave
HUMINT	Human Intelligence
IAEA	International Atomic Energy Agency
ICT	Information and Communication Technology
IDEW	Improvised Directed Energy Weapon
IED	Improvised Explosive Device
ILP	Intelligence-led Policing
IRA	Irish Republican Army
IMINT	Imagery Intelligence
INTDIV	Intelligence Division of the EU Military Staff
Interpol	International Criminal Police Organisation
IT	Information Technology
JHA	Justice and Home Affairs
MASINT	Measurement and Signatures Intelligence
NBC	Nuclear, Biological and Chemical
NCIS	National Criminal Intelligence Service of the UK
NLW	Non-lethal weapons
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security and Cooperation in Europe
OSINT	Open Source Intelligence
PJC	Police and Judicial Cooperation Matters
R&D	Research and Development
RDD	Radiological Dispersion Device

RFID	Radio Frequency Identification Device
SCADA	Supervisory Control and Data Acquisition System
SIGINT	Signals Intelligence
SITCEN	Joint Situation Centre of the EU
SCCOPOL	Section Centrale de Coopération Opérationelle de Police in France
SOCA	Serious and Organised Crime Agency of the UK
TED	Transient Electromagnetic Device
TELINT	Telemetry Intelligence
THB	Trafficking in Human Beings
TOC	Transnational Organised Crime
TV	Television
UAV	Unmanned Aerial Vehicle
UNDP	United Nations Development Program
UNODC	United Nations Office on Drugs and Crime
UNSCOM	United Nations Special Commission for Inspections in Iraq
WMD	Weapons of Mass Destruction

Fighting the Pre-eminent Threats with Intelligence-led Operations

Fred Schreier

Introduction

This paper discusses the role of intelligence, intelligence services and intelligence-led operations as crucial components of the efforts to counter the new risks, dangers and threats to states and their population.

The end of the Cold War and globalisation has not only brought a multiplication of actors, sources of conflict and means to fight. Indeed, globalisation, accelerating techno-logical innovation, growing interdependence and vulnerability of modern states has dramatically enhanced the number and diversity of risks, dangers and threats. The fact that these are increasingly transnational in nature, originate more and more often from non-state actors and appear and mutate ever more quickly, renders the fight against them more difficult. This is particularly true for the unholy trinity of transnational terrorism, proliferation of weapons of mass destruction (WMD) and transnational organised crime (TOC) that have become the pre-eminent security challenges confronting the world and the new intelligence priorities. TOC is growing in volume, geographic reach and profitability, and is well positioned for further growth because it does, in many ways, have the most to gain from globalization. Growth and spread of TOC increase the risks of proliferation of WMD and, with it, of catastrophic transnational terrorism as proliferants and terrorists collude ever more symbiotically with TOC groups to move money, men and materials around the globe.

The more the international order is threatened by asymmetric warfare of Islamistic terror networks, the more the threat perception will become multifaceted and chaotic if more actors can acquire WMD. These developments not only diminish the predictability of risks and dangers. The more diffuse and unpredictable the situation and the threat perception, the more difficult it will become to clearly distinguish between external and internal, civilian and military threats to a country, and between the strategic, operational or tactical levels of risks and dangers.

More than ever before intelligence is the pre-requisite for all measures that aim at the effective prevention, disruption and suppression of these threats. But countering the pre-eminent threats from multiplying non-state actors that operate clandestinely requires more than just intelligence services. These threats can only be effectively counteracted, disrupted, pre-empted and prevented when the operations of all security sector organisations that are mandated to deal with them are *intelligence-driven* or *intelligence-led*. This requires a paradigm shift in national security strategy that not only entails a 'whole of government' approach and multilateral engagement, but a radical new approach with more intensive

collaboration, interaction and information exchange by these organisations with the agencies of the intelligence community.

This paper (1) sketches the main threats currently confronting all states. Part (2) elaborates what intelligence is and explains why intelligence is key to counter the expanding array of threats more effectively. Part (3) shows the application of intelligence and the contributions of intelligence-led operations to the fight against the pre-eminent threats. Part (4) explores patterns and problems of intelligence cooperation. In part (5) some of the implications which intelligence-led operations may have for democratic control, supervision, oversight and accountability are indicated. The paper ends with a list of key recommendations

1. The Pre-eminent Threats

The threats of yesterday were predominantly of the symmetric type: static, predictable, homogenous, hierarchical, rigid and resistant to change. The new threats are more of the asymmetric type: dynamic, less predictable, networked, fluid, self-organising and constantly adapting and evolving.

These changes have far-reaching consequences for ensuring national security. The old strategic approach of *risk avoidance*, which served states relatively well in terms of ensuring national security against predictable state adversaries no longer works. Risk avoidance is no longer financially affordable; it is also no longer adequate against the threats posed by the growing number of less predictable, more evasive and clandestinely operating non-state actors. Hence, budgetary constraints and the new threats force states to move from the *prevention of the known* to the *management of the unknown*: from risk avoidance to *risk management*. Thus, old concepts of threat analysis have to be supplemented by *risk analysis* and *vulnerability analysis*. This means that resources for ensuring national security are now allocated on the basis of *threats or risks* and *national vulnerabilities*. Threats are measured in terms of the likelihood and severity of the consequences, while risk is accepted as equalling threat divided by vulnerability.

The activities of the unholy trinity of the pre-eminent threats are transforming the international system, upending the rules, creating new players, and reconfiguring power in international politics and economics. The changes in the last decade of the 20th century not only empowered terrorists, proliferants and criminals, but at the same time weakened the agencies in charge of fighting them. The networks of transnational terrorists, proliferants and TOC thrive on international mobility and their ability to take advantage of the opportunities that flow from sanctuaries and separate marketplaces into sovereign states with borders. For terrorists, proliferators and TOC, frontiers create opportunities and convenient shields. But for the government officials chasing them, borders still too often represent obstacles. The privileges of national sovereignty are turning into burdens and constraints on governments. Because of this asymmetry in the global clash between governments, transnational terrorists, proliferators and TOC,

governments are systematically losing – everywhere. But ultimately, it is the fabric of society that is at stake.

1.1 The Risks and Threats of Transnational Organised Crime

Definitions of *organised crime* abound,[1] but analytical sharpness is hard to find.[2] Most definitions fail in what they are designed to do: delineating the intended phenomenon. Many contain redundant or overlapping components – a violation of the parsimony principle. Moreover, they vary according to the needs and experiences of different investigative or research organisations. And because legal definitions do not explain its impetus, scale and impact, organised crime has been described in Clausewitzian terms as *the pursuit of profit as a continuation of business by criminal means*.[3]

This indicates that 'organised crime' remains a deeply contested terrain. There is no universally accepted definition, neither of *organised crime* nor of *transnational organised crime*. Since 1994, researchers define TOC to include offences whose inception, prevention and/or direct and indirect effects involve more than one country.[4] It is criminal activity coordinated across national borders. More precisely, a crime is considered transnational if it is committed: (1) in more than one state; (2) in one state but a substantial part of its preparation, planning, direction or control takes place in another country; (3) in one state but involves an organised criminal group that engages in criminal activities in more than one state; and (4) in one state but has substantial effects in another state.[5]

Due to the fact that TOC groups vary considerably in terms of structure, strength, size, geographical reach, scope and diversity of their operations, the UN sought a suitably broad definition in its *Convention against Transnational Organised Crime*. Article 2(a) defines an organised criminal group as: "… a structured group of 3 or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences … in order to obtain, directly or indirectly, a financial or other material benefit".[6] This definition has 4 *mandatory* and 7 *optional* criteria with at least two of the latter needing to be applicable to qualify a criminal group or crime as 'organised crime'. The *mandatory* criteria are: (1) collaboration of three or more people; (2) for a prolonged or indefinite period; (3) suspected or convicted of committing serious criminal offences; and (4) with the objective of pursuing profit and/or power. The *optional* criteria are: (1) having

---

1 See, for example, the more than 100 definitions collected by Klaus von Lampe in *Organized Crime in Europe*, at: www.organized-crime.de/dtindex.htm

2 James O. Finkenauer, "Problems of Definition: What is Organized Crime?", *Trends in Organized Crime*, 2005, Vol. 8, No. 3, p. 63. Petrus C. van Duyne, "Organizing cigarette smuggling and policy making, ending up in smoke", *Crime, Law & Social Change*, 2003, No. 3, pp. 263-283.

3 Antonio Maria Costa, "Trafficking: Transnational Crime and International Terrorism", *United Nations Office on Drugs and Crime*, at: www.unodc.org/unodc/en/speech_2002-12-06_1.html

4 Gerhard O.W. Mueller, "Transnational Crime: Definitions and Concepts", *Transnational Organized Crime*, Vol. 4, Autumn/Winter 1998.

5 See also United Nations Convention against Transnational Organized Crime, 2000, Article 3.

6 The United Nations Convention Against Transnational Organized Crime, adopted by the UN General Assembly on 15 November 2000, at: www.unodc.org/unodc/en/crime_cicp_convention.html No UN Convention has ever had so many signatories immediately upon its opening for signature and less than a month after its formal adoption by the UN General Assembly.

a specific task or role for each participant; (2) using some form of internal discipline and control; (3) using violence or other means for intimidation; (4) exerting influence on politics, the media, public administration, law enforcement, the administration of justice or the economy by corruption and other means; (5) using commercial or business-like structures; (6) engagement in money laundering; and (7) operating on the international level. Article 2(b) states that a 'serious crime' means "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty".[7] But what constitutes 'serious crime' is not stated in the convention.

The crimes of trafficking in illicit drugs, weapons, munitions, and in human beings, as well as child pornography, money laundering and mass vehicle thefts are all likely to satisfy the definition of 'serious crime'. Likewise, the illegal trade or proliferation of chemical, biological, nuclear weapons and technology, posing a serious global security threat, constitute a serious crime.[8]

The definition encompasses a broad spectrum of criminal groups in all continents engaged in what Moisés Naím[9] calls the 5 wars of globalization: the illicit markets for *arms, drugs, human beings*, *intellectual property* and *money*. TOC is not the only participant in illicit activities for there are also petty criminals and terrorists that engage in such activities. However, TOC is the most organised. What makes it more dangerous than other criminality is its highly organised or entrepreneurial method in the following widely varying activities:

Organised Crime Activities

- Corruption
- Intimidation
- Theft
- Kidnapping
- Arms trafficking
- Smuggling
- Labour racketeering
- Illicit telemarketing
- Sex exploitation
- Pornography
- Bribery
- Coercion
- Robbery
- Piracy
- Drug trafficking
- Counterfeiting
- Loan sharking
- Computer & IT crime
- Slavery
- Money laundering
- Extortion
- Assassination
- Hijacking
- Illicit trading
- Illicit technology transfer
- Fraud
- Gambling
- Electronic mail schemes
- Prostitution
- Environmental crimes

TOC groups act *conspiratorially* in all activities and possess certain characteristics which may include, but are not limited to:[10]

- In at least part of their activities they commit violence or other acts which are likely to intimidate, or make actual or implicit threats to do so;

7 Ibid.
8 These offences are covered by a number of other conventions on proliferation of WMD.
9 Moisés Naím, *Illicit. How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*, New York, Doubleday, 2005.
10 See: *Overview of the Law Enforcement Strategy to Combat International Organized Crime*, U.S. Department of Justice, April 2008, p. 2.

- They exploit differences between countries to further the objectives, enriching their organisation, expanding power and avoiding detection and apprehension;
- They attempt to gain influence in government, politics and commerce through corruption as well as through legitimate means;
- They have economic gain as their primary goal, not only from patently illegal activities but also from investment in legitimate business; and,
- They attempt to insulate both their leadership and membership from detection, sanction and prosecution through their organisational structure.

1.1.1 Structures and forms of organised crime

TOC is a dynamic process that is constantly changing over time as it adapts to an ever changing environment and to new opportunities for crime to resources and skills available. TOC profits from globalization in taking tailored advantage of the accelerating technological innovation, improvements in modes of communication and transport, of increased travel, trade, rapid money movements and IT. There is no single structure under which TOC operates. The self-perpetuating associations of individuals operating internationally for the purpose of obtaining power, influence, monetary and commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and violence, are characterised by a large degree of *fluidity* and *structural complexity*. As opposed to the popular mafia stereotypes, they use diverse forms and sizes of clusters, network structures and groups, as suited for their diverse forms of illegal activities and as dictated by emerging opportunities across the globe. Today, network-like structures seem to be more prevalent than ethnic, region or family-based groups.

Results of a pilot survey conducted by the UNODC of 40 selected TOC groups in 16 countries confirmed the existence of this structural fluidity in the 5 typologies that were identified and related to the observed groups: standard hierarchy, regional hierarchy, clustered hierarchy, core group, and criminal network.[11] The major Colombian cartels provide a good example of a complex network type structure: compartmentalised, mimicking large multinational corporations, with the home-based president and vice-presidents taking decisions, monitoring and managing acquisition, production, transportation, sales and finances for the drug-trafficking business and the overseas cells handling the import, storage and delivery of the product, as well as money laundering.

TOC groups tend to use legitimate import-export firms, service industries, whole-sale markets, the construction and food industry, waste disposal, multinational financial institutions and other businesses as cover for their activities. Some TOC groups function primarily in the illegitimate sector such as drug trafficking; others span both the legitimate and illegitimate sectors of the economy. Sometimes a

[11] United Nations, Office on Drugs and Crime, *Global Programme against transnational organised crime: Results of a pilot survey of forty selected organised criminal groups in sixteen countries*, September 2002.

TOC organisation only nests itself inside a larger business; at other times it actually controls it. There are legal firms that engage in white-collar crime such as banks specialising de facto in the facilitation of money laundering and tax evasion. Furthermore, there are licit enterprises founded, in whole or in part, by money obtained from organised crime. TOC groups reach out to individuals with the best skills and expertise that exist that are necessary to facilitate criminal ventures. These individuals involved include lawyers, accountants, IT experts, hackers, bankers, or members with expertise in the stock market, money laundering, transportation, etc. The border line between the activities of white-collar or corporate crime and TOC is becoming fuzzier.

The massive privatisations of the 1990s in the former USSR and in Eastern Europe have given many TOC groups a large and important foothold in the economies of their countries, which is still used for their further development in other parts of the world.[12] Crime syndicates and networks are exploiting new ventures and markets, particularly in areas of accelerating economic growth and opportunity. A complex, more often symbiotic and clientelistic than confrontational relationship is developing between TOC groups, the state, and society.

Different developments are underway: (1) there may be more individuals and smaller groups empowered by high-tech computer skills and telecommunication capabilities that do not require the infrastructure or protection of syndicates to engage in cyber crime. (2) The trend of greater cooperation among criminal organisations may be replaced by one in which large international crime groups are able to produce, acquire, move, market and distribute drugs and other contraband without reliance on outside brokers. (3) There may also be more large, interactive networks of small, highly specialised independent organisations that cooperate on the basis of comparative advantage and in joint ventures. (4) TOC groups having access to weapons arsenals may displace arms brokers that still dominate the grey arms markets by establishing sophisticated acquisition, transportation and financial networks to facilitate evasion of international sanctions. In addition, (5) ever more TOC groups are likely to take advantage of the scientific and manufacturing advances to produce new synthetic drugs and more high-quality counterfeit products.

[12] The picture becomes even more complex with the involvement of the state apparatus, political parties, the military, and intelligence services. The decline in totalitarian states, and the peace dividend that has enabled the rapid drawdown of military and security forces, has driven many former members of security and intelligence services and of specialists in the armed forces into the TOC business. For TOC, this influx of professional security, intelligence, police and military know-how has meant a quantum jump in sophistication. This to such an extent that TOC groups can in some cases outsmart law enforcement and judicial investigations because they have better techniques, better equipment, and much more resources. It is clear that there are still large gaps in the intelligence on various aspects of TOC. These gaps jeopardise the ability to keep pace with TOC threats as they emerge and develop.

1.1.2 The risks and threats posed by transnational organised crime

TOC poses a threat to all nations and is a fundamental threat to democracy, the rule of law and human rights. TOC disrupts free markets, drains national assets and inhibits the development of stable societies. When it escalates, economic development, political independence, the environment, as well as human and global security are all threatened. As practiced today, TOC undermines civil society, political systems and the sovereignty of states by normalizing violence, graft, and by introducing a corruptive cancer into political structures. It distorts market mechanisms, including some government regulatory activity, and deprives consumers and producers of the benefits of fair, free, safe and secure economic and commercial systems. In extreme cases, whole legitimate economic sectors are dislocated by commerce based on illegal activities, subverting loyalties from the nation-state and habituating individuals to operate outside the legal framework. Moreover, TOC undermines the integrity of the banking and financial systems, the commodities and securities markets as well as cyberspace. It degrades environmental systems through the evasion of environmental safeguards and regulations.[13] It burdens societies with the enormous social and economic costs of illegal drugs. Moreover, TOC hinders the progress of, and foreign investments in, economies in transition and developing countries.

TOC poses *strategic threats* that can affect or destabilise strategically important states:

- TOC groups have penetrated and control significant positions in the global energy and strategic materials markets that are vital to national security interests of a number of major powers. They corrupt the normal workings of these markets, and have a destabilising effect on national interests, as well as on foreign and economic policy.[14]

- TOC groups provide logistical and other support to terrorist groups, to certain intelligence services and to some rogue governments. Each of these groups is either targeting strategically important nations or otherwise acting in a manner that goes against the national interests of these and other states.[15]

---

[13] Major environmental impacts already arise from the clandestine trade in endangered species, unsustainable logging and mining, and destruction of crops in favour of drug production. UNODC, *Annual Report*, Vienna, UNODC, 2005, pp. 36-37. The relationship between deteriorating natural systems and TOC is not unidirectional: climate change and resulting environmental crises seem likely to create sudden scarcities and even social upheaval which TOC groups will be well-positioned to exploit.

[14] One of the examples is the criminal organisation of Semion Mogilevich, which exerts influence over large portions of the natural gas industry in parts of the former Soviet Union. He was arrested by Russian police on tax related charges in January 2008 while other members of his group remain at large.

[15] Victor Bout, formerly a Soviet GRU major who became arms dealer and embargo buster, supplied weapons to the Taliban and Al Qaeda, made huge arms shipments to Armenia for the Nagorno-Karabakh war and to African conflicts in Angola, Cameroon, Central African Republic, Democratic Republic of Congo, Equatorial Guinea, Kenya, Liberia, Rwanda, Sierra Leone, Sudan and Uganda. He was in business with anyone, irrespective of ideology, and often contracted on both sides of a war. In May 2006, when 200,000 AK-47 assault rifles went missing in transit from Bosnia to Iraq, one of Bout's airlines was the carrier. He was arrested in Bangkok in March 2008 and charged with conspiring to sell millions of dollars worth of weapons, including surface-to-air missiles, to the Revolutionary Armed forces of Colombia (FARC) – another terrorist organisation. Leonid Minin, an Ukrainian turned Israeli businessman, is another person who is part of a new generation of highly sophisticated post-Soviet criminals and arms dealers.

- TOC smuggling and trafficking activities seriously compromise border security and at times national security. Smuggling of contraband and counterfeit goods cost businesses large sums annually, while the smuggling and trafficking in human beings (THB) leads to exploitation that threatens the health and lives of human beings.[16]

- TOC exploits national and international financial systems to move illicit funds and to launder money. They transfer billions of dollars of illicit funds annually through the financial systems of many nations, and corrupt financial and non-financial intermediaries globally to continue this practice.[17]

- TOC uses cyberspace to target victims and the critical national infrastructure of developed nations. They steal huge amounts of money at a cost to consumers and the national economy, jeopardise the security of personal information, the stability of business, national infrastructures, and the security and solvency of financial markets.[18]

- TOC is manipulating national and international securities exchanges and perpetrating sophisticated frauds using the Internet, wire services and mail. They use fraud to steal from investors and rob consumers and government agencies of huge sums of money without the need to set up a base of operations in any one location.[19]

- TOC corrupts public officials by legal and illegal means in ever more nations. It is successful in systematically corrupting public officials around the world in order to operate and protect their illegal operations, and to increase their sphere of influence, including in countries of vital strategic importance to major powers.[20]

- TOC uses violence as a basis for power. This poses a threat to the physical security of the public, the economic well-being of people and neighbourhoods, and the ability of law enforcement to investigate their

---

16 In March 2006, one of the most successful alien smugglers of all time, Cheng Chui Ping, better known as "Sister Ping", was sentenced to 35 years in prison for her role in leading an international alien smuggling organization, which smuggled more than 1000 aliens into the US. She also hired armed thugs from the Fuk Ching, a vicious gang in New York's Chinatown, to transport her customers and ensure they paid their smuggling fees.

17 The Bank of New York (BNY) case is an early example of such a scheme. In 2000, Berlin and his wife Edwards, Russian *émigrés* and she a BNY vice president, pleaded guilty to conspiracy to commit money laundering and to operate an unlawful banking and money transmitting business, and to aid and abet Russian banks in conducting unlicensed banking activities in the US. During more than 3 years, some $7 billion flowed through the BNY accounts they had established to third-party transferees around the world.

18 One example is the DSW case that arose in 2005 when DSW Inc. and 8 other major US retailers reported that information from 1.4 million credit cards and 96,000 checks used by customers had been stolen. The indictment of 5 August 2008 alleges that 11 hackers – 3 US citizens, 1 Estonian, 3 Ukrainians, 2 Chinese, 1 from Belarus and 1 known only by an alias online – installed "sniffer programmes" to capture card numbers, passwords and account information, then concealed the data in computer servers that they controlled in Eastern Europe and the US. The charges brought against them were computer fraud, wire fraud, access-device fraud, aggravated identity theft and conspiracy.

19 US Postal Inspectors have been working with law enforcement in Nigeria, Canada, The Netherlands and the UK to stop scam artists that have been preying on North American consumers via mail or over the Internet passing counterfeit checks and money orders. Since the global counterfeit initiative targeting these international criminal groups began in January 2007, 77 arrests have been made and more than 600,000 fake cheques valued at over $2.5 billion have been seized. Telemarketing fraud is yet another means by which organised criminals fraudulently obtain funding.

20 For example, former Ukrainian Prime Minister Pavel Lazarenko defrauded and extorted $44 million from Ukrainian citizens and proceeded to launder $20 million of these funds through US banks.

crimes. It also threatens national interests and national policies when violence increases the power of such groups to operate globally.[21]

Trafficking in human beings (THB) is a particularly despicable activity of TOC. THB is closely tied to other illicit trades. They function the same way, by means of highly effective, decentralised mobile networks, and they feed on each other. Supply and demand, risk and return, are the trafficking industry's main drivers. Unless and until THB faces diminished incentives – less demand, lower margins, higher risks – it is more or less futile to talk about other remedies.

THB is also political – it has infiltrated governments. The enormous incentives associated with the profits involved in the trade drive this criminalisation of politics and public service. THB is also political in another sense: public opinion and politicians define many of the expectations and constraints that shape anti-trafficking efforts. These include the definition of what is criminal, the severity of penalties for different crimes and the budgets allocated to combating these crimes.

THB is keeping up with the explosive growth of *people smuggling*. Both are lucrative activities of TOC and internationally agreed criminal offences. But THB is distinct from people smuggling. It does not require an illegal border crossing nor is it necessarily transnational such as in cases of internal trafficking, whereas people smuggling always involves an illegal border crossing. While victims of THB are regarded as commodities, individuals who are smuggled across borders are more like clients who pay for the service. However, there is much crossover and overlap between these two categories.

1.1.3 The impact of transnational organised crime

The impact of TOC in Europe is manifest in the rise of personal insecurity, ever larger losses to property, increasing drug use, in particular by unemployed youth, other deleterious impact on youth, growing violations of labour law by illegal immigrants, the spread of venereal disease, HIV/AIDS and related problems through THB, increasing health costs for society, serious health risks due to environmental crimes, cybercrime and fast growing financial losses, and in the enormous profits made that continue to fuel and sustain TOC.

In Europe, TOC and corruption problems are most severe in countries with large economies, those that are closest to the Balkans, Eastern Europe and the Mediterranean and those with major ports. Some countries have the full range of TOC, whereas in other countries TOC groups focus primarily on money laundering and on receiving profits from crimes committed in other regions.

Outside of Europe, TOC groups thrive from terrorism and civil war. In some 30 countries, groups engaged in armed rebellion against the government finance their

[21] See the August 2007 killing of 6 Italian men as they left a pizzeria in Duisburg, Germany, committed by the Italian 'Ndrangheta crime syndicate, the roughly 6,000 members of which specialize in kidnapping and political corruption, and are engaged in drug trafficking, murder, bombings, counterfeiting, gambling, frauds, thefts, labour racketeering, loan-sharking and alien smuggling

insurgency and terrorist campaigns, in whole or in part, with income generated by taxing the production of drugs or by being directly involved in trafficking. The fuel that keeps civil wars going changes. Sometimes it is illicit drugs, sometimes Colton, diamonds, other scarce materials, or products like oil.

Among the various forms of TOC, the trade in illicit drugs[22] carries the largest societal, political and economic consequences, and is threatening the fabric of societies through addiction, crime and disease.[23] It exacerbates corruption in already weak states, impairing their economic and political functioning, thus deterring foreign investments. Drug cartels challenge and may supplant governments. Moreover, through its linkages to terrorism and insurgency, the drug trade is an increasing threat to regional and international security in a most traditional military sense.

TOC is eager to profit from every aspect of these wars, even the human tragedy of refugees. In order to leave combat zones, refugees often rely on TOC traffickers to get them to safety. Others make use of TOC smuggling networks to leave the country for economic or other reasons, hoping to rebuild their existence in more promising economies. Whether the cause is war, poverty or unemployment, the displacements tend to drive the best and the brightest to foreign shores, often into communities formed by ethnic diasporas.

The numbers are staggering. As many as 1 million men, women, and children are trafficked every year across national borders by criminal groups; of these, about 80 percent are said to be female, and up to half minors. The majority of victims are trafficked into commercial sex exploitation, adding to the already existing millions living under modern forms of slavery.[24]

1.1.4 The profits gained by transnational organised crime

While it is notoriously difficult to estimate the profits gained, these are enormous. The illicit global economy or global black market is estimated to amount to $1 trillion.[25] The trade in illicit drugs is said to have reached a value of $322 billion in

---

22 In Afghanistan, the production of opium, the raw material for heroin, soared in 2007, rising 34 percent above the already record levels of 2006, according to the *Afghanistan Opium Survey 2007* of UNODC. Production reached 8,200 tonnes, a vast narcotics harvest of unprecedented size in modern times and unseen since the opium boom in China during the 19th century. That output represented 93 percent of the world's supply and outstripped global demand, which is estimated at 4,500 tonnes. Much of the opium ends up on European streets as heroin, the hardest of drugs. Drug abuse also rose rapidly in Afghanistan as the number of addicts, both adults and children grew. The size of Afghanistan's opium economy exceeded half the country's licit gross domestic product (53 percent), according to the Survey. The total export value of opiates in Afghanistan reached about $4 billion, a 29 percent increase compared to 2006. See also: United Nations, Office on Drugs and Crime, *Annual Report 2008, covering Activities in 2007*, Vienna, 2008.

23 Every year illegal drugs kill about 17,000 Americans. See: "Actual Causes of Death in the United States, 2000", *Journal of the American Medical Association*, Vol. 291, No. 10, 10 March 2004, pp. 1238, 1241. Illicit drugs are estimated to represent about $160 billion in social and economic costs and $67 billion in direct costs for the US annually. See: Drug Enforcement Agency, "Speaking Out Against Drug Legalization", at: www.dea.gov/demand/speakout/director.htm

24 The International Labour Organization (ILO) estimates that 12.3 million people throughout the world are enslaved in forced labour, bonded labour, sexual servitude, and involuntary servitude at any given time.

25 See: www.havocscope.com/ with counterfeit and piracy amounting to $533 billion, the global drug trade $322 billion, environmental goods $57 billion, trafficking in humans $44 billion, consumer products $60 billion, and trafficking in weapons $10 billion.

2005[26] – equivalent to a GDP ranking of 30th in the world, measured against national economies, and roughly 75 percent of the total GDP of Sub-Saharan Africa.[27] However, by far the biggest part of the illicit trade is not the drug trade, which amounts to some 32 percent, but the 53 percent of counterfeiting and piracy.[28] Environmental goods constitute 6 percent of illicit trade, THB 4 percent,[29] consumer products another 4 percent, and the weapons trade 1 percent.[30] And the placing of stolen assets abroad has now reached unprecedented levels.

At the same time, TOC also provides certain goods and fulfils certain services for which there is public demand – services and goods that a given state or society does not want to provide for reasons of politics, public health, religion, ethnic or cultural norms. Once again, the motive of TOC is profit. But to think of a clear line between good and bad is to fail to capture the reality of trafficking today. Governments will never make progress if all their attention is placed on the suppliers and not the citizens whose appetite for such services and goods creates the incentives that make it all possible. Any solution needs to include the customer – 'normal' members of their communities who have habits, needs and behaviours that feed the demand that makes illicit traffickers rich.

1.1.5 Outlook

The greater regional integration and worldwide interdependence of national economies make it easier for TOC to operate on an international scale and blend their operations into legitimate economic activity. Improvements in transportation infrastructure and modalities increase volume, speed and efficiency of smuggling and commercial transaction by crime. And the resources and opportunities available to TOC have increased exponentially along with the magnitude of their potential profits.

The scope and power of TOC groups has unsettled governments and international organisations around the world. By classifying it as manifesting a threat to national security, G-8 leaders have long recognised that the threat posed by TOC transcends the sum of individual crimes committed. However, illicit trade is more about transaction than products. States usually parse the illicit trades into separate product lines, and thus task different government agencies or international organisations with fighting each distinct trade. But the trades are no longer distinct. Illicit traders move in and out of product lines as economic incentives dictate and practical considerations permit. Governments need to shed

---

[26] United Nations Office on Drugs and Crime Annual Report 2005, p. 4. It was higher in retail price than the GDP of 163 out of the 184 countries for which the World Bank held data. See: www.drugwarfacts.org/economi.htm

[27] This estimate only includes, revenues and not law enforcement costs ($67 billion in the US alone in 2005) or indirect social and economic costs ($160 billion in the US in 2005). See: The Library of Congress, Congressional Research Service, "Transnational Organized Crime: Principal Threats and US Responses", 20 March 2006, p. 5.

[28] US businesses estimate that counterfeiting costs them between $200 and $250 billion per year in lost sales. Interpol, "The Impact and Scale of Counterfeiting", at: www.interpol.com/Public/News/Factsheet51pr21.asp

[29] Perhaps $10 billion annually. Moisés Naím, "It's the Illicit Economy, Stupid", *Foreign Policy*, No. 151, Nov/Dec 2005, pp. 95-96.

[30] See. Havocscope.com, op. cit.

the illusion that the different illicit trades can be kept separate and start thinking of illicit traders as economic agents who have developed functional specialties, not product niches. Instead of distinguishing between traffickers, smugglers, pirates, etc., governments better think of illicit traders in the roles they truly perform: investors, financiers, entrepreneurs, bankers, brokers, marketing managers, transporters, warehouses, wholesalers, logistics managers, distributors and more. When states consider illicit traders as opportunistic, profit-minded economic agents, it becomes clear that these should have no reason to stick to just one product.

Economic and commercial crimes and more major fraud against governments will continue to grow as a percentage of revenue for those involved in TOC. The need to corrupt and co-opt civil authorities will expand hand-in-hand with the ambitions of the various TOC groups. Now, more than ever, money and power will be the incentives. Hence, given the nature and breadth of the threat, governments need *intelligence* on the illicit traders engaged in TOC and THB in order to go about their business in the best interests of their citizens.

1.2 The Risks and Threats of the Proliferation of WMD

Proliferation refers to the diffusion of weaponry and technology. It is a process in which a new type of weaponry is introduced into an area where it was previously not available. The most dangerous is the proliferation of WMD. There is no treaty or customary international law that contains an authoritative definition of WMD. Instead, international law has been used with respect to the specific categories within WMD, and not to WMD as a whole. The term WMD is customarily used to embrace all nuclear, biological and chemical weapons, irrespective of particular characteristics, potency and possible application. Some years ago radiological weapons have been added. But there are important differences among these weapons. So much so that lumping together all of these weapons in one category of WMD is misleading, since nuclear weapons, in view of their tremendous destructive potential, are in a class all to themselves.

The development and use of WMD is governed by international conventions and treaties, though not all countries have signed and ratified them.[31] The proliferation of WMD and their means of delivery such as ballistic missiles constitute a threat to international peace and security and a growing danger to all states. The EU recognises "the proliferation of WMD as potentially the greatest threat to our security"[32] and, in December 2003, agreed on a Strategy Against Proliferation of WMD with the stated objective of preventing, deterring, halting and, where possible, eliminating proliferation programmes of concern worldwide.[33] Adopted by the UN Security Council in 2004, UN Resolution 1540 recognises the threat

[31] (1) Partial Test Ban Treaty; (2) Outer Space Treaty; (3) Nuclear Non-Proliferation Treaty (NPT); (4) Seabed Arms Control Treaty; (5) Comprehensive Test Ban Treaty (CTBT); (6) Biological and Toxin Weapons Convention (BWC); and (7) Chemical Weapons Convention (CWC).

[32] A Secure Europe in a Better World – European Security Strategy, Brussels, 12 December 2003.

[33] Strategy, § 2.

posed to international peace and security by nuclear, chemical and biological weapons, as well as their means of delivery. It calls upon greater effort by nations to limit the proliferation of such weapons.[34]

While the international treaty regimes and export controls arrangements have slowed down the spread of WMD and delivery systems, a number of states and non-state actors have sought or are seeking to develop such weapons. The risk that terrorists will acquire nuclear, chemical and biological weapons, radiological or fissile materials and means of delivery adds a new critical dimension to this threat. Opportunities for mass-casualty terrorist attacks using chemical, biological or nuclear weapons will increase as technology diffuses and weapons programmes expand.

1.2.1 The risks and threats of nuclear proliferation

Nuclear weapon designs and related technology can spread from one country to another, either directly from state to state, from state to non-state actor, from non-state actor to state, or through clandestine or criminal supplier networks – such as the notorious activities of Abdul Qader Khan,[35] the 'father' of the Pakistani nuclear bomb, who was at the centre of two illicit supplier networks: one bringing sensitive technology into Pakistan, and another one transferring it from Pakistan to Iran, Libya, North Korea and elsewhere. Thus, threats may also arise from the illicit transfer or theft of sensitive design information, for example, a Chinese bomb design sold by the Khan network to Libya.[36]

The spread of nuclear technologies and expertise is generating concerns about the potential emergence of new nuclear weapon states and the acquisition of nuclear materials by terrorist groups. Ongoing low-intensity clashes between India and Pakistan continue to raise the spectre that such events could escalate to a broader conflict between these nuclear powers. The possibility of a disruptive regime change or collapse occurring in a nuclear weapon state such as North Korea raise questions regarding the ability of weak states to control and secure their nuclear arsenals.

---

[34] …all States shall refrain from supporting by any means non-state actors that attempt to acquire, use or transfer nuclear, chemical or biological weapons and their delivery means, at: www.ub.org/News/Press/docs/2004/sc8076.doc.htm

[35] A shrewd businessman, Khan saw potential for financial gain between his network of clandestine suppliers and a burgeoning market for nuclear arms. North Korea, Iran, Iraq, Syria and Libya were foremost on his list. But he also met with potential customers in Egypt, Saudi Arabia, Sudan, Malaysia, Indonesia, Algeria, Kuwait, Myanmar and Abu Dhabi. In 1997, at a series of meetings in Istanbul and Casablanca, Khan made a deal to sell Libya a complete bomb-making factory for approximately $100 million. Seif Islam, Gadhafi's elder son, approached the British SIS with the offer to talk about Libyan WMD. The CIA and the British SIS held sporadic talks with the head of Libyan intelligence, Mousa Kusa. The US and the UK wanted Libya to end its WMD programme, and Gadhafi wanted assurances that in return economic sanctions would be removed. In August 2003, SIS got a tip about a shipment leaving Khan's factory in Malaysia for Libya, and US spy satellites tracked the shipment. In October 2003, the German flagged cargo vessel *BBC China* was seized by the US and Italy.

[36] An old 22 kiloton uranium implosion device. See: Christoph Wirz & Emmanuel Egger, "Use of nuclear and radiological weapons by terrorists?", *International Review of the Red Cross*, Vol. 87, No. 859, September 2005, p. 499.

In addition to these concerns, new political-military developments could further erode the nuclear 'taboo'. A nuclear-armed Iran spawning a nuclear arms race in the greater Middle East will bring new security challenges to an already conflict-prone region, particularly in conjunction with the proliferation of long-range missile systems. A number of states in the region are already thinking about developing or acquiring nuclear technology useful for the development of nuclear weaponry. This will add a new and more dangerous dimension to what is likely to be increasing competition for influence within the region, and competition among outside powers anxious to preserve their access to energy supplies and to sell sophisticated conventional weaponry in exchange for greater political influence and energy agreements. Future asymmetries in conventional military capabilities among potential rivals might tempt weak states to view nuclear weapons as a necessary and justifiable defence in response to the threat of overwhelming conventional attacks. If the number of nuclear-capable states increases, so will the number of countries potentially willing to provide nuclear assistance to other countries or to terrorists. The potential for theft or diversion of nuclear weapons, materials, and technology also would rise.

Another threat exists with weapons-grade fissile materials being stored in hundreds of military and civilian sites located in nearly 60 countries. The total worldwide stockpile of highly enriched uranium (HEU)[37] is some 1,600 tonnes, which is theoretically enough to build 130,000 nuclear weapons. The stockpile of plutonium[38] separated from spent fuel is over 480 tonnes, enough to manufacture 110,000 nuclear bombs. Fissile material used in nuclear reactors cannot easily be used to produce nuclear weapons, or only in particular circumstances. However, less than a quarter of these stockpiles are secured according to the 'gold standard'.[39] Some 60 tonnes of HEU, theoretically enough to build over 1,000 nuclear weapons, is in civilian use or storage throughout the world, most of it associated with research reactors and about half of it outside of the US and Russia.[40] Today, roughly 135 operating research reactors in 40 countries still use HEU as fuel, and an unknown number of shutdown or converted research reactors still have HEU fuel on-site.[41] Many of these facilities do not have enough fuel on-site for a bomb, but some with 20 kg of HEU or more do. Most of these installations have very modest security – in some cases, no more than a night watchman and a chain link fence. Some of these are located on university campuses, where providing serious security measures against attack would be difficult.

---

37 Weapon-grade uranium in which the percentage of fissionable isotope U-235 has been increased from the natural level of 0.7 percent to some level equal or greater to 20 percent, usually around 90 percent.

38 Plutonium can also get lost: 69 kg at the Tokai-Mura plutonium fuel production facility, Japan, in 1994, 8 kg in 1996, and 206 kg in 2003; 19 kg at Sellafield, UK, in 2004, and 29.6 kg in 2005.

39 Protection existing as in Fort Knox, the US Army Armor School and training base, where the US gold reserves are stored.

40 David Albright & Kimberly Kramer, "Civil HEU Watch: Tracking Inventories of Civil Highly Enriched Uranium", in *Global Stocks of Nuclear Explosive Materials*, Washington D.C., Institute for Science and International Security, 2005, at: www.isis-online.org/global_stocks/end2003/tableofcontents.html

41 Government Accountability Office, Nuclear Nonproliferation: DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium in Civilian Research Reactors, GAO-04-807, Washington D.C., GAO, 2004.

The physical protection of fissile materials refers to controls designed to prevent sabotage, attacks, thefts or other criminal acts. This is most important for military fissile materials. By ensuring the detection, prevention and recovery of missing materials, physical security controls also seek to discourage illicit uses. Physical protection involves more than just guards, gates and fences at particular facilities. It also requires reliable personnel to design and implement controls, employing people who have both technical competence and professionalism, which entails extensive background checks and vetting before recruitment, and thorough training after. This is lacking in many countries, even in the US where personnel of private security companies, among them also Israeli companies, that are responsible for the security of nuclear power plants, have been found who have not been vetted.

Because all states apply and implement their own standards, their chain of physical security is only as strong as its weakest link. This is why the concerns that the theft of fissile material somewhere could jeopardize security elsewhere have inspired international initiatives in this area. However, many obstacles hinder progress in strengthening physical security. More international cooperation is inhibited by governmental concerns over the erosion of sovereignty, legal liability, budgetary constraints, etc. Such obstacles also hinder the development of stronger multi-lateral standards or expanded roles for international institutions. And the lack of serious consequences for non-compliance with existing standards further erodes both the effectiveness and credibility of those standards.

While some consider the uranium enrichment route less likely for proliferation than the plutonium option, the latter is definitely more difficult to realise. There is considerable HEU held by nuclear powers, and those interested in assembling a weapon might well look to gathering HEU from these sources through stealth, bribe or other illegal efforts.[42] Russia has endorsed the goal of nuclear non-proliferation, recognising that it could be a target of potential proliferants. Security for Russia's nuclear warheads and materials has improved substantially over the last years. Nuclear experts and workers are now paid a living wage, on time, reducing the incentives to divert material or sell knowledge. And Russian security services are more pervasive than they were a decade ago, also at nuclear sites. Far more daunting, however, is the prospect of tracking unknown quantities of weapons-grade material – which even Russian and other authorities have been unable to account for with accuracy – and the international movement of experts from other countries of the former USSR, from South Africa, Iraq and Libya. The end of the privileged status that these scientists once enjoyed is incentives to would-be proliferators and terrorist groups alike.

[42] IAEA states that 25 kg of HEU (U-235) or 8 kg of plutonium Pu-239 are the minimum amounts required for a 20 kiloton explosion = 20,000 tons of TNT. However, a group with more sophisticated technology could build the same weapon with as little as 5 kg of HEU or 3 kg of plutonium – the size of a soccer ball. Uranium enrichment is a complex industrial process requiring facilities that house sophisticated equipment, and consume large quantities of electricity. However, a nation or group that possesses an amount of HEU sufficient to make a nuclear weapon may be able to amass the engineering and scientific skills to actually build the weapon.

There is an additional concern. It is widely expected that global reliance on nuclear power will increase in the next decades, as the price of fossil oil and gas goes up and the greenhouse gas-free nuclear energy becomes more attractive.[43] If so, there will be a greater demand for uranium and plutonium fuel, leading to expanded use of enrichment. As reprocessing of spent fuel will allow a drastically better use of the energy content of the original uranium or plutonium fuel, there may be a demand for more reprocessing plants. An increased flow of fissile material and larger stockpiles increase the risk of misuse and diversion. Technically, all 12 countries possessing an enrichment or reprocessing capability can produce reactor fuel or bomb-grade material or both.[44] The larger the existing stocks, the greater the danger of leakage and misuse.

Other concerns challenging the intelligence services are the buyers of uranium ore, the activities of shipping companies that might be transporting weapons parts or fissionable materials, and the governments of powers known to sell missiles and related materials. Until recently, the major concern was the movement of material and expertise from Russia's cooperation in the development of Iran's nuclear, weapons and missile programmes, and China's sale of missiles to Pakistan and Iran. Today, the most immediate concerns are North Korea's sales and Iranian delivery of missiles and related technology.

1.2.2 The risks and threats of proliferation of chemical weapons

While many states have the capability to make chemical weapons, few have the motivation to do so. Such weapons remain repugnant to the overwhelming majority of states, and have demonstrated their dubious utility as weapons of war. Nevertheless, there is little to suggest that chemical weapons will not be sought and used again – as seen in the case of the Tokyo subway attack by the religious sect Aum Shinrikyo. Since the late 1990s, US and Israeli intelligence services have reported on the production of Sarin and VX by Syria.

The factors that are conducive to proliferation of chemical weapons are: (1) the relative simplicity of technologies for producing poisons at the present level of development of the chemical industry; (2) the ease with which dual-use technologies, equipment, and materials suitable for producing chemical weapons can be acquired; (3) the economic profitability and relative ease of carrying out chemical weapon development; and (4) the difficulty to detect such programmes. The dual-use nature of the commodities and technology that go into the manufacture of chemical weapons remains a persisting concern and a source of uncertainty in any estimates of arsenal size or latent capabilities to manufacture such weapons.

---

43 See: Nader Elhefnawy, "The Next Wave of Nuclear Proliferation", *Parameters*, Autumn 2008, pp. 36-47.

44 The plutonium obtained from spent reactor fuel can be used to make bombs though its isotopic composition is not ideal.

New risks of proliferation also arise with the research and development of so-called non-lethal (NLW) or less lethal weapons, using the latest advances of the pharmaceutical industry. Research on NLWs has been prompted partly by the 2002 incident at the Dubrovka Theatrical Centre in Moscow during which at least 125 hostages were killed by an opioid that was used by Russian Special Forces to put Chechen hostage takers to sleep.[45] There are concerns that NLWs may cause deaths either through deliberate or inadvertent misuse. Terminology complicates the NLW issue. Chemical or biological-based substances may be referred to as bioregulators, incapacitants and riot control agents. Currently, research on, and tests of, non-lethal chemical and biological agents are under way in several countries to determine the effective radius of action of such agents, and the best means of delivery.

1.2.3 The risks and threats of proliferation of biological and toxin weapons

The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, BTWC, requires parties "not in any way to assist, encourage, or induce any state, group of states or international organisations"[46] to manufacture biological agents for use as weapons. But unlike nuclear weapons, biological weapons do not require unique ingredients that are objects of arms control. Hence, regrettably, export-import controls are not enough to prevent the proliferation of these weapons. The large biological weapon programme discovered in Iraq – a party to the BTWC – after the 1991 Gulf War relied to a large extent on imported agents and growth material, some sent by mail from US and European laboratories.[47] But not only do dangerous biological agents travel internationally unaided by man, they also exist in nature inside countries all over the world.

The rapid advances or innovations in the life sciences influence the availability of information and expertise required to make toxins and genetically modified viruses and other pathogens. As the scientific, engineering and industrial uses of biological organisms grow throughout the world, states and non-state actors will increasingly be able to produce volumes of lethal biological agents, engineer new pathogens and develop effective delivery systems, should they so decide. The interest in acquiring biological weapons may be based on the following reasons: (1) to offset an opponent's conventional or nuclear military advantage;[48] (2) high economic profitability and relative technical ease of carrying out biological warfare programmes; (3) dual-use of technologies, equipment and materials suitable for

---

45 J. Hart, F. Kuhlau & J. Simon, „Chemical and biological weapon developments and arms control", *SIPRI Yearbook 2003: Armaments, Disarmament and International Security*, Oxford, Oxford University Press, 2003, pp. 659-666.

46 The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, BTWC of 1972, is the first multilateral treaty banning the acquisition and retention of an entire category of WMD.

47 The Reagan administration had authorised at least 40 shipments of specific biological agents to Iraq from the American Type Culture Collection, a big scientific institute that has cultures of every type of exotic disease in the world.

48 Biological weapons, which kill people but leave infrastructure intact, could become the "poor man's neutron bomb".

creating biological weapons – for example, the capability of using them both for peaceful and for military purposes; (4) the possibility of the covert existence of military biological warfare programmes connected with the lack of clear distinctions between offensive and defensive operations; and (5) the difficulties of detecting relevant infrastructure.

US intelligence assessments have highlighted biological weapons proliferation concerns about such nations as North Korea and Syria.[49] However, apart from Russia, Iraq is the only other country confirmed in recent years to have had an offensive biological weapons programme. Inspectors from UNSCOM uncovered sufficient evidence of a covert bio-weapon programme to compel Iraq to admit that it had produced and weaponised biological agents – anthrax, aflatoxin and botulinum toxin.[50] The Iraqi as well as the Soviet programmes went undetected for years, underscoring the problem of relying solely on national technical means to monitor compliance with the BTWC. A related concern is that a state might decide to share its biological weapon capabilities with non-state actors.

Concern also arises from the possible misuse or negative impact of biodefense programmes, such as their potential to provide cover for the illegal development or maintenance of biological weapons-related expertise. Yet another risk of biological weapons proliferation is occasioned by the prevalence, and in some cases the lack of control over the circulation, trade and transfer of components for acquiring these weapons – strains of causative agents of dangerous infectious diseases, dual-use equipment, nutritive media, and technological information.

What makes the prevention of biological weapons proliferation a particularly formidable task is that the biotechnical revolution[51] is using the blueprints of all life – DNA – to create new forms of life and modify existing ones. There are three trends in the biotechnology revolution: (1) It offers tools to unravel the complex genetic codes and functions of organic molecules upon which all life depends: the science of genomics – a powerful weapon for understanding how diseases affect the body in order to develop new countermeasures. At the same time, it can also aid in developing more precisely targeted and therefore more effective weapons. New sequencing technologies coupled with bioinformatics are exponentially increasing the speed and accuracy of genomics. Entire 'genomic encyclopaedias' for various bacteria, viruses, fungi and higher animals, including man, will soon be available. Numerous viruses, bacteria, and higher order of forms have already been geno-typed. (2) New tools for precisely targeting and

---

49 "Testimony of Carl W. Ford, Jr.", Senate Foreign Relations Committee Hearing on Reducing the Threat of Chemical and Biological weapons, 19 March 2002. And: "Testimony of General Thomas A. Schwartz", Senate Armed Services Committee, 5 March 2002. US Arms Control and Disarmament Agency, *Adherence to and Compliance with Arms Control Agreements,* Washington D.C., US Department of State, 1998.

50 United Nations, Report of the Secretary-General on the Status of the Implementation of the Special Commission's Plan for the Ongoing Monitoring and Verification of Iraq's Compliance with Relevant Parts of Section of Security Council Resolution 687(1991), 11 October 1995. www.un.org/Depts/unscom/sres95-864.htm Security Council Resolution 687 also called on Iraq to ratify the BTWC, which it finally did in June 1991.

51 There is a revolution in biotechnology in the sense of the revolution in computer and information processing power. The US Military Critical Technology List reports technological doubling rates of 6 months for basic genetic engineering, the Human Genome Project, bio-regulators, and other biotechnical applications. This can result in enhanced infectivity and virulence, novel toxins and regulatory peptides, greater antibiotic resistance and novel genetic weaponry as a distinct possibility.

manipulating organic molecules, commonly referred to as genetic engineering or recombinant DNA technology, allow gene transfer and subsequent cloning to produce new 'species' with multiple pathogenicities – such as plague with myelin toxin or endemic, non-pathogenic bacteria with regulatory peptides. Soviet scientists have successfully transferred the myelin toxin, which degrades the central nervous system, into the plague bacteria *yersinia pseudo-tuberculosis*, managed to engineer *tetracycline resistant anthrax* and extensively studied *regulatory peptides*.[52] (3) The third trend operationalises the first two. Production technology is rapidly advancing, enabling more efficient and compact means for manufacturing and distributing biological material. Genetic decoding, molecular manipulation and efficient mass production enable designer vaccines, antidotes and other therapies. As bioscience becomes more computational and less about wet labs, and as genomic data becomes easily available on the Internet, at some point, it will be possible to design vaccines on the laptop. Conversely, the same trends could combine to enable designer bio-weapons for those that have the will, knowledge and resources to apply the technologies, creating *binary weapons*, *novel designer genes* and life forms, *stealth viruses* and *host-swapping viruses*. The other side of the coin is, fortunately, that the same technologies may also produce novel antibiotics, *broad-spectrum immune enhancers*, rapid and precise detection, *new antivirals* as well as *metabolic-based defences*.

Potential problems may emanate from the rapid developments in the life sciences, including new understandings of genes and proteins that could eventually outpace national and international efforts to prevent, control or manage hostile uses of biology. In recent years, materials and technologies have become accessible to many more researchers and technicians through the pharmaceutical and biotechnology industries. Inevitably, scientific advancements in biotechnology and the wide spread of facilities capable of producing biological agents make it more difficult to prevent the development of biological weapons, complicate efforts to ensure their non-production and elimination of stocks, and make it exceedingly difficult to pinpoint potential biological threats.

1.2.4 The risks and threats of proliferation of radiological weapons

Radiological weapons – with the controversial exception of depleted uranium munitions[53] used by the US in the 1991 Gulf War, in the 1999 Balkans wars and

---

[52] Ken Alibek & Stephen Handelman, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told from inside by the Man Who Ran it*, New York, Delta, 1999. And: Alexander Kouzminov, *Biological Espionage. Special Operations of the Soviet and Russian Intelligence Services in the West*, London, Greenhill Books, 2005.

[53] Is uranium that has a reduced proportion of the isotope U-235, and is mostly made of U-238. Depleted uranium (DU) is very dense, at 19.05 g/cm^3 it is 1.7 times that of lead, and easier to work with than the slightly denser tungsten. Because of its density, it is used as kinetic energy ammunition. The weapons include 120, 105, 30, and 20 mm rounds for use by tanks, APC cannons, aircraft and naval guns, cruise missiles, and bunker-buster bombs (GBU-28, 15, 24, 27, 31 and 37, and AGM 130C with F-15, B-2, A-10, AC-130 Spooky airplanes, Apache helicopter AH-64, and cruise missiles). These range from 200 g in a 20 mm projectile, 4.5 kg in 120 mm penetrators to 1.5 tonnes in the BLU-109 penetrator delivered with the B-2 bomber. DU is pyrophoric and burns on impact providing a self-sharpening penetrator through conventional armour and other target material. 304 tons of DU munitions were fired during the 1991 Gulf War, some 11 tons in the Balkans Wars, and more than in these alone in Afghanistan. About 70-80 percent of all DU munitions remain buried in the soil. Up to 20 states have weapons incorporating DU in their arsenals. They include the US, the UK, France, Russia, Greece, Turkey, Israel, Saudi Arabia, Bahrain, Egypt, Kuwait, Pakistan, Thailand, and

again in Afghanistan 2002 to 2003 and in Iraq 2003 – have not been deployed or used in conflict for both practical and ethical reasons. Neither have radiological weapons yet been used to deliberately cause harm by irradiating a population or an environment. So far, Chechen militants are the only known group that has attempted to use a Radiological Dispersion Device (RDD).[54] A few countries have pursued the development of radiological military weapons, only to abandon these efforts in favour of more practical and effective weapons.[55]

While nuclear waste is a less likely proliferation option for weapon source material, potential radiological weapons materials exist in hundreds of thousands of locations worldwide. There are an estimated 10 million radioactive sources in existence around the world. But even in the US, there is no effective mechanism either at the federal or state level for tracking throughout their lifecycle the numbers and locations of the estimated 2 million radioactive sources.[56] Hundreds of plutonium, americium and other radioactive sources are stored in dangerously large quantities in university laboratories and other facilities. In all too many cases they are not used frequently, resulting in the risk that attention to their security will diminish over time. At the same time, it is difficult for the custodians of these materials to dispose of them.[57]

Significant amounts of radioactive materials are stored in laboratories, food irradiation plants, oil drilling facilities, medical centres and many other sites worldwide. Among those, there are at least 8 powerful radioactive elements that pose a serious threat if sufficient quantities were used for RDDs: (1) *Americium-241* – an alpha and gamma ray emitter with a half-life of 432.7 years, used in smoke detectors and in devices that find oil sources, to detect petroleum deposits,

---

Taiwan. DU ammunition is manufactured in 18 countries. Because DU is radioactive, producing alpha and beta particles and gamma rays, and is chemically toxic, polluting water supplies and producing other health hazards, some states and NGOs have asked for a ban on the production and military use of DU weapons.

54 In November 1995, Chechen militants under Commander Basayev placed a small quantity of caesium 137 in Moscow's Izmailovsky Park. Rather than disperse the material, however, the Chechens used the material as a psychological weapon by directing a television news crew to the location and thus creating a media storm. The material in this incident was thought to have been obtained from a nuclear waste or isotope storage facility in Groznyy. In December 1998, the pro-Russian Chechen Security Service announced it had found a dirty bomb consisting of a land mine combined with radioactive materials next to a railway line. It is believed that Chechen militants planted the device.

55 In 1950, the US considered using radiological weapons in Saudi Arabia as a way to prevent a Soviet invasion force from using the Saudi oil or destroying the oil fields. The CIA ultimately recommended against the use of radiological weapons (according to a declassified 1950 CIA memorandum). By 1953, the USSR developed a radiological warhead for the R-2 ballistic missile, which was retired as nuclear warheads became available. In 1987, Iraq pursued development of a radiological weapon. The purpose was to combine the effectiveness of conventional aerial munitions with the spreading of radioactive materials as a means of 'area denial' to be used in the final stages of the Iran-Iraq War. 3 prototypes were made, based on modified 'Nasser 28' aerial bombs. The results of the tests were disappointing in that the majority of the radioactive material concentrated on the crater with a sharp decline in the radiation level at a relatively short distance away. Moreover, the weapon was found to be impractical because the radioactive isotopes in the weapon would decay quickly, rendering it useless within a week after manufacture. Furthermore, it was found that for the radioactive material to spread, weather conditions had to be ideal. The development was discontinued as Iraq concentrated on chemical, nuclear, and biological weapons programs. Radiological weapons are widely considered to be militarily useless. Such a weapon is of no use to an occupying force, as the target area becomes uninhabitable. Moreover, area-denial weapons are generally of limited use to an attacker, as it slows its rate of advance. Finally, like biological weapons, radiological weapons can take days to act on the opposing force. They therefore not only fail in neutralizing the opponent, but they also allow time for massive retaliation.

56 Government Accountability Office (GAO), *U.S. and International Assistance Efforts to Control Sealed Radioactive Sources Need Strengthening*, GAO-03-638, August 2003, p. 9.

57 In the US, for example, only the Department of Energy (DoE) is authorized to recover and transport them to permanent disposal sites

to calibrate instruments, in industrial gauges, distance-sensing devices and medical diagnostics; (2) *Californium-252* – an alpha and strong neutron emitter with a half-life of 2.65 years, used to detect oil deposits; (3) *Cesium-137* – a gamma ray emitter with a half-life of 30 years, used in moisture-density, levelling and thickness gauges, to treat diseases, sterilise food and medical equipment, detect oil deposits and for well-logging in the drilling industry; (4) *Cobalt-60* – a beta and strong gamma ray emitter with a half-life of 5.27 years, used in industrial gauges and radiography, to treat diseases and cancer, to sterilise spices, food and medical equipment and to detect hidden flaws in structures; (5) *Iridium-192* – a beta and gamma ray emitter with a half-life of 73.8 days, used to detect hidden flaws in structures, metal parts, pipes and welds, and for treatment of diseases; (6) *Plutonium-238* – an alpha ray emitter with a half-life of 88 years, used to generate low-levels of power for devices which must function without direct maintenance for timescales approximating a human lifetime in spacecraft and interplanetary probes, and to power artificial heart pacemakers; (7) *Strontium-90* – a beta ray emitter with a half-life of 29 years, used to generate low-levels of nuclear power supplies for use in remote locations, weather stations, space vehicles, navigational beacons, electron TV-tubes, in industrial thickness gauges and for treatment of eye disease; and (8) *Radium-226* – an alpha and gamma ray emitter with a half-life of 1,600 years, used in industrial gauges, luminescent paints and dials, tips of lightening rods, radiography devices, and to produce radon for cancer treatment. What makes these elements especially proliferation-prone is their combination of radioactivity levels and relative prevalence. Because of their level of radioactivity and relative facility in handling and manipulating, the weapons of choice may be Strontium-90, Cobalt-60 and Cesium-137.

1.3 The Risks and Threats of Transnational Terrorism

There is not just one form of terrorism but many, often with few traits in common. What was true of one variety is not necessarily true of another. There are more varieties today than existed some 30 years ago, and many are so different from those of the past and from each other that the term terrorism no longer fits some of them. Terrorism has been defined in many different ways, but little can be said about it with certainty except that it is the use of violence by a group for political ends, usually directed against a government. Mainly because of this, there is no internationally accepted definition of terrorism. Not even the United Nations have been able to achieve consensus on this contentious issue. While definitions focus on acts of terrorist groups, the context for understanding these acts must include the response of the target government and, in turn, the effects of that response on the political climate of the society. Among other things, the old adage that 'one man's freedom fighter is another man's terrorist' is at the root of the ongoing debate.

Nonetheless, all terrorist acts are crimes. All involve violence, or the threat of it, often coupled with specific demands. And violence is ever more indiscriminate. Its purpose is to demonstrate the ineptitude of the government and as a tool to intimidate and coerce populations. Terrorists adopt irregular warfare methods for

one key pragmatic reason: to offset their military and organisational weaknesses. Their motives are political, and the ultimate goal is political power for the purpose of political, social, economic or religious change. The targets are mainly civilians. The actions generally are designed to achieve maximum publicity. The perpetrators are usually members of an organised non-state group, and unlike other criminals, they often claim credit for the act. Intrinsic to a terrorist act is that it is intended to produce psychological effects and fear far beyond the immediate physical damage.

Continued terrorist acts have compelled individual states to develop their own definitions for the purpose of enacting legislation to counter the terrorist threat. The politically charged term of terrorism has been used to describe a variety of acts and methods of violence. But in practice, the attempts have neither amounted to an internationally recognised classification nor to a coherent legal definition. Moreover, national experiences have not contributed to the establishment of a general European policy.[58] In addition, scholars and decision-makers disagree over whether such violence should be rationalised and legitimised. One consequence has been an inability to forge a meaningful consensus on what constitutes terrorism, which, in turn, has impeded attempts to proscribe it internationally. However, given the rising necessity to differentiate terrorism from other forms of political violence in the interest of protecting vital international community interests and values, a coherent definition of terrorism is needed, already in order to harmonise efforts and ensure closer cooperation in combating terrorist activities.

Previously, terrorism operated within limits and usually had easily identifiable ends: territory, the release of prisoners or political concessions. Now we face a terrorist threat quite different from anything experienced in the past. Since the beginning of 1990s, terrorism began to outgrow its former national and regional dimensions, has become more international and global in reach, more ideological and more strategic in its objectives. With the advent of 4th generation terrorism we witnessed with 9/11, the Bali, Madrid, London and other recent attacks, the aim is to maximise the number of casualties. This reflects a shift in the goals of the new terrorists from trying to make a political statement through violence to maximising damage to the target as an end in itself.

Of all the terrorist groups, religiously motivated ones are the most likely to resort to mass-destructive terrorism. Because such groups perceive violence to be part of an all-encompassing struggle between good and evil, religious extremism is converging with three other factors: the deliberate quest to acquire or develop WMD, a willingness to accept martyrdom, and a perception that the only 'audience' of worth is that of a deity – with the result that jihadist groups, in particular, lack the moderating influence of an external 'audience' or constituency, are more detached from 'moral norms' and other social constraints, thus are less constrained in using WMD, and more difficult to deter. Limitless in the scale of their ambitions, the

[58] See: "The Nature of Terrorism. Defining Terrorism within the EU", *Transnational Terrorism, Security & the Rule of Law,* Work package 3, Analysis of definition of EU institutions, 28 June 2007, at: www.transnationalterrorism.eu

new terrorists are not interested in extracting concessions from victims or negotiating with governments, and they will not compromise over their goals. The new terrorism in its various forms wants to convince a target population and its leadership that the stakes of a conflict are not worth the current and potential future costs. It deliberately targets the non-combatant civilian population, icons and other symbols associated with the state, the ruling government's power base or the critical national infrastructure. What they want is to destroy the way of life and the social fabric of the target society.

Transnational terrorism has manifold dimensions: security, economic, political, environmental and others that can affect the future of the planet. Today, transnational terrorism is being perpetrated in the name of an extremist Muslim cause. But it is a type which, in a future world order, could be applied by others. It signals a new era of conflict. While the numbers of lives lost due to terrorist acts in the recent past have been small by comparison to the lives lost from other causes, this can change dramatically if transnational terrorists obtain and use WMD. Senior Al Qaeda members have threatened to use, and have demonstrated the will to carry out attacks with WMD.[59] This is also the desire of various other terrorist groups.[60] Thus, past experience is not a reliable guide to what terrorists may be planning next.

1.3.1 The risks and threats of nuclear terrorism

Nuclear weapons are unique in their capacity to inflict instant loss of life on a massive scale, which gives them special appeal to terrorist. The greatest cause for fear from terrorist attack is the prospect that some terrorists come into possession of an operational nuclear weapon. Current nuclear programmes in Iran and North Korea,[61] and the nuclear arsenal existing in a destabilising Pakistan, are of major concern, as well as the prospects of weapons and fissile materials from existing nuclear powers falling into terrorist hands.

But nuclear weapons are generally located at well protected and guarded nuclear weapons storage facilities. A theft would involve many risks and great efforts in terms of personnel, finances and organisation. Without the support of insiders with local and specialised knowledge, a theft is improbable. Even if a nuclear warhead could be stolen or acquired with the help of organised crime, there are several different types of safety and security systems incorporated in a weapon, ensuring that no unwanted nuclear explosion can take place, and that successful

---

59 Bin Laden has called the acquisition of WMD a 'religious duty'. For the best available summary of al Qaeda's nuclear efforts see David Albright, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents", *Special Forum 47*, Berkeley, Nautilus Institute, 6 November 2002, and David Albright, Kathryn Buehler & Holly Higgins, "Bin Laden and the Bomb", *Bulletin of Atomic Scientists*, Vol. 589, No. 1, January/February 2002.

60 There is little doubt in this regard. Terrorist websites, which now number over 400, are overflowing with 'doctrine' and objectives about the aim of destroying infidel populations. Were *Al Qaeda* or some other such organisation to obtain a nuclear weapon, the same doctrine that guided the 9/11 attacks would likely apply again.

61 The danger that these states would intentionally provide nuclear material to terrorists is probably far smaller than the danger of nuclear theft, for to provide the key ingredients for an act of nuclear terror would be to run the risk of being found out and facing overwhelming retaliation.

use of a stolen weapon would be unlikely.[62] Such systems will destroy critical components or render them useless if the weapon is handled improperly or if someone tries to open it.

The other option, that terrorists could build a working improvised nuclear device[63] themselves, cannot be excluded. Even a crude nuclear device is likely to produce enormous casualties. Used in an urban environment, casualties are likely to be in the order of tens to hundreds of thousands of deaths.[64]

Terrorist groups generally lack industrial infrastructure. What they most often have is funding, either covertly from nations that sponsor them or from criminal and other sources, to acquire weapons, components or fissile material on the world market. For terrorists to develop a crude nuclear device, the greatest difficulty is to obtain weapons-grade fissile material. It is difficult and very expensive to develop and manage the substantial infrastructure that is required to produce enriched uranium or plutonium in sufficient quantity for building a nuclear device. Designing a weapon, while not easy at all, is a less difficult task, since the basic information needed to design a crude nuclear explosive device is publicly available. But beyond a critical mass of fissile material, construction of a nuclear weapon requires other exotic materials; a substantial manufacturing capability; and very substantial technical expertise in building such a weapon, particularly its igniters.

Terrorists would probably prefer HEU as fissile material, because the assembly design using this material is simpler than the design relying on plutonium. Yet, the possibility of a terrorist plutonium bomb cannot be excluded, given that smaller amounts of such material are needed for it, and that knowledge about implosion designs is now more widely distributed.

The greatest unknown is how sophisticated a facility is required for construction. South Africa, Pakistan and others have already demonstrated that a Los Alamos type of operation is no longer needed. Another question also remains as to what size device could be constructed by a terrorist group. The first nuclear weapons built were on the order of 10 tons each. During the Cold War both the US and the USSR developed much smaller nuclear devices, including nuclear artillery shells,

---

62 Among these are: (1) inertial switches and acceleration sensors allowing priming only after a threshold level has been reached; (2) environmental sensing devices monitoring the trajectory, which are switching on only at a distinct ratio of the longitudinal to lateral acceleration; (3) a barometric switch, which activates the electric circuit only at a distinct height above ground; (4) a so-called permissive-action link (PAL) is needed, consisting for instance of several number codes with up to 12 digits and allowing a limited number of tries. The code has to be entered by more than one person, i.e. each person concerned knowing only part of the entire code; (5) certain types require a high energy electrical impulse.

63 For a discussion of the vast difference between a safe, reliable, efficient weapon that can be carried on a missile, and a crude, inefficient, unsafe terrorist bomb that might be delivered in a truck, see: Matthew Bunn & Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?", *Annals of the American Academy of Political and Social Science*, 607, September 2006.

64 A bomb with the explosive power of 10,000 tons of TNT, half the size of the bomb that obliterated Hiroshima, if set off in midtown Manhattan on a typical workday, could kill half a million people, and cause more than $1 trillion in direct economic damage. Devastating economic aftershocks would reverberate throughout the world. See: John P. Holden & Matthew Bunn, "Technical Background: A Tutorial on Nuclear Weapons and Nuclear-Explosive Materials", in *Nuclear Threat Initiative Research Library: Securing the Bomb*, Cambridge, and Washington D.C., Project on Managing the Atom, Harvard University and Nuclear Threat Initiative, 2002, at: www.nti.org/e_research/cnwm/overview/technical.asp

atomic demolition munitions[65] and what have been called 'suitcase nuclear weapons'.[66] While both were able to shrink the size of these weapons, the technology needed to do so is not trivial and in fact exceedingly complex. Whether a terrorist group could effectively duplicate this feat in the foreseeable future is a difficult question, about which there continues to be substantial debate. However, even before the US intervention in Afghanistan, US intelligence concluded that "fabrication of at least a 'crude' nuclear device was within Al Qaeda's capabilities, if it could obtain fissile material".[67]

There is the risk that security weaknesses could allow terrorists to steal enough material or even a nuclear device either from storage or during transportation, or to obtain these with the help of TOC. The most crucial step in preventing nuclear terrorism is to keep terrorists from acquiring access to such materials or devices – a step that requires strict implementation of physical protection measures and security routines that the US National Academy of Sciences has described as 'the stored-weapon standard',[68] wherever such devices or materials exist. Important practical measures must be put in place to limit the available sources, to increase physical security and safety where transportation is deemed unavoidable,[69] and to block terrorist access through better intelligence and security. Nonetheless, there remain possibilities of insider conspiracies to steal nuclear weapons or material, or to help outsiders to do so. El Baradei, director general of the IAEA, recently stated that "in the past 5 years, the international community has made great progress in securing these materials. But it is a race against time, and it is not yet certain who is winning".[70] Hence, the prospect of a black market in fissile materials and even complete nuclear devices cannot be discounted. Thus, export-import controls, border guard and customs enforcement activities serve vitally important roles in reducing the risk of nuclear terrorism.

Another question is whether terrorists could bring either fissile materials or an entire weapon into a target country. Presently, this is possible for both cases. The current generation of detectors will not find packages containing nuclear materials that have even the most minimal amount of lead shielding, particularly in the case

---

65 A man-portable, low-yield nuclear device weighing less than 40 kg. A Russian commission formed on 3 July 1996 investigated reports that Chechen fighters had possibly gained access to such weapons. The US had also developed about 300 Special Atomic Demolition Munitions – "backpacks" – based on its W-54 warhead.

66 See for example: "Suitcase Nukes: A Reassessment", Monterey, Center for Non-proliferation Studies, 12 September 2002, at: http://cns.miis.edu/pubs/week/020923.htm, and Nikolai Sokov, "Suitcase Nukes: Permanently Lost Luggage", Monterey, Center for Non-proliferation Studies, 13 February 2003, at: http://cns.miis.edu/pubs/week/040213.htm, also: Suitcase bomb, from Wikipedia, at: http://en.wikipedia.org/wiki/Suitcase_bomb

67 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President*, Washington D.C., WMD Commission, 2005, at: www.wmd.gov/report, p. 276.

68 See: NTI, Research Library, *Securing Nuclear Warheads and Materials. Global Nuclear Security Standards*, at: www.nti.org/e_research/cnwm/securing/standards.asp. Also: Gunnar Arbman & Charles Thornton, *Russia's Tactical Nuclear Weapons, Part II: Technical Issues and Policy Recommendations*, Stockholm, Swedish Defence Research Agency, Report ISSN 1650-1942, February 2005.

69 The IAEA has published some common standards contained in Information Circular 225 for the transportation of such materials, in accordance with the multilateral Convention on the Physical Protection of Nuclear Material, which in 2006, had 116 state parties. These controls serve as a basic model for state regulatory authorities to follow in implementing their own controls.

70 Statement of the Director General IAEA, *Security Today: Challenges and Opportunities*, Basel, Nobel Laureate Lecture, Biozentrum, University of Basel, 14 February 2007, at: www.iaea.org/NewsCenter/Statements/2007/ebsp2007n003.html

of HEU, which is far less radioactive than plutonium. While more effective sensors are under development, the challenge is that the nuclear powers need to develop and exercise sufficient control over both fissile materials and nuclear weapons themselves, to ensure that these do not fall into terrorist hands.

A further danger remains: terrorists could attack nuclear facilities, provoking a nuclear incident. However, successfully causing a large release of radiation through a terrorist attack on a nuclear power plant requires knowledge of the plant's physical design and layout, security measures and weaknesses. It also demands either accurately attacking and damaging the core of the nuclear reactor or causing a sustained loss of coolant to the core, which is usually heavily shielded and protected by automatic shutdown functions and emergency cooling systems. The containment structures as well as the reactor design for modern commercial nuclear power plants make a deadly radiation release through sabotage or attack exceedingly difficult to produce. Thus, terrorists may find it easier to gain access to radioactive materials in order to build a dirty bomb, or use hazardous radioactive materials, spent nuclear fuel or attack nuclear materials in transit, which is a serious problem, again calling for high standards of physical protection.

1.3.2 The risks and threats of chemical terrorism

Chemical weapons are chemical compounds that have a strong, deleterious effect on the human body, even when encountered in small doses. The different types of chemical weapons include vesicants, which blister and burn on contact; chocking agents, which cause lung damage; and nerve agents, which interfere with the nervous system and may lead to death. The effects from chemical weapons may occur very quickly after exposure, on the order of minutes to hours.[71]

Toxic chemical agents might be acquired by terrorists either through theft or attacks on industries, stocks or shipments.[72] Terrorist groups may also produce such agents themselves. However, delivering toxic materials effectively enough to kill large numbers of people is more difficult than simply acquiring or making the weapon agents. There are multiple ways to disseminate chemical agents, probably the optimal being by aircraft. Clearly terrorists are likely to have access to sprayer aircraft or various small aircraft that can carry 100 kg of anything as well as 1,000 kg of sarin.[73]

---

71 For more information on specific chemical agents see chapters 1-17 of *Medical Aspects of Chemical and Biological Warfare*, Frederick R. Sidell, Ernest T. Takafuji, David R. Franz, eds., at: www.nbc-med.org/SiteContent/HomePage/WhatsNew/MedAspects/contents.html

72 Chemical threat information has surfaced because of Al Qaeda suspect debriefings, technical intercepts and analysis of Al Qaeda's anticipated actions. Various seized documents demonstrate a significant interest on the part of Al Qaeda planners and trainers in the potential for chemical attacks. Training manuals were found at training camps in Afghanistan indicating that the network possesses crude procedures for producing VX nerve agent, sarin, mustard gas, and hydrogen cyanide gas. And some experimental training took place at camps in Chechnya and Georgia's Pankisi Gorge. Jordanian intelligence officials also claim an interdicted plot to attack the intelligence service headquarters and the US Embassy in Amman, involved the detonation of a large "chemical bomb" that might have killed as many as 20,000 people. At least one arrested plotter backed up the chemical claims in a televised confession.

73 Ownership, sale, and rental of small aircraft are generally not well controlled, and in the US even unregulated and unaccounted for. Getting a small plane in the US is as easy as renting a car, and loading it with a chemical agent would present few problems for a terrorist group.

The most plausible use of chemicals as weapons is in attacking aggregations of people in enclosed spaces like subways, airports, financial centres, universities, stadiums, theatres and cinemas. This, in ways that would cause disruption to crucial infrastructure services or render them unusable, and potentially causing widespread loss of confidence in the ability of the government to protect its citizens. Small quantities of chemicals would usually be all that would be needed – for nerve agents a few hundred grams. Important conferences, exhibitions, major public sport events or games could be prime targets.

A deadly means of spreading a volatile chemical agent is to inject it in, or to break glass jars of the substance on, the intake vents of ventilation, heating and air-conditioning systems of a high-rise office or other building. The intake fans would vaporise the agent and distribute it to the floors supplied by the vents, essentially to a captive group of victims. Air turnover in office buildings is deliberately controlled to reduce energy loss, thus making large complexes inviting targets. Stock markets, important financial centres, highly symbolic government agencies and buildings, as well as some corporate headquarters could be preferred targets.

Underground sewers or utility tunnels could be used as conduits for releasing gases and volatile liquids of chemical and toxic agents, which could disperse through these systems, and eventually emerge from manholes, drains and other openings. Dissemination might also work in subway tunnels, where the agents would be 'pumped' through the city by the trains.

Other ways to use chemicals as weapons include attacking people indirectly by contaminating facilities frequented by large numbers of the public, such as subway and railway stations, stadiums, theatres, cinemas and department stores. Since non-volatile chemicals can be very persistent, thus able to taint their targets and interfere with critical services for longer periods of time, prime targets could be important financial, banking and insurance centres, to disrupt their services or to render them unusable. Also the various stages of food production, processing and distribution offer many potential avenues for attack and good prospects for toxic contamination, particularly for foods consumed quickly, such as milk, fresh meats and vegetables.

Pharmaceutical products can be used for deliberate contamination of larger segments of the population via the vast array of vitamins, health supplements and 'natural' remedies, which do not need approval by governmental agencies. For example, producers of excipients offer good possibilities for attack. Widely used, of which several are often common to more than a hundred approved drug formulations, excipients often account for a relatively high fraction of the final dosage form, thus allowing for lethal contamination at low concentrations. While there are multiple suppliers of excipients, contamination of only one source could have a wide-spread impact, including an erosion of public confidence in the safety of medicines generally.

The water supply system can also be used, but might not be the most likely target for producing mass-casualties by chemical warfare or toxic agents. Many of these

agents hydrolyse in water, react with a disinfectant residual or are rendered harmless, especially under alkaline conditions. However, some insecticides that are chlorine esterase inhibitors, similar in action to nerve agents, do persist in water, and could – like forced entry of some other highly toxic agents into the supply system after water treatment – have serious consequences.

Harmful agents could also be delivered through existing systems already designed for rapid and widespread distribution, such as the postal system. A concerted attack from multiple locations could result in widespread contamination of many of the automated centres where mail is sorted and distributed, resulting in large numbers of infected mail workers and recipients, possibly shutting down the postal service. Other mass distribution systems like currency, newspapers or junk mail might also be used to expose large numbers of people to the effects of toxic substances or to interfere with the functioning of society.

Mass-transit rail and subway systems in major cities remain vulnerable to Madrid-style attacks with chemical weapons. Improvised Explosive Devices (IED) containing a chemical agent can be detonated, dispersing toxic chemicals causing mass casualties.[74]

Rather than seeking to attack large numbers of civilians directly, terrorist groups could choose to attack targets that would release dangerous chemical agents, like plants, tankers and transport vessels containing hazardous chemicals, or cause leakages or large releases of toxic industrial chemicals. An IED could be detonated in close proximity to, or within, a chemical storage facility. Or chlorine and ammonia storage facilities could become targets. Chlorine stores at water treatment plants are a top concern because they tend to be close to cities, and some locations have large stockpiles of liquid chlorine, the most viable form for a large-scale terrorist attack. Also industrial solvents and fertilizers can be extremely dangerous if disbursed in large quantities that can produce deadly concentrations. Civilian industries that use or produce highly toxic materials are sitting targets.[75]

---

[74] Such devices with chlorine gas have been used by insurgents in Iraq. Chlorine gas has also been used by the Liberation Tigers of Tamil Eelam in 1990. The Aum Shinrikyo cult filled 11 vinyl bags with sarin and punctured them after having planted them in 5 different Tokyo subway trains in 1995, killing 12 people. In 10 of the 17 CBW attacks they used chemical agents – 4 with sarin, 4 with VX, one with phosgene and one with sodium cyanide. In June 1994, the cult used a van equipped with a sarin dispenser in the attempt to kill 3 judges hearing a case against the group. It also reportedly killed several dissident members using VX nerve agent. Poisoning attempts with toxics are also known to have happened in the US: in 1982, when cyanide-laced Tylenol was placed in retail stores in the Chicago area; in 1984, when 14 white supremacists plotted in Mountain Home, Arizona, and stockpiled 30 gallons of cyanide to poison the water supplies of Chicago and Washington; and in 1998, the chance prevention of a mailing in which sodium cyanide was sent packaged as free sample of a nutritional supplement. Years prior to 9/11, Abdel Basit said that he had considered a cyanide gas plot targeting the World Trade Center towers, before settling instead on a truck bomb as the vehicle for his 1993 attack. In February 2002, Italian authorities arrested several Moroccan men – allegedly planning to attack the US Embassy in Rome – who were found with about 9 lbs of potassium ferrocyanide. But a threat assessment based solely on the extrapolation from these past, rather unsuccessful experiences can be misleading. More effective chemical weapons may become part of terrorist arsenals. And the concept of manufacturing binary chemical weapons also has been around for decades.

[75] The potential effects of an attack on a chemical plant – or trains of tank cars, trucks, barges or ships – are illustrated by some large industrial accidents such as that in Bhophal, India, when more than 3,000 people died after an accidental release of methylisocyanate from a pesticide plant in 1984. The accidents in the same year at a liquefied gas storage facility in Mexico City, where explosions killed more than 500 and injured about 7,200 people, and the massive explosions at a fertilizer plant in Toulouse in 2001 are other examples. Such chemical industries exist in the vicinity of many cities and some are even located in cities. The regular transport of dangerous chemicals to and from such facilities also raises security risks. In the US alone, more

While chemical weapons are not optimal for terrorist use, this is not to say that some terrorists will not use them, only that biological and nuclear weapons seem to hold greater promise for them. While definitely a threat, chemical weapons will not necessarily kill more people than conventional bombings. Chemical weapons pose the most likely risk of being used in a number of small-scale attacks, perpetrated either with weaponised agents or industrial chemicals, or by causing chemical accidents through sabotage. Attacks could be conducted either simultaneously or sequentially as part of an extended terror campaign that is directed as much at causing panic as at killing.

Terrorist attacks with chemical weapons would yield almost immediate casualties and would not necessarily involve persistent agents. Although only persistent chemical agents result in contamination by military definitions, even minute residual amounts of a non-vaporised nerve agent are outside acceptable bounds for civilians. The appearance of casualties would be something of an immediate spike, leaving medical personnel with a tremendous overload but without the spectre of additional casualties. Medical requirements would be immediate and massive in nature for casualty management consisting of the administration of atropine and pralidoxime chloride. If neurological involvement is severe, diazepam may be necessary to reduce convulsions and brain damage. Ventilation and suction of airways may also be required. Liquid contamination, a less probable occurrence than vapour but still possible, requires immediate removal of the agent from the victim's skin and then chemical decontamination if possible.

If a terrorist attack with chemical weapons happens, identification of the agent employed is time-critical. Fortunately, the physical characteristics of chemical weapons has made the analysis of agents amenable to the analytical techniques commonly employed for most environmental analyses, namely gas and liquid chromatography, with a variety of detectors including mass-spectrometry. Synthetic or relatively pure samples not requiring chromatographic separation are frequently characterized by nuclear magnetic resonance or Fourier transform infrared spectroscopy.[76]

1.3.3 The risks and threats of bioterrorism

Weaponisation of biological toxins and agents has been undertaken by the major powers and others countries for decades, and their potential lethality has been well identified.[77] The NATO handbook dealing with biological warfare defence lists 39

---

than 800,000 shipments of hazardous materials are moved along highways, railways, and pipelines each day. Moreover, the number of such sensitive facilities that would need improved protection is in the many thousands, while, in comparison, there are rather few nuclear facilities. Furthermore, there are very few industrial or manufacturing facilities of any kind with security levels sufficient to withstand a determined attack by a committed terrorist group.

[76] P. A. D'Agostino & C. L. Chenier, *Analysis of Chemical Warfare Agents: General Overview*, LC-MS Review, IN-House LC-ESI-MS Methods and Open Literature Bibliography, Defense Research and Development Canada, Technical Report DRDC Suffield TR 2006-022, March 2006.

[77] For more on the characteristics of biological weapons, their manufacture, and delivery systems, see *Textbook of Military Medicine: Medical Aspects of Chemical and Biological Warfare, Part I: Warfare, Weaponry, and the Casualty*, Frederick R. Sidell, Ernest J. Takafuji, & David R. Franz, eds., Washington D.C., Surgeon General, U.S. Department of the Army, 1997. Also see: US Congress, *Technologies Underlying Weapons of Mass Destruction*, OTA-BP-ICS-119, Washington D.C., US Government Printing Office, December 1993.

agents that could be used as biological weapons.[78] The Soviets organised biological warfare programs around three types of action: anti-personnel, anti-livestock and anti-crop; and three modes of action: inhalation, oral and cutaneous. Bioagents can be manufactured or obtained with far less difficulty than nuclear weapons. Rapid changes in the life sciences influence the availability of the information and expertise required to make toxins and genetically modified viruses and other pathogens.

Biological and toxin weapons kill by using pathogens to attack cells and organs in human bodies. They can also be used to target crops and livestock on a massive scale. Biological weapons are more dangerous than chemical weapons since they are easier to conceal, can cause a larger number of casualties, and do not require rare materials, finances, knowledge or infrastructure to produce. Its underlying sciences and technologies are not secret and mostly dual-use.

For a micro-organism causing disease in man, plants or animals, or deterioration of material to be selected for use as biological agent, it must be such that only a few organisms are needed to initiate the disease, have a relatively short incubation period, high infectivity, high potency, and be unlikely to meet with widespread immunity, natural or acquired, among the target population. Ease of production and its ability to deliver are important additional considerations.

There are a number of organisms which have the necessary characteristics for selection as biological agents. Bioagents can be lethal or non-lethal, transmissible or non-transmissible, and may enter the body by being breathed in, swallowed, or absorbed across the mucous membrane. The delivery of an aerosolised biological agent in ultra-fine particles that can be inhaled into the lungs poses the highest risk of mass-casualties. Such agents may exhibit themselves in minutes or seconds in the case of toxins, or days, if not weeks, to fully manifest themselves in the case of contagious diseases. Biological agents can be grouped in four categories: *viruses; bacteria; rickettsiae and chlamydiae;* and *fungi*. In addition, there are some genetically modified micro-organisms – natural or synthesised proteins affecting body metabolic and other functions.

The biological terrorist threat probably is the most pressing today. Biological weapons are strategic due to their great potential for lethality. The insidious nature of biological warfare, coupled with its ease of concealment and potential for mass-casualties, increases its attractiveness to terrorist groups.[79] Biological weapons have utility across the spectrum of conflict that allows them to be employed for a

---

[78] Departments of the Army, Navy, and Air Force. *NATO Handbook on the Medical Aspects of NBC Defensive Operations*, Washington D.C., Defense Department, 1996.

[79] There is evidence that Al Qaeda is looking at possibilities of acquiring pertinent materials. But expressions of interest by non-state actors in acquiring biological weapons do not prove the existence of a weapon programme, nor do they constitute evidence of a credible capability to deploy such weapons on a large scale. Despite a diverse and highly trained scientific workforce, modern technical equipment, financial resources reportedly of a value of over $1 billion, and little scrutiny either from law enforcement or intelligence agencies for a number of years, the Japanese Aum Shinrikyo cult failed in its attempts to use chemical and biological weapons with large-scale effects in 17 known CBW attacks or attempted attacks between 1990 and 1995, 7 using biological agents, 4 with anthrax, and 3 with botulinum toxin. However, past failures by terrorists offer a fragile basis for confident predictions that bioterrorist events will not occur in the future.

variety of attacks, large or small, against a wide range of targets and with an equally wide range of effects.[80] The diversity of the biological threat inventory and the ubiquity of targets make it impossible to provide a uniform picture of the threat problem. Choices in agents and tactics are perhaps the most difficult aspect of the terrorism problem to assess or predict.[81] But some agents could have massive, unpredictable and potentially uncontrollable consequences, and could profoundly affect the health also of future generations.

The list of agents that could pose the greatest public health risk in the event of a bioterrorist attack is short. But it includes agents that, if acquired and properly disseminated, can cause a difficult public health challenge in terms of a country's ability to limit the numbers of casualties and control the damage to cities and the nation. Probably one of the greatest dangers is that the smallpox virus could be used by terrorists. Cessation of the practice of vaccination in almost all countries may have catastrophic consequences.

Bioterrorism is a real threat, though cataclysmic incidents are probably less likely than smaller-scale attacks. The historical record of individual killings is long. A large number of toxins are suitable for terrorist use as sabotage-infectants, or to bring about the death or temporary incapacitation of individuals or groups of persons. Complicating the terrorist quest for producing biological agents of mass destruction is the substantial technical proficiency required to produce highly virulent agents. What is more, the difficulties involved with proper aerosolisation, and the creation of a milled, powdered agent – rather than the less effective slurry – further hamper a terrorist group's ability to cause mass-casualties.

However, vulnerability and capability, the two prerequisites of bioterrorism, are in place. In fact, there is a heightened fear of the impact of terrorist actions, coupled with profound concerns that modern economies may be particularly vulnerable to disruption from the deliberate spread of disease. The variety of biological attack methods is nearly inexhaustible. So many high-value targets are at risk and so many vulnerabilities exist that biodefense will remain problematic for the foreseeable future. In addition to potentially substantial economic costs associated with such an attack, the psychological impact an attack will have on the population could also prove attractive to some terrorists. Humans, obviously, are

[80] Non-state actors in the US have used biological agents already in 1972, when the 'Order of the Rising Sun', a neo-Nazi group, produced 80 lbs of typhoid bacillus. In 1984, followers of the Bagwhan Shree Rajneesh poisoned with salmonella the salad bars of a small Oregon town. In 2001, 2003 and 2004, biological agents have been used in local incidents, including some that produced fatalities: anthrax infected individuals in Connecticut, New York, Washington D.C. and Florida, and ricin were mailed to the White House in 2003 and Congress in 2004. Other states also have had to cope with bioterrorist threats. In 1979, a Palestinian terrorist poisoned Israeli orphanages. In 1984, Paris police raided an apartment rented by the Baader-Meinhof gang and found flasks of clostridium botulinum culture. In 2003, British law enforcement officials arrested several people accused of manufacturing ricin in a London apartment. While none of these incidents resulted in many casualties, the risk will remain in the years ahead that biological or toxin weapons could be used by terrorists.

[81] Studies at the Monterey Institute of International Studies showed that there had been 285 incidents throughout the world since 1976 in which terrorists had used chemical or biological weapons. In 44 percent of those cases, no one had been killed or seriously injured; in 76 percent of them, 5 or fewer people had been hurt. The small data set relating to terrorist attacks using biological weapons to date only increases the difficulty for assessing the BW risks.

highly susceptible, but also at risk are agricultural assets – livestock, crops and even soil.

Plant and animal pathogens may be acquired more easily than human pathogens, with isolating pathogens from the environment or obtaining them from state sponsors being the most likely sources. Unlike human pathogens, these avenues for acquisition require less specialised equipment and expertise. Terrorists can chose among several plant or animal pathogens that need to come in contact with only the surface of the target host to cause infection. Moreover, for many diseases, once the initial infection has been established, they can be spread effectively through the wind. Because agro terrorism involving biological agents has largely been overlooked until recently, agriculture is nearly unprotected against serious attack – in spite of the potentially huge economic impact of a successful attack, not so much in terms of numbers of casualties, but rather economic dislocation and shortages. Such attacks could come in any number of forms, from contamination of crops using organic pesticides or herbicides; contamination of livestock, food and animal feed; engagement of adulterated seeds; to more complex and difficult contamination of water supplies; aerosol clouds from sprayers, ground or aerial, which would need to be modified to achieve the correct particle size for dissemination; automobiles, boats or missiles. Bombs are less useful since they tend to destroy the agent. To make matters worse, attacks could involve a mix of different biological agents that could confuse and disrupt identification of, and response to, an attack.

There are few barriers to developing such weapons with a modest level of effort. Tricothecene mycotoxins, known as 'yellow rain', can be produced simply using a corn – meal slurry and the appropriate strains of fungus. The specific laboratory technologies needed are common to the pharmaceutical, dairy and beer industry, not subject to international controls and are readily available on the world market. Common laboratory supplies can be easily obtained from commercial suppliers or through the Internet, and are largely uncontrolled, unregulated and unknown. Thus, a terrorist group could construct a substantial laboratory with equipment and supplies purchased anonymously. It would be difficult to locate and detect a covert laboratory. If the equipment and supplies were in fact purchased anonymously, and operational security maintained, there would be few, if any, signatures that could be detected by external means.

There is also the possibility that terrorists could recruit highly skilled scientists. Any group able to recruit skilled professionals will increase its chances of obtaining or successfully developing biological agents, will need less time to construct a BW capability and will increase its chances of conducting an effective attack. However, while it could be within the reach of a group of skilled biologists to concoct a lethal biological agent, it requires a different set of skills, expertise and equipment to weaponise it to target and deliver it over a large population. It is less clear whether terrorists would soon be capable of doing this.

Should a bioterrorist attack occur, however, it may go undetected for some time, particularly if it were a naturally-occurring pathogen, and the vector was food-

borne or via water contamination rather than aerosol dissemination. Both naturally-occurring and human-created diseases pose serious challenges to national security. It must be recognised that, since biological weapons can be disseminated by means of air, food or water, and it is not possible to predict where, when and with what a bioterrorist might strike, full protection is not possible to achieve. The point is to be as well prepared as possible. This calls for cooperation between civilian health and security-oriented authorities, nationally, regionally and world-wide. Responses to bioterrorism will differ greatly from responses to nuclear and chemical terrorism and much more closely resemble responses to emerging infectious diseases or pandemics.

Enhancing emergency preparedness and supporting advanced pharmaceutical re-search for multivalent drugs, among other measures, will help to deter and defeat deliberate and naturally occurring pathogen releases and increase the general health and well-being of the population. The intention of potential attackers is difficult to manage. Therefore, limiting the vulnerabilities is the most promising way to prevent or mitigate biological attacks.

A pervasive sense of vulnerability to unseen microbes is more disturbing to the public psyche than many other potential threats. The 5 deaths and 18 infections caused by the 'anthrax-by-mail' incidents in the US were a fraction of one day's carnage from American traffic accidents, but round-the-clock media coverage fuelled public fear and an overreaction by legislators. The incidents also revealed the inadequacy of current defence measures in responding to even minor incidents.

Nuclear, chemical and biological threats each present unique complexities. But the detection and control of biothreats is by far the most complex. These difficulties reflect several unique aspects of the threat. In assaults with nuclear and chemical weapons, the scale of damage is evident immediately. In contrast, the effects of a bioattack are unlikely to be recognised quickly. Depending on the method by which a pathogen is released or dispersed, initial infection of victims can, for large airborne releases, occur within a few hours or, for release by contagious carriers, extend over weeks or months. The initial symptoms of many bioagents are often indistinguishable from common infections such as colds and flu.

Biological agents used offensively can be genetically engineered to resist current therapies and evade vaccine-induced immunity. Though it is vital that the molecular mechanisms by which classes of organisms cause disease be elucidated in order to understand and counter their effects, this is no simple matter. Preparedness for a biological attack against people, crops or livestock is complicated by the large number of potential agents, the long incubation periods of some agents, and their potential for secondary transmission.

Preventing bioattacks before they occur is obviously the most desirable situation. Substantial R&D investment has been made by the US since the Gulf War to

develop sensors to detect biothreat agents in the environment.[82] However, this is a difficult technical challenge and progress has been slow. The use of environmental sensors to detect illicit production of bioagents is unlikely in the near future. Hence, biodefence must rely mainly on faster medical diagnosis and containment of an incident once it has begun.

The fragility of current public health capabilities in most countries means that the first indication that a bioattack has occurred will only come after doctors report abnormal numbers of people getting ill and presenting the same symptoms. The most realistic object for diagnosis is an infected person or group of people. Speed and precision in establishing an accurate diagnosis of the disease are critical and require both the presence of reliable methods and test systems and highly trained infectious disease specialists. However, the diagnostic laboratory tests for many of the anticipated biothreats are either not yet developed or are only available in a few specialist laboratories. This makes it difficult to ascertain the full scope of an attack and to guide treatment strategies. Moreover, genetically engineered micro-organisms 'raise the technology hurdle' that must be overcome to provide for effective detection, identification and early warning of biological attacks.

Just a few hundred casualties requiring intensive care would overwhelm the hospital network in most cities. Health facilities would not only have to diagnose and treat victims of the attack while still providing care for those ill from natural disease, but they would also be confronted with a tidal wave of 'the worried well' who believe they are victims. If the agent is contagious in human-to-human transmission, the first people to die would be the medical caregivers and the emergency responders. Then, doctors, nurses, ambulance crews, firemen and police could disappear fast. Already a relatively low end of the range of numbers of possible deaths from a biological attack could leave a city without any medical-care system, except for what could be taken care of by the military.

Management of a bioincident would be complicated by a lack of drugs and vaccines. Stockpiles of the few drugs and vaccines which are currently approved for use against biothreats are insufficient if a bioincident required treatment of many thousands of people. And little investment has been made to develop new drugs and vaccines against the bioagents for which no meaningful medical interventions exist.

Actions to limit the consequences of a bioattack require a swift response by public health, military and law enforcement authorities in concert with multiple private sector entities. These groups may have little or no prior experience of working together. Decision-makers would be confronted with unfamiliar and complex technical issues that have the potential for catastrophic outcomes if the wrong judgments were to be made. National leaders would have to decide whether to impose martial law and quarantine, ban trade and travel, and authorise emergency seizure and diversion of private assets.

---

[82] Michell L. Wise & Jon J. Calomiris, „Detection Systems for Biological Warfare Agents, Present and Future", *Combating WMD Journal*, U.S. Army Nuclear and CWMD Agency, Fort Belvoir, Issue No. 3, 2009, pp. 4-13.

Those involved in the containment of infection would also be forced to make hard decisions regarding the rationing of drugs and vaccines, the mandatory testing and treatment of people without their consent, imposition of quarantine, and other constraints on freedom. They would also be required to maintain essential services, and to address the problem of mass-disposal of corpses.

Mass psychological trauma would be aggravated by any perception, real or imagined, that a bioincident was being mismanaged or was out of control. The near certainty of irresponsible actions by the media would augment public panic and civil disorder.

1.3.4 The risks and threats of radiological terrorism

A radiological weapon is any device that is designed to spread harmful radioactive materials into the environment, either to kill or to deny use of an area. Americans use the term Radiological Dispersion Device (RDD) because radioactive materials can be spread in many ways – not only by conventional explosives with what is generally called a 'dirty bomb'. For example, radioactive powders scattered by the wind could theoretically have as severe an effect and would not be considered a bomb. Thus, dirty bombs are simply one type of RDD. Depending on the motives of those involved in planning the incident, such a device could be a low-key weapon that surreptitiously releases aerosolised radioactive material, dumps out a finely powdered radioactive material, or dissolves the radioactive material into water. It would be intended to slowly expose as many people as possible to the radiation. A dirty bomb, in contrast, is a RDD made of a traditional Improvised Explosive Device (IED) with a radiological substance added. Not only is radioactive material dispersed, but the dispersal is accomplished in a planned manner, and the explosion immediately alerts the victims and authorities that an attack has taken place.

Although radioactive material is utilised in constructing RDDs and dirty bombs, they are not nuclear weapons. Nuclear weapons induce nuclear chain reactions in bomb materials – materials less radioactive than the products of the reaction. This produces large energy releases along with radioactive daughter products more radioactive than the original material. In contrast, radiological weapons disperse material that is already radioactive. They cannot be equated to the catastrophic effects of nuclear weapons. Radiological terrorism may be a more attractive option than nuclear terrorism because of the relative ease with which either a radiological weapon can be made and used, or an already existing nuclear facility can be attacked. Of the two types of radiological terrorism, use of a RDD or a dirty bomb can be considered easier than attacking a nuclear facility.

Due to their inherent features and demonstration effects, dirty bombs may also prove to be a more reliable, tempting and prestigious option than chemical and crude biological weapons. The first terrorist use of a radiological device might set a dangerous precedent, particularly because they would be able to capitalise on the psychological impact stemming from the fear of radiation among the general

population. A radiological attack would most likely result in mass panic, perhaps some human deaths and injuries, extensive physical and economic damage, and a great deal of attention for the terrorists themselves. Theoretically, this outcome might be considered ideal for groups that seek publicity for their name and cause, without causing widespread devastation.[83]

The detonation of a dirty bomb in a densely populated or industrial area would produce both local and extensive contamination. Terrorists can place explosive RDDs in parcels and luggage of various types, which can be triggered either with an internal mechanism such as a timer, or remotely through a cell phone connection or similar technique. Such devices can vary greatly in size, ranging from birdcages to much larger luggage left on subways, or vehicles, such as cars, taxis or trucks at places where people congregate. The degree of sophistication depends on the ingenuity of the designer, the tools, as well as the materials available. Since a dirty bomb is intended to cause a panic, the explosion of such a device in a heavily populated urban area could very well result in a panic that could kill more people than the IED or the radiation it disperses. Moreover, the radiological effects of a dirty bomb will be larger than the killing radius of the IED itself, and will persist for far longer. While the radiation level may not be strong enough to affect people who are exposed briefly in the initial explosion, the radiation will persist in the contaminated area and the cumulative effects of such radiation could prove very hazardous. Due to this contamination, it will be necessary to evacuate people from the contaminated area in many, if not most, cases involving a dirty bomb. People will need to stay out of the area until it can be decontaminated, a process that can be lengthy and very expensive.

While RDDs would cause few immediate casualties from radiation, they would leave behind radioactively contaminated areas and buildings, up to several city blocks. Little is known about the techniques for, or costs of, large scale decontamination of buildings. The difficulty of decontamination depends on the type of isotope used in the RDD because each element has a different chemical reactivity. Decontaminating streets, squares and buildings is complicated; they must be sprayed with plenty of water and scrubbed, sometimes even vacuumed.

The choices for recovery are limited to decontamination, demolition or abandonment. No one knows how much it would cost to clean up, abandon or demolish these buildings. Other economic costs would include jobs and services lost while the buildings remain contaminated. The affected town or region would lose much of its attraction for inhabitants, investors, companies and tourists. Because they temporarily render the contaminated areas uninhabitable, RDDs have been referred to as weapons of *mass-disruption* or *mass-dislocation* rather than

[83] Evidence uncovered in Afghanistan in January 2003 has led the British authorities to believe that al Qaeda already possesses a dirty bomb, although the weapon has not yet been used. On 28 September 2006, an audio statement was released by the Al Qaeda leader in Iraq, Abu Hamza al-Muhajer, who called for scientists to join his group's efforts against US and coalition forces in Iraq, advising them that the large US bases there are good places to "test your unconventional weapons, whether chemical or 'dirty' as they call them". See: "British Terrorist Dhiren Barot's Research on Radiological Weapons", *Global Terrorism Analysis*, The Jamestown Foundation, at: http://jamestown.org/terrorism/news/article.php?articleid=2370201

WMD. The vast expense of decontaminating a large, densely populated area would also make a dirty bomb a type of *economic weapon*.[84]

Not all nuclear materials are equally useable. HEU and plutonium may be suitable for direct use in an improvised nuclear explosive device with little or no additional processing. Nuclear material in the form of low enriched uranium, depleted and natural uranium and thorium requires extensive, technically complex processing to be used in a device that would be intended to slowly expose as many people as possible to the radiation. By its very nature, this kind of RDD will not generate immediate terror, panic or the type of media coverage coveted by most terrorists.

Generally, a dirty bomb that uses a large quantity of highly dangerous radioactive material such as Plutonium-238 or Cesium-137 will produce more contamination than a device that uses less material or material that is less radioactive. However, the most highly radioactive materials are the hardest to obtain, the most difficult to work with and so dangerous that even suicide bombers would die before they could use one if they were not properly shielded.[85] There are many more common, less dangerous materials that would be easier to obtain and work with. Radioactive sources are used in medical, industrial, agricultural, petroleum survey and research applications. They can be found in hospitals, universities, medical, industrial and food irradiation facilities and even homes. However, not all of these sources would be suitable for use in a RDD. Many are far too weak to cause extensive damage. Furthermore, many radioactive sources are in metallic form, thus would not be dispersed very effectively by strong explosives.

Nonetheless, the ubiquity of radiological materials, and the crude requirements for detonating such a device, suggest a high likelihood of use, even if the technical feasibility is not trivial. It requires advanced know-how and planning, a very targeted approach and some expenditure. The impact would be great if the radiological device in question released the enormous amounts of radioactive material found in a single nuclear reactor fuel rod. But it would be quite difficult and dangerous for anyone to attempt to obtain and ship such a rod without death or detection.

It is the portability of certain types of radioactive sources that enhances the attractiveness of radiological terrorism. Radioactive sources differ greatly in size and level of radiation. Some sources may be relatively big and bulky because of the layers of shielding surrounding the radioactive material. The difficulty in moving these around may make them less attractive to terrorists. Other sources, however, are small enough to even be carried by hand. Radioactive Cobalt 'pencils' from a food irradiation plant are about 25 mm in diameter and some 25 cm long, with hundreds of such pieces often being found in the same facility. Some Cobalt rods may contain 10,000 curies.

---

84 Fred Burton, "Dirty Bombs: Weapons of Mass Disruption", *Stratfor*, Predictive, Insightful, Global Intelligence, 4 October, 2006, at: www.stratfor.com/products/premium/print.php?storyId=277090

85 For example, in September 1999, two Chechen militants who attempted to steal highly radioactive materials from a chemical plant in the Chechen capital of Groznyy were incapacitated after carrying the container for only a few minutes each; one reportedly died. See: "Dirty Bombs: Weapons of Mass Disruption", *Stratford*, op. cit.

Different scenarios for employments are possible. Apart from engagement as dirty bombs, terrorists could use RDDs as an enclosed radiation source; to contaminate food; to irradiate drinking water; or as an aerosol. Thus, a strong gamma-emitting source could be hidden in high-profile areas such as densely populated urban sites or government facilities, which could expose a large number of people to intense radioactivity over a shorter or longer period of time. For the short time case, it is unlikely that people would suffer an acute radiation syndrome. However, on discovery, panic reactions may be expected among all persons who have spent time close to it. In the longer time case, persons could suffer from acute radiation syndrome, and could even die as consequence of the irradiation, but the number of victims of such an attack would be limited.[86]

Food or beverages could be contaminated by adding radioactive substances, for example in production plants, at distribution centres, during transport or at retail shops. The main danger in this case is internal contamination of the consumer. Even a selective and weak contamination of only a small number of items would have a considerable effect on the public, cause panic and greater economic damage. An alternative option would be the contamination of drinking water by addition of soluble radioactive substances in the water supply and distribution system of larger cities, which equally would have a considerable effect on the public. However, because of the high dilution of soluble radioactive substances in large amounts of water, this may not result in highly dangerous contamination for the consumer. Nonetheless, the low tolerance values for drinking water may well be exceeded and require costly mitigation and cleaning measures.

With suitable technical equipment, an easily breathable aerosol can be produced. The introduction of aerosol into air intakes or air-conditioning systems, or its dissemination with crop dusters or sprayers from the top of elevated buildings, or even the spraying of a solution of radionuclide in a major building, would result in people breathing contaminated air. In addition, the deposition of aerosols would cause a contamination both of the people and of the ground surface or the floor of a building. Such an attack may give rise to fears of cancer for the people involved, lead to closure of the area for the time required for decontamination, subsequent economic loss, and high decontamination costs.

1.3.5 The risks and threats of cyberterrorism

The advent of the computer age has opened up possibilities of yet another kind of mass-disruption: information- or cyberterrorism. Attempts to define cyberterrorism suffer from the same dilemmas as definitions of terrorism.

[86] In the case, for instance, of aerosolised plutonium, the main hazard is the dose to the lungs from particles retained in the pulmonary system. If the levels are high enough, the resultant dose can lead to fibrosis and collapse of the lungs with death occurring within a matter of days or weeks. Long-term lung impairment can leave people disabled and in need of intensive care for the remainder of their lifetime. Below the threshold for 'early effects', alpha irradiation of the lungs can lead to lung cancer. Some of the inhaled plutonium will be transferred to the blood via the lymphatic system and become deposited in other organs, notably the liver and on bone surfaces, where it will also produce a cancer risk. See: "Radiological Dispersion Weapons: Health, Social, and Environmental Effects", a Briefing Paper from International Physicians for the Prevention of Nuclear War, *Global Health Watch Report*, originally published in 1996.

Generally, cyberterrorism is a result of the convergence of technology and terrorism, and consists of two mutually dependent elements: (1) It refers to attacks against computers, networks and the information stored within them, for the purpose of intimidating or influencing a government or society to further political or social objectives, and (2) the attack results in violence against persons or property, or at least causes enough harm to generate fear.

Progress in computer networking technology has blurred the boundaries between cyberwarfare, cybercrime and cyberterrorism. Hence, labelling a cyberattack as cybercrime or cyberterrorism is problematic because of the difficulty in determining with any certainty the identity, intent, or the political motivations of an attacker. Cybercrime and cyberattack services now available for hire from TOC groups are a growing threat to national security as well as to the economy. While the threat of a terrorist cyberattack may still be less likely than conventional physical attack with kinetic energy weapons or explosives directed against computers, an IT facility or transmission lines disrupting the reliability of equipment, past terrorist incidents have already been linked with cybercrime.[87] A terrorist cyberattack could actually prove more damaging because it could involve disruptive technology that might generate unpredictable consequences that give terrorists unexpected advantages. Moreover, new and sophisticated cybercrime tools could operate to allow terrorist groups to remain unidentified while they direct cyberattacks through the Internet.

Cyberattacks come in two forms: one against data, the other on control systems. The first type attempts to steal, corrupt or destroy data and deny services. The vast majority of Internet and other computer attacks fall into this category, such as credit card number theft, Website vandalism and the occasional major Distributed Denial-of-Service (DDoS) assault. Control-system attacks attempt to disable or take power over operations used to maintain physical infrastructure, such as distributed control systems that regulate water supplies, electrical transmission networks and railroads. While remote access to many control systems have previously required an attacker to dial in with a modem, these operations are now increasingly using the Internet to transmit data or are connected to a company's local network. Still, any damage resulting from electronic intrusion would be measured in loss of data, not life. It is relatively easy to conduct an attack given the endemic vulnerability of IT systems. It is much harder to kill people or have a lasting effect using cyberattacks.

What makes cyberterrorism different is the ease with which an immense amount of damage can be inflicted on IT systems of government, the armed forces and the critical national infrastructures of a country from almost any point on earth by very few terrorists, at low personal risk and costs.[88] IT is essential to virtually all of

---

87 Brian Krebs, "Three Worked the Web to Help Terrorists", *The Washington Post*, July 6, 2007, p. D01. Louise Shelly, *Organized Crime, Cybercrime and Terrorism*, Computer Crime Research Center, September 27, 2004. Glenn Curtis & Tara Karacan, *The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe*, a study prepared by the Federal Research Division, Library of Congress, December 2002.

88 See: Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", *CRS Report for Congress*, Congressional Research Service, Washington D.C., RL32114, Updated January 29, 2008.

the nation's critical infrastructures, which makes any of them vulnerable to terrorist attack. IT plays a critical role in managing and operating nuclear power plants, dams, the electric power grid, oil and gas pipelines, water treatment, sewage and waste management systems, air and ground traffic control, rail and other transportation systems, digital and voice communication systems as well as financial institutions. Many of these are operated with networks of computer-controlled devices, known as Supervisory Control and Data Acquisition Systems (SCADA), which can be hacked. SCADA systems could be attacked by overloading a system that, upon failure, causes other operations to malfunction as well. Such cascading or domino effects have been seen in incidents resulting from natural events.[89] IT is equally important for emergency operations centres, police, fire and medical services, and can also play a major role in the prevention, detection, and mitigation of terrorist attacks.

IT systems serve as weapons and targets. The main weapons of this new kind of warfare are the use of computers and the Internet in conducting warfare in cyberspace against IT software, and the use of high-powered radio signals to disable or destroy IT hardware.

Software can be damaged by computer viruses and logic bombs, set to detonate at a certain time and destroy or rewrite data. Malicious code can be used in a cyber-attack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting a vulnerability in computer software or a weakness in the computer security practices of an organisation. Computer viruses can shut down entire IT networks and systems through self-replication on available disc space. In addition to logic bombs, hostile programmes like trapdoors, Trojan horses, worms and spyware can be clandestinely introduced into target computers. Moreover, there are Botnets that are made up of vast numbers of compromised computers infected with malicious code, which can be remotely controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information or distribute spam, viruses or other malicious code. And there are Distributed Denial-of-Service Attacks: where large numbers of computers in one country can launch a DDoS attack against systems in other countries.[90]

---

89 For example, in August 2003, Ontario and much of the north-eastern US were hit by the largest power blackout in North America's history. Electricity was cut for 50 million people for up to 4 days, causing massive disruption of all transportation. Large previous blackouts include the November 1965 outage stretching from Toronto to New York, one in July 1977 in New York City, triggering widespread looting, and in August 1996 in 9 western US States. In Europe, Scandinavia and Italy were hit by large blackouts in September 2003, and Western Europe in November 2006, where the outage hit millions of homes.

90 Known attacks have occurred against the US from computers and networks situated in China and Russia. See: Jim Wolf, "U.S. Air Force prepares to fight in cyberspace", Reuters, November 3, 2006. In May 2007, Estonia came under cyberattack where the Estonian parliament, ministries, banks and media were targeted. See: Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, May 17, 2007. On the first week of September 2007, the Pentagon and various French, German and British government computers were attacked by hackers of Chinese origin. On 14 December 2007, the website of the Kyrgyz Central Election Commission was defaced during its election. And Georgia fell under cyber attacks during the 2008 South Ossetia War.

Hardware can be destroyed either with High-Energy Radio Frequency (HERF) guns, Transient Electromagnetic Devices (TED), Electromagnetic Bombs or Improvised Directed Energy Weapons (IDEW), all disabling electronic targets through high-powered radio signals. A HERF gun consists of a power source, an apparatus to generate RF energy and an antenna to direct the energy to affect all electronic components in the vicinity, essentially 'frying' them. However, it must be tuned to the frequency of the target, is complex, usually large in size and hard to 'aim', and it requires large amounts of power and a cooling system. A TED, in contrast, emits a transient pulse of electromagnetic radiation of a few picoseconds in length and is not limited to a single frequency. TEDs generally use spark gap switches, in oil or in gas pulse storage lines or explosively pumped flux compression generators. TEDs are cheaper and easier to build in briefcase, van-size or backyard versions, are virtually undetectable and thus the weapon of choice for 'cyber warriors'. An Electromagnetic bomb is a weapon designed to disable electronics with an electro-magnetic pulse (EMP) that can couple with electrical and electronic systems to produce damaging current and voltage surges by electromagnetic induction. The effects are usually not noticeable. Devices susceptible to EMP damage include integrated circuits, silicon chips, transistors, diodes, inductors, electric motors and even vacuum tubes. An IDEW can be built using the basic microwave cooker element, which has to be adapted, as the principal component.

Microwave weapons can be aimed at computers, electronic devices and persons. Indeed, they have strong physical and psychological effects on people.[91] Such weapons are also part of crimes that almost nobody knows about except for the victims and the offenders. Some claim that high-power microwave (HPM) weapons – using magnetrons, micro-wave-generators, amplifiers and integrated systems – and their proliferation into subversive organisations, offer the means to commit the 'perfect crime'.[92] HPM attacks typically leave no residual evidence, and their effects can range from a nuisance to truly catastrophic.

The number of potential targets is almost endless and growing along with the proliferation of computer systems. And as the directed energy technology develops, so does the number of possibilities to create havoc. The most vulnerable infrastructure computer systems are probably the Internet itself, and the computer systems that are part of the financial infrastructure.[93] Computers seized from Al Qaeda indicate that its members are becoming more familiar with hacker tools and services that are available over the Internet.[94] However, cyberterrorists would probably need to attack multiple targets simultaneously for longer periods of time to gradually create terror, achieve strategic goals, or to have any noticeable effects

---

91 The effects of a microwave beam on the victims include extreme weariness, headache, irregular heartbeat, diarrhoea, painful testis, damaged nervous system and internal organs, burned skin and eye damage. Later effects include blindness, heart attack, stroke and cancer. Cancerous tumours have been diagnosed in some of 40 victims found in Germany. Interference with breathing poses the most significant and potentially lethal results.

92 Reinhard Munzert, "Targeting the Human with Directed Energy Weapons", September 2002, at: www.mikrowellenterror.de

93 If an attack were to cause the collapse of the international funds transfer networks CHIPS and SWIFT, then the global economy could be thrown into chaos.

94 Richard Clarke, "Vulnerability: What are Al Qaeda's Capabilities?", *PBS Frontline: Cyberwar*, April 2003.

on national security.[95] This is why it might be more likely that any severe cyberattacks that take place in the near future will be used by terrorist groups to simply supplement the more traditional physical terrorist attacks. A coordinated cyberattack, particularly if directed against emergency operations centres, first responders, police, fire and medical services, could be used to amplify the effects of a conventional terrorist attack or a terrorist attack with WMD.

The increasing sophistication of, and growing reliance on, computer systems and networks by the military, government agencies and critical infrastructure makes security imperative. Conventional thinking in governments and the armed forces is that prevention is far better than dealing with the consequences of breached IT systems, whether the purpose is spying, disruption or destruction. The risks are simply too great, with IT security companies benefiting from this growing and potentially vast market. IT security is a fast-developing industry, where technological developments in hardware and software, combined with the development of hacking and virus-spreading techniques, demands constant development and updating, with large potential for long-term repeat sales of products and services.

The government's efforts should focus on multidisciplinary problem-oriented R&D that is applicable to both civilian and military users of IT, yet is driven by a deep understanding and assessment of vulnerabilities to terrorism. To achieve long-term advances, R&D must extend beyond improving the security of existing systems, and investigate new approaches to secure and reliable operations that do not directly evolve from the IT of today.

[95] Scott Nance, "Debunking Fears: Exercise Finds 'Digital Pearl Harbour' Risk Small", *Defense Week*, April 7, 2003.

2. What Is Intelligence?

While definitions of intelligence abound,[96] they are more often obfuscating rather than clarifying. A definition acceptable to all nations remains elusive. The simplest and clearest definition is: 'information plus analysis equals intelligence'. It clarifies the distinction between collected information and produced intelligence, namely: without analysis, there is no intelligence. Intelligence is not what is collected; it is what is produced after collected data and information is evaluated and analysed. More precisely, intelligence is data and information that has been subjected to the intelligence process of collection, collation, evaluation, analysis and assessment with the aim to produce the knowledge needed for national decision-making on security policy and strategy.

In more general usage, intelligence can be seen as an umbrella term denoting five things: a particular knowledge; the organisation producing that knowledge; the activities pursued by this organisation; the process guiding these activities; and the products resulting from these activities and processes.

The purpose of intelligence is to inform government: telling 'best truth' unto power – providing knowledge and understanding upon which national decisions can be made. Intelligence produces that *particular knowledge* that a state must possess regarding the strategic environment, other states and hostile non-state actors to assure itself that its cause will not suffer nor its undertakings fail because its statesmen and the organisations and means for implementing security policy plan, decide and act in ignorance. Intelligence is production of – in theory – *unbiased information* about risks, dangers and threats to the national vision, the state and its population, as well as chances and opportunities for the advancement of national interests. The more accurate and timely the intelligence, the more it will allow for limited resources to be applied efficiently towards national security goals and policies.

Intelligence services exist to: (1) support the national decision- and policymaking process; (2) ensure early warning; (3) assist good governance; (4) provide long-term expertise; (5) support national and international crisis management; (6) support national defence and, in case of conflict or war, military operations; and (7) maintain and protect secrets.

All intelligence services have three basic functions: *collection, analysis* and *counter-intelligence*. *Covert action*, the more occasional fourth function, may be performed by external intelligence services or, as is increasingly the case also domestically, in disruptive actions by the police.

Collection is the bedrock of intelligence: the acquisition of data and information that forms the basis for refined intelligence and knowledge creation. Without collection, intelligence is little more than guesswork. The collection process involves open and secret sources, who provide information that is obtainable in

[96] See: http://intellit.muskingum.edu/whatis_folder/whatisintelintro.html

no other way, as well as a number of secret technical collection disciplines using a variety of collection methods and means.

Analysis is collation, evaluation and analysis of data and information of all sources and their transformation into intelligence products. If collection is dominated by smart technology, analyses still reflect the perspicacity of the human mind. No amount of data and information can substitute for an insightful analyst able to discern the critical policy or operational significance of an event, action or trend which may be hidden within a mass of confusing and contradictory information. Analysis and appraisal occur at all levels of intelligence and can be single source, multi-source, or all-source. Assessment is the final step in the analytical process, and strategic assessment is the final all-source intelligence product of actionable knowledge provided to government to anticipate risks and reduce uncertainty in its pursuit of furthering or protecting national political, economic and security objectives. While analysts must prove their capability to 'connect the dots', the overarching goal of analysis is *to minimise uncertainty* with which policymakers must grapple in making decisions about national security and foreign policy. Furthermore, analysis must help *to make sense of complex issues* and to *call attention to emerging problems or threats to national interests*. The importance thereby is not only to determine what is accurate, but foremost what is *relevant* to the decision- and policymaker's needs.

Counterintelligence is intelligence designed to uncover hostile operations against the nation – the national effort to prevent foreign intelligence services and foreign-controlled political movements or groups from infiltrating the state's institutions at home and abroad in order to engage in espionage, subversion, sabotage and terrorism. It is *not* security, but intelligence on which security policies should be based. Straddling the foreign and domestic boundaries, counter-intelligence consists of offensive and defensive measures of protection: *defensively* by inquiries and vetting of civil servants and employees, through investigations, monitoring of known or suspected agents, and surveillance activities to detect and neutralise the foreign intelligence service' presence; *offensively* through the collation of information about foreign intelligence services and their *modus operandi*, recruiting agents, and initiating operations to penetrate, disrupt, deceive and manipulate these services and related organisations to own advantages. Counter-intelligence is, moreover, an integral part of the entire intelligence process: to make sure that what is collected is genuine through continuous evaluation of the *reliability of sources* and the *credibility of information*. It differs from intelligence collection in that it exists to counter a threat and is to some degree reactive. Results are not generally produced in the short term, and counterintelligence investigations cannot be limited to arbitrary time periods.

Covert action comprises activities to influence political, military or economic conditions, situations and developments abroad, where it is intended that the role of the government will not be apparent or acknowledged publicly. These may consist of propaganda measures, support to political or military factions within a specific country, technical and logistical assistance to foreign governments to deal with problems within their countries, or actions to disrupt illicit activities that

threaten the own national interests or security such as terrorism, proliferation, organised crime or narcotics trafficking. Covert action is an option short of military action to achieve objectives which diplomacy and other means of security policy alone cannot. A limited policy tool, covert actions are often carried out in conjunction with other tools of statecraft or, domestically, in disruptive actions by law enforcement or the police.

These functions or roles of intelligence services are common to most intelligence systems. How they are distributed between and among the intelligence agencies differs from state to state. These functions operate most effectively as part of a process in close conjunction with one another. Collection of intelligence cannot be done effectively without analysis that provides guidance or 'tasking' to collectors. Counterintelligence is necessary to protect collectors from becoming known, neutralised and exploited by adversaries. Similarly, a successful programme of covert action must be grounded in effective collection, analysis and counterintelligence. Thus, the nature of intelligence is such that the several elements of intelligence are parts of a single unified system whose success depends on all parts working effectively.

2.1 How Is Intelligence Produced?

Intelligence is produced in a process by which the government, the military leadership, other agencies and customers request the intelligence needed, and by which intelligence services respond to these needs in six steps of activities of the **intelligence cycle:** (1) *defining the needs, planning and direction*; (2) *collection;* (3) *processing;* (4) *analysis and production*; (5) *dissemination* of finished intelligence products, and (6) *feedback*.

Defining the needs, planning and direction – involves the management of the entire intelligence production effort, from initiation by requests or requirements for intelligence on subjects based on the needs of decision- and policymakers; the identification of the need for data that is derived from the threat assessment; or from the priority listing of unsolved strategy and policy issues; deciding which states or non-state actors warrant intelligence surveillance and collection; to the delivery of an intelligence product to the customer.

Collection – is the procurement of data and information pertinent to decision- and policymakers, the military leadership, other agencies or intelligence customers. Collection management systems of a variety of methods and means are used in the following *intelligence collection disciplines:*

- **Open source intelligence** (OSINT) – is the assembling of all openly available data and information from radio, television, journals and printed news sources, books, grey literature, studies, official reporting, from Internet search and conversations, the deep web, as well as facts and forecast from businessmen, think tanks, universities, travellers, etc.

- **Human intelligence** (HUMINT) – is information collected by humans: from spies, agents, insiders or informers; gleaned from defectors, turncoats, walk-ins; or elicited from diplomats, businessmen, travellers, academics; as well as information gained by debriefings, interrogation, from discussions with foreign personnel; or resulting from counterintelligence operations, etc.

- **Signals intelligence** (SIGINT) – is data and information collected through intercepts, monitoring and localising of radio, microwave, radar and other electromagnetic emission, including laser, visible light and electro optics, gathered by overt or clandestine ground sites, ships, submarines, aircraft, UAVs or satellites, all generally recording and reporting what has happened. SIGINT can provide data on intentions, plans, activities or events related to threats as well as on the characteristics of materials and weapon systems. SIGINT has five *subsets* of collection disciplines:

  i. **Communications intelligence** (COMINT) – is data and information collected through intercepts of communications, direction finding, traffic analysis and monitoring of the changes in volume, pattern and other characteristics of communications like burst, frequency hopping, spread spectrum, etc.

  ii. **Electronic intelligence** (ELINT) – is electromagnetic pickup and signals monitoring of electronic emissions of events, activities, relationships, frequency or scale of occurrence, modes, sequences, patterns, signatures as well as content; or intercepts of emissions from tracking, radar and weapons systems for gauging their capabilities such as frequencies and the range on which they operate.

  iii. **Foreign instrumentation signals intelligence** (FISINT) – is the pickup and monitoring of data relayed by weapons or beacons and video links, etc. Non-imaging radar can detect and track missile launches and gather data on missile characteristics. One category therein is telemetry intelligence (TELINT) – data obtained from intercepting the signals transmitted during missile tests, enabling the performance of missiles to be evaluated.

  iv. **Cryptology intelligence** (CRYPINT) – is code-breaking and decryption of ciphered messages, which requires supercomputers and mathematicians.

  v. **Computer network exploitation** (CNE) – is data and information collected from network and traffic analysis or by monitoring, mail and messages interception, computer intrusion and penetration of databanks.

- **Imagery intelligence** (IMINT) – data and information collected via photography (PHOTINT), film, video, high-definition TV or radar by satellites, aircraft, UAVs and ships. It is imagery and satellite signals – data

streams captured and reconstructed as images from the reflections of several bands, including infrared, ultraviolet or other image-capturing technologies[97] – all more often recording and telling what may happen. Cartography and mapping have come to depend ever more heavily on IMINT.

- **Measurement and signatures intelligence**[98] (MASINT) – is straddling both IMINT and SIGINT, using visible light, infrared, ultraviolet, multi- (2-100 bands), hyper- (100-1,000 bands) and ultra-spectral (1,000 + bands) data derived from spectral analysis of reflections across the spectrum of light and exploitation of physical or magnetic properties, emitted and reflected energy of radio frequencies, lasers, shockwaves, acoustics of mechanical sound, vibration or motion, as well as materials sampling of soil, water, and air. It enables one to detect the shape, material composition, density, temperature, brightness, movement and chemical composition of objects.

Processing – is the conversion of data and information collected into a more suitable form for analysis and production of intelligence, such as language translation, decryption, rendering texts readable and translating film or digital signals into visible imagery. Data and information not directly analysed is tagged, sorted and made available for rapid computer retrieval. Thus, processing also refers to sorting by subject matter, as well as data reduction – interpretation of the information stored on film or tape through use of highly refined photographic and electronic processes.

Analysis and production – is the conversion of data and information into finished intelligence products. It comprises collation, correlation, integration, analysis and evaluation of all available data and its transformation into a variety of intelligence products. Data and information collected are frequently fragmentary and at times contradictory, requiring the human mind and specialists to give it meaning and significance. Thus, good analysis depends upon assembling the best brains possible to evaluate events and conditions, drawing upon a blend of public knowledge and secrets purloined from adversaries. The subjects involved may concern intentions, events and activities, capabilities and vulnerabilities, possible and probable future developments, different regions and problems, and personalities in various contexts – political, geographic, economic, scientific, military or biographic. Exercising collection management, analysis draws on the

---

[97] Today, most IMINT systems are digital and operate in near real-time. The optical systems rely on charged couple devices, which translate the varying visible-light levels of the object viewed into numbers (0 and 1), which are immediately relayed back to earth, sometimes via relay satellite, and reconstructed into an image. Since radio waves are not blocked by clouds, radar imagery can be obtained not only in the day or night but even when clouds block the view of a satellite's visible-light and infra-red sensors. Moreover, radar may also find underground installations. The infrared radiation reflected by an object can be used to produce an image during daylight and night. IMINT remains important to treaty verification and can provide a warning about impending events. During the Cold War, US and Soviet overhead reconnaissance capabilities allowed the negotiation of arms control agreements, since each side had independent means of monitoring compliance, and providing reassurance that the other side was not in the process of preparing for a surprise attack.

[98] MASINT is officially defined as "technically derived intelligence that, when collected, processed, and analysed results in intelligence that locates, tracks, identifies, or describes the signature of fixed or dynamic target objects and sources". Numerous scientific disciplines and advanced technologies are applied in dedicated MASINT systems. Whereas SIGINT is akin to hearing and IMINT to sight, MASINT is akin to touch, taste and smell.

collection disciplines to provide data and information for evaluation and the tailoring of the products precisely for the users' needs.

Dissemination – involves the distribution of the finished intelligence product to the customer – the same decision- or policymakers whose needs triggered the intelligence cycle. A product must have five essential characteristics for it to be useful: *relevance; timeliness; accuracy; breadth;* and *purity* – meaning that it is free of political spin, disinformation, propaganda, deception, etc. The products should contain what is known – *the facts*; how it is known – *the sources* where possible; what drives the judgments – *linchpin assumptions;* the impact if the drivers change – *alternative outcomes;* and *what remains unknown*. The key issue for intelligence services is how to present the collected, processed and analysed information in a manner which meets the requirements of the customer, both in content and presentation, *while ensuring that it highlights the limitations of the intelligence to answer the questions adequately.*

Feedback – is what the customers must provide, expressing satisfaction or discontent and convey new requirements for answers to new questions. The user of intelligence then ideally provides additional direction to the collectors and intelligence producers, who should in turn provide more and better intelligence. Feedback may also be used to guide *new areas of inquiry, to identify gaps* in information, and to *adjust priorities or emphasis*.

2.2 What Types of Intelligence Services Are There?

Four different categories of intelligence can be distinguished that have spawned separate intelligence services or agencies: *foreign, domestic, military* and, more recently in some countries, *criminal* intelligence.

- **Foreign** or **External Intelligence Services** collect, analyse and produce intelligence relevant to *external security* and for warning purposes. Protection of external security requires knowledge of the risks, dangers, threats, opportunities and chances, of the possibilities and probabilities of developments and the likelihood of events and outcomes. Intelligence is therefore needed on *intentions, plans, capabilities* and *activities* of foreign powers, organisations, non-state groups and their agents that represent actual or potential threats to the state and its national interests.

- **Domestic** or **Internal Intelligence Services**, often called **Security Services**, collect, analyse and produce intelligence relevant to *internal security* and for warning. Internal security aims to protect the state, sovereignty, territory, critical infrastructure, society and people against malicious acts and hostile activities. What Foreign Intelligence covers externally Domestic Intelligence does internally, depending on the situation with different priorities: uncovering terrorism; espionage; sabotage; subversion; political, ethnic and religious extremism; organised crime, narcotics production and trafficking; money faking and laundering; proliferation of WMD; illegal arms

dealing; arms, human, contraband and other smuggling; illegal immigration; electronic and cyberattacks, hacking and data theft; and dissemination of pornography, etc.

- **Military** or **Defence Intelligence Services** collect, analyse and produce intelligence relevant for defence planning, the armed forces and support of military operations. Support to defence planning entails intelligence on foreign military capabilities; vulnerabilities; doctrines; order-of-battle; operational concepts; tactics; and weaponry performance in order to shape the size, types and deployments of the armed forces, to guide military R&D and future defence acquisitions. Support to military operations encompasses intelligence for force projection and targeting support; to ensure transparency of the battle space, localising the centres of gravity and decisive points; and to enable through network-centric and effects-based operation decision dominance and the achievement of strategic and operational objectives.

- **Criminal Intelligences Services** – a more recent institutional development in response to the growth of organised crime since the end of the Cold War – collect, analyse and produce intelligence on TOC groups, corruption and criminal activities with the aim to prosecution.

Different collection methods with sophisticated technical means can give rise to more specialised intelligence agencies. Such entities include imagery, signals and cryptology intelligence agencies. The US NSA, NGA, NRO, and NAO, the Australian DSD and DIGO, the successor organisation of FAPSI in Russia, the British GCHQ and the Canadian CSE, for example, are the biggest and most expensive of their intelligence agencies.[99] Together with the Foreign or External Intelligence Service, the Domestic or Internal Intelligence Service, the Security Agency, the Military and Defence Intelligence Services and the Criminal Intelligence Service, they constitute the *national intelligence community*.

Countries with larger intelligence communities often have some additional central or functional bodies for coordinating assessments or – a post-9/11 development – for the fusion of intelligence, such as the National Counterterrorism Center, the National Counterproliferation Center, the National Counterintelligence Executive, the National Center for Medical Intelligence, the National Cybersecurity Center, and the National Intelligence Council in the US; the Joint Terrorism Analysis Centre and the Joint Intelligence Committee in the UK; and the Office of National Assessments in Australia.

---

[99] US: *National Security Agency* (NSA) responsible for SIGINT and CRYPINT; *National Geospatial Agency* (NGA) responsible for earth information, IMINT and mapping; *National Reconnaissance Office* (NRO) responsible for operating SIGINT, IMINT and other reconnaissance satellites; *National Applications Office* (NAO) within the Department for Homeland Security, responsible for centralising and sharing of imagery for domestic purposes. Australia: *Defence Signals Directorate* (DSD) responsible for SIGINT, communications and computer security; *Defence Imagery and Geospatial Organisation* (DIGO) responsible for IMINT. Russia: successor organisation of FAPSI, together with GRU 6th Directorate responsible for SIGINT and communications. UK: *Government Communications Headquarter* (GCHQ) responsible for SIGINT. Canada: *Communications Security Establishment* (CSE), together with the *Canadian Forces Supplementary Radio System* (SRS) responsible for SIGINT.

The distinction between internal and external intelligence services has never been absolute. There are states with a single agency having both internal and external roles. Since risks, dangers and threats are of expanding transnational reach, impact and consequences, ever more intelligence is collected by the different services on the same subjects. The traditional limits between external, internal and also criminal intelligence are becoming increasingly blurred. Missions and objectives overlap, enhancing the opportunities for misunderstandings and rivalries. There is convergence, notably in countering the pre-eminent threats of transnational terrorism, TOC and proliferation of WMD. Hence, the separation of external and internal intelligence services is becoming more artificial and thus questionable.

While separation might still be the best practicable solution for great powers like the US with 16 huge intelligence bureaucracies, it requires an ever greater effort of coordination and control, better regulated access to each other's information and assurance of the production of *joint assessments* and *estimates*. This is why smaller countries with fewer resources might prefer to have just one intelligence service. It avoids wasting efforts, resources and time; solves the risk of unhealthy competition and rivalry between the different agencies; simplifies contacts, liaison, information exchange and cooperation with intelligence services of other countries; facilitates high subordination of intelligence in the state's hierarchy and also cooperation and coordination with other ministries and agencies; and it alleviates control and oversight of intelligence.[100]

Today, the tasks assigned to intelligence services have become more complex, more volatile and more numerous than they ever have been in the past. Because of the expanding need to serve a much broader range of government and other clients with a growing variety of requirements, and this ever more speedily, intelligence services have become too demand-driven. The result is that the intelligence services can no longer do everything at once and do it all well.

2.3 What Are the Problems for, and the Limits of, Intelligence?

The nature of modern terrorism makes it difficult to defeat. The first line of defence against terrorists is the attempt to find out who they are, and what they are up to. This can be done by agents that infiltrate terrorist groups, by using paid informants or through eavesdropping, surveillance and communications monitoring. Controls on financial transactions can be used to discourage money laundering and transfers of illicit funds. But the most important limits to collecting information on terrorists are inherent to the subject and the way they operate. These limits are permanent and cannot be eradicated. Only a few of the conspirators know the intentions. Though they might get help from others, nobody whom they cannot trust completely is informed about their plot. Plans are no longer communicated in a form that can be easily intercepted and interpreted. Terrorists do not expose any materials that would betray their intentions to others.

[100] Among others, the Spanish CNI, the Dutch AIDV, the Turkish MIT, and OSA of Bosnia-Herzegovina are examples of 'fused' intelligence services, which have found their own solutions to overcome the problem that different rules and laws apply to intelligence operations on national soil and abroad.

They do not purchase, procure or build anything that is suspicious. They live and move inconspicuously, and any preparations that cannot be done behind closed doors are done as part of those movements. Moreover, the bulls eye of this intelligence target – an individual terrorist plot – lacks the size and signatures of most other targets. Compounding the problem is the fact that the conspirators may not have had any prior involvement in terrorism or be members of a previously known terrorist group. Thus, the target for intelligence is anyone who might commit terrorism in the future. Hence, terrorism is a fundamentally different and more difficult object than the great majority of other topics the intelligence community is asked to cover. And there can be no guarantee that intelligence services can provide a foolproof warning of an impending terrorist attack so that it can either be avoided or adequate preparations made.

Though the safeguards against non-proliferation are weaker today than 15 years ago, intelligence coverage of proliferation is still somewhat easier than that of TOC and transnational terrorism. Proliferation from state to state dominates, as does that from state to non-state actor, which was the case of Semtex that Libya had acquired and passed to the IRA, and the rockets fired against Israel by Hezbollah in the Lebanon conflict of 2006, which Iran and Syria have provided. Apart from the Abdul Qader Khan mafia network, there are very few confirmed cases of proliferation from non-state actor to state,[101] or from non-state actor to non-state actor. Hence, intelligence collection on proliferation may require less transformation of intelligence services as is the case with TOC and terrorism. However, efforts are needed to more comprehensively reunite, integrate and fuse the disparate intelligence disciplines of analysis of WMD and proliferation; the monitoring of treaties, international organisations, and agencies engaged in proliferation issues; while concomitantly striving to cooperate much more intimately with those engaged in combating terrorism and TOC.

It is obvious that there are limitations in intelligence on WMD. Even before the serious questions raised by the Iraq experience, there were long-standing concerns about the capabilities of intelligence services to track WMD programs and identify required reforms. The track record of intelligence is a mixed one. There have been major successes. There have also been significant failures and chronic dysfunctions stemming from a broad range of organisational, operational and analytical shortfalls.[102]

In key areas related to nuclear, biological and chemical weapons, there continue to be large gaps in knowledge and understanding of both suspect programmes and technology trends. Since 2003, a number of western intelligence communities began conducting 'gap attacks' that focus attention on the most serious and

---

101 There was the German OTRAG, the Orbital Transport und Raketen AG, or Orbital Transport and Rockets, Inc., which set up testing and launch facilities for missiles at Shaba, Zaire in 1975, and later in Libya. OTRAG was accused of missile proliferation to Libya – a project stopped by the then German minister of foreign affairs under pressure from France and the Soviet Union. See: http://www.univ-perp.fr/fuseurop/otra_e.htm

102 See for example: Jeffrey T. Richelson, *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea*, New York, W. W. Norton, 2006. Dennis Gormley, "The Limits of Intelligence: Iraq's Lessons", London, IISS, *Survival*, Vol. 46, No. 3 Autumn 2004. Jason D. Ellis & Geoffrey D. Kiefer, *Combating Proliferation, Strategic Intelligence and Security Policy*, Baltimore and London, The Johns Hopkins University Press, 2004.

difficult of these intelligence deficits. But all were totally ignorant of the fact that Syria, with the help of Iran and North Korea, had built a plutonium reactor at al-Kibar. That the Pyongyang-Damascus-Tehran nuclear axis went undetected and unacknowledged for so long is an intelligence failure of the highest magnitude. It was only thanks to information delivered by a defector to the CIA that Israel was able to launch the air strike that destroyed the reactor in the morning of 6 September 2007.[103]

It is, however, important to have realistic expectations. Determined, adaptive proliferators skilled at deception and denial will find ways to conceal at least some of their activities from even a greatly improved WMD intelligence enterprise. To some degree, uncertainty will always outweigh certainty. Policymakers, therefore, must accept that there are inherent limits to WMD intelligence, while intelligence services are challenged to improve their ability to convey uncertainty in ways that policymakers can understand and apply.

As they work to reduce uncertainty, the intelligence services must sharpen their focus on the 'softer' elements of the proliferation problem – people, plans and intentions. Far too much of intelligence' intellectual and financial resources remain targeted against the 'harder' elements of facilities, technology and systems. This is a legacy of the Cold War era that has diminished utility in the face of today's proliferation challenges. Additionally, intelligence services must continue to transition from simply reporting on proliferation to sustained engagement in the proactive fight against WMD – a fight where even the US Army is deficient in the capabilities required to proactively detect, identify, track and engage threat WMD networks before they launch an attack.[104] Finally, intelligence organisations responsible for setting strategic direction and coordinating community-wide efforts must work more closely with the operational communities to ensure that collection and analysis directly support planning and execution of counter-proliferation missions.

Countering TOC is qualitatively different from fighting proliferation and terrorism. TOC is embedded within economies in ways that proliferation and terrorism are not. Police resources will hardly ever be such that they can do more than investigate a small proportion of TOC. The process of determining targets and priorities is therefore crucial to the intelligence process. A number of problems make this no easy task, for example, should TOC groups be targeted based on the suspected sums of money involved, the degree of occurrence of violence, or the degree of political corruption existing or suspected? And there is always the dilemma of whether to continue surveillance in order to develop intelligence or to act to disrupt TOC activities and to arrest the actors. More and sustained intelligence efforts are needed for anticipating major activities of TOC groups, their operational methods for moving various forms of contraband, innovations in money laundering, the development of new markets and, in

[103] General Ali Reza Askari, Deputy Defence Minister of Iran, defected in February 2007 to the US. See: Hans Rühle, "Wie Iran Syriens Nuklearbewaffnung vorangetrieben hat", *Neue Zürcher Zeitung*, 19 March 2009.

[104] See: *The United States Army Concept Capability Plan for Combating Weapons of Mass Destruction for the Future Modular Force, 2015-2024*, Department of the Army, HQ, U.S. Army Training and Doctrine Command, Fort Monroe, TRADOC Pamphlet 525-7-19, Version 1,0, 25 March 2009.

particular, the measures they are taking to counter law enforcement operations. The latter is of increasing significance, because eluding national law enforcement control is the most important working principle of criminal groups. TOC is becoming ever more adept at concealment and disguise and exhibits a degree of flexibility and adaptability in methods and modes that pose an increasing challenge to law enforcement and society at large.

2.4 Why Is Intelligence Important for Fighting the Pre-Eminent Threats?

Unlike the traditional threats to national security from rival nation-states, the threats posed by non-state actors are more difficult to anticipate, assess and combat. Clandestinely operating conspiratorial groups of often unknown non-state actors make intelligence services central to the security of the state. More than ever intelligence is the prerequisite and most important tool for the prevention of, and timely counteraction against, these new threats. The fact that terrorists, proliferants and TOC groups seek to hide their intentions, plans, capabilities and activities and engage in disinformation, denial and deception operations to mislead the authorities, creates a need for a national organisation with secret and covert capacities capable of being tasked to discover what is kept secret, and to obtain foreknowledge of hidden and unpredictable actions. Such knowledge cannot be acquired better, more safely or more cheaply by any other organisation or means. Thus, intelligence services are a key factor for combating the pre-eminent threats and have become the first line of defence.

But countering the pre-eminent threats from multiplying non-state actors more effectively requires more than intelligence services. In fact, it requires a security sector transformation. The pre-eminent threats can be dealt with only when all actors mandated with the countering of these threats interact with each other more closely. Therefore, existing guidelines, processes and structures need to be transformed. The aim of this transformation must be to strengthen leadership, and to establish effective processes and structures commensurate with the challenges of countering these threats. To this end, three principles form the core of the transformation agenda: *network centric security governance, cooperability, and an intelligence capability orientation.*

Network centric security governance refers to systematic interlocking of four domains: (1) all security sector actors mandated with countering the pre-eminent threats; (2) all levels of decision-making – international, national and local; (3) all security instruments, and (4) all tasks to be accomplished.

The emphasis on network centricity directs attention to *cooperability*, meaning smooth cooperation among security sector actors and between them and relevant third parties. An integrated security approach, however, extends the understanding of cooperability beyond traditional confines in two ways. First, operations commensurate with the new security demands require seamless interplay among all actors. A joint approach of all security sector actors is necessary to improve

efficiency and effectiveness. Furthermore, a joint approach is prerequisite for the second extension of cooperability: cooperation with third parties and with the corporate sector. Both extensions need to take place at the national and the international level, because neither purely national nor single-agency solutions are adequate to deal with these threats.

Capabilities are the currency of the security sector. The provision of capabilities is focused on mission critical functions, rather than the means required for fulfilling them. But the pre-eminent threats can only be effectively counteracted, disrupted, prevented and pre-empted when the *operations of all security sector organisations* mandated to deal with them are *intelligence-driven* or *intelligence-led.*

This requires a radical new approach of more intensive collaboration, interaction and information exchange of these organisation with all agencies of the intelligence community. This new approach calls for the establishment of an intelligence function that produces operational and tactical intelligence in all organisations where it is absent. Foremost, these intelligence cells should do analyses of what is seen, heard and reported by the personnel of their own organisation, from open sources and from intelligence reports exchanged, so that they can accomplish their missions in smarter ways, with more agility, more effectively and efficiently. This is particularly the case in all organisations that suffer from budgetary restraints and a lack of other resources. And in order to improve the information exchange, classified, protected communication means as well as information management capacities must be provided. *Intelligence-led operations* are often cheaper overall. Prevention and pre-emption is more cost-effective than simple reaction. Moreover, proper operational or tactical intelligence allows better targeted and much more tailored operations, generally requiring less resources.

An *intelligence-led approach* is needed foremost in the fight against terrorism. But an intelligence-led approach is equally needed in all agencies and inspectorates that have a mission in the prevention of the proliferation of WMD. This in the work processes of the export-import control and licensing office; the offices that have to survey academic institutions and companies that have stocks of pathogens, high-level microbiological containment facilities and bioreactors; the pharmaceutical sector and biotechnology companies that have expertise in genetics and molecular biology, and the inspectorates that have to monitor bioengineering firms as well as consultants that could help in the industrial microbiological process. Moreover, there are the offices mandated with the surveillance and inspection of the chemical industry, and those in charge of security of nuclear power plants, the nuclear-fuel cycle, nuclear waste deposits, the control of radiation protection and measurement, and the control of radioactive materials used in hospitals, X-rays and irradiation facilities as well as in industry and for food conservation purposes. An intelligence-led approach is equally needed in the work processes of all offices responsible for the prevention of proliferation of missiles, materials or relevant dual-use items.

Also the organisations responsible for homeland defence, the protection of critical national infrastructures, defence against electronic and cyberattacks, and those for the mitigation of terrorist acts and for the engagement of emergency responders should switch to intelligence-led operations.

The *raison d'être* of intelligence is knowledge of intentions, capabilities, methods and means. Its essence is information plus insights derived from subject-matter knowledge. Intelligence provides a sound basis from which inferences can be drawn to guide strategic, operational and tactical activity. Intelligence analyses and assessments inform decision-making and preventive, pre-emptive and disruptive actions *in ways that can make a positive difference in mission accomplishment*. Timely intelligence warns of surprises and looming crises; identifies threats, dangers, risks and chances; monitors fast-breaking situations; illuminates issues and detects trends. And intelligence helps decision- and policymakers consider alternative options and outcomes. All this is also needed in other agencies and organisations of the security sector that are mandated with combating the pre-eminent threats.

The increasing sophistication of TOC makes it imperative to disrupt and demolish network structures instead of merely arresting individual criminals. But attempts to break up criminal networks will never be effective until all available information is developed and transformed into intelligence for use by all government agencies involved in countering TOC. In short, *intelligence-led* operations are needed for the improvement and expansion of the fight against TOC in a more tailored and more effective way.

Although it is within the policing of organised crime that intelligence-led methods have been developed in the first place, all law enforcement agencies have to shift their basic *modus operandi* to *intelligence-led policing*. The same approach also redefines the intelligence functions as they exist or must be developed in other ministries and agencies: the border guard, coast guard and customs services. They cannot function effectively without intimate cooperation, information and intelligence exchange with passport, consular and visa, immigration and naturalisation, migration and health services; export-import, money laundering and financial controls; agencies of the ministries of communications and transport, air traffic control and others, including some private sector enterprises.

3. The Application of Intelligence and the Contributions of Intelligence-led Operations to Fighting the Pre-eminent Threats

For some years now, modern law enforcement agencies have gained great benefits from *intelligence-led policing*. What has been learned from ILP shows the way ahead.

3.1 Intelligence-led Policing

Intelligence-led policing can be defined as "… a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders".[105]

Intelligence methods had long been used by police against organised crime in the US, and there and in some European countries generally for 'political policing' for many years. The intelligence-led policing (ILP) paradigm as it emerged in the UK in the 1999s has its foundation in the recognition of the inability of the traditional reactive model of policing to cope with the inexorable rise in crime. The police were loosing the battle on the streets and public confidence with it. This brought about the rapid growth of private sector security which saw police marginalised in some areas of public safety. Concomitantly, this resulted in increasing calls for police to be more effective and cost-efficient.[106]

The police' search for a new strategy was helped by the 1993 Audit Commission report into police effectiveness[107] that advocated increased use of intelligence, surveillance and informants to target recidivist offenders, so that police could be more effective in fighting crime. The recommendations sought to move the police away from a reactive, crime focus to a proactive, offender focus.[108] This was followed by further official publications that provided a road map to ILP. The aim can be gleaned from the tactical tasking priorities of the UK National Intelligence Model as disseminated by the National Criminal Intelligence Service (NCIS),[109] the four essential elements of which concentrate on:

- Targeting offenders, especially active criminals through overt or covert means;
- Management of crime and disorder hotspots;
- Investigation of linked series of crimes and incidents; and

---

105 Jerry H. Ratcliffe, "Intelligence-Led Policing" in: Wortley R., Mazerolle L., Rombouts S., eds., *Environmental Criminology and Crime Analysis*, Cullompton, Devon, Willan Publishing, 2008.

106 Peter Gill, "Making sense of police intelligence? The use of a cybernetic model in analysing information and power in police intelligence processes", *Policing and Society*, Vol. 8, pp. 289-314.

107 Audit Commission, *Helping With Enquiries: Tackling Crime Effectively*, London, HMSO, 1993.

108 The report was based on three main arguments: (1) Existing policing roles and the levels of accountability lacked integration and efficiency; (2) The police were failing to make the best use of resources; and (3) Greater emphasis on tackling criminals would be more effective than focusing on crimes.

109 National Criminal Intelligence Service, *The National Intelligence Model*, London, 2000.

- Application of preventative measures, including working with local partnerships to reduce crime and disorder.

This focus emphasises that crime is not randomly distributed, with the corollary that identification of hotspots of criminal activity is a worthwhile pursuit. It recognises the importance of working with partnerships to achieve crime prevention, and finally that there should be a spotlight on targeting the criminals and not focus on the crime. This latter principle is based on research, which shows that a small percentage of active and repeat offenders commit a disproportionately large percentage of crimes.

ILP provided an argument for the police to reengage with what they considered to be their core business: fighting crime and arresting serious offenders. Further publications provided the framework for implementation. To promote the idea to all police forces of the UK, in 1997 Her Majesty's Inspectorate of Constabulary identified the central tenets of a successful ILP model:[110]

- Enthusiastic and energetic *leadership* that endorses ILP and promotes it through a *Director of Intelligence;*
- A published *strategy* that sets the *intelligence agenda* for a force, as well as explains what is meant by 'proactivity';
- An *integrated intelligence structure*, so that analysts can work at the hub of operational policing activities;
- Criteria to measure performance to determine the effectiveness of the introduction of the *crime intelligence function* and the tasking of operational units;
- The forging of effective partnerships with local agencies that may be able to help police combat local crime and disorder problems.

At its most fundamental, ILP involves collection and analysis of information to produce an intelligence end product designed to inform police decision-making at the tactical and strategic levels. It is a model of policing in which intelligence serves as a guide to operations rather than the reverse. It is innovative and, by some standards, even radical, but predicated on the notion that a principal task of the police is to prevent and detect crime rather than simply to react to it.

Intelligence is the end result of a process that starts with data, becomes information, that then becomes knowledge and – if employed to have an impact on decisions affecting the criminal environment – intelligence. As Ratcliffe[111] explains, a computer database can store locations of drug-related incidents and arrests. These records are *data* – which can come from open sources (the media or the Internet), government sources (motor vehicle or drivers license records), from suspects and informants, police records, and private but lawfully accessed data

[110] HMIC, "Policing with intelligence", London, Her Majesty's Inspectorate of Constabulary, 1997.
[111] Jerry H. Ratcliffe, "Intelligence-led Policing", in: Wortley R., Mazerolle L., Rombouts S., eds., *Environmental Criminology and Crime Analysis*, Cullompton, Devon, Willan Publishing, 2008.

(like cellular phone records). When a crime analyst analyses the data and recognises a new pattern of drug market incidents at a particular street corner, then this becomes *information* – which is data given meaning and structure, and the understanding of the implications of that meaning. If the analyst talks to a narcotics intelligence officer and shares this information, and the narcotics officer remembers that this was a favourite corner for a particularly violent drug set and that the gang leaders have just been released from prison, this collective understanding of the context of the drug corner now becomes *knowledge*. Finally, when the analyst and the narcotics officer take their knowledge to a senior commander who agrees to mount both a surveillance operation to arrest ringleaders as well as a problem-oriented policing project to identify and resolve why the particular corner is attractive to drug dealers, then this actionable knowledge becomes *intelligence*. Crime intelligence is therefore knowledge that is geared towards action.

ILP is a conceptual model that uses *crime analysis*[112] and *criminal intelligence* – collectively termed *crime intelligence* – in a strategic manner to determine offenders for targeting. Crime reduction tactics concentrate on enforcement and the prevention of offender activity with a particular interest in using *crime intelligence* against the activities of prolific and serious offenders – focussing on the small minority of offenders that commit a majority of crimes. The techniques to be deployed include an expanded use of confidential informants, analysis of recorded crime, and calls for service,[113] surveillance of suspects and offender inter-views.

Where ILP was revolutionary is in the use of intelligence derived from covert information as a *strategic planning resource* rather than as a means to develop case-specific evidence. ILP has become synonymous with the greater integration of criminal intelligence and crime analysis. Criminal intelligence provides information on prolific offenders and organised criminal groups while crime analysis provides the crime context of the environment in which they offend. Both are essential to a full understanding of crime problems and recidivist criminality, and are prerequisites for good decision-making and effective crime reduction.

Already the official embrace of TOC as a problem by the UN in the 1990s served to fuel a growing international interest in ILP. Realising that a reactive, investigation-focussed approach was of diminishing comfort to a public seeking prevention and disruption of future incidents, rather than swift investigations, police in a number of countries began exploring ILP as a framework for the reduction, disruption and prevention of crime. In most, if not all, EU member states, there has been a noticeable shift towards a more proactive ILP approach to tackling all forms of criminal activity. This has been precipitated by the increasing sophistication of many TOC groups, which has made it imperative to disrupt and demolish network structures instead of merely arresting individual criminals. With its adoption in Australia, New Zealand and many other countries, ILP is now

[112] See for example: Rachel Boba, *Crime Analysis and Crime Mapping*, Thousand Oaks, Sage Publications Inc., 2005.

[113] It is well known that service calls – as a majority of crime reports do – often cluster predominantly at specific locations or narrow, easily-defined areas.

firmly established into the worldwide policing lexicon. Most of these police forces have regulated ILP, developed sophisticated crime analysis[114] and IT-supported crime mapping.[115] In 2000, authorities in the UK developed a multi-agency operational response to tackle TOC with intelligence-led operations.[116] And based on recommendations from the Criminal Intelligence Sharing Summit in 2002, the US established a National Criminal Intelligence Sharing Plan[117] to promote information sharing and ILP.

The *UN Convention against Transnational Organized Crime*, the most global international legal reference in the fight against TOC,[118] contains investigative, intelligence and preventive legal tools most conducive to the application of intelligence-led operations. While neither explicitly referring to, nor regulating, intelligence-led operations, Article 20, *special investigative techniques*, is creating sufficient room for the application of *intelligence-led operations*. This, particularly "for the appropriate use of *controlled delivery* and, where [each State Party] deems appropriate, for the use of other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, by its competent authorities in its territory for the purpose of effectively combating organised crime". Article 29, *training and technical assistance*, Article 30, *other measures: implementation of the Convention through economic development and technical assistance*, and Article 31, *prevention*, create the proper environment for the application of *intelligence-led operations across borders*.[119]

Over the last four decades, the standard model of policing[120] in the US was re-shaped by the theories of *community policing*,[121] *problem-solving policing*,[122] *'Broken*

---

114 *Intelligence-Led Policing: The Integration of Community Policing and Law Enforcement Intelligence*, Austin, Texas Police Department, no date; *Intelligence Led Policing: Getting Started, Professionalizing Analysis Worldwide*, International Association of Law Enforcement Analysts, IALEIA, Richmond, 3rd edition, January 2005; *Practice Advice Introduction to Intelligence-Led Policing*, National Centre for Policing Excellence, Wyboston, Bedfordshire, 2007.

115 *Crime Analysis, GIS Solutions for Intelligence-Led Policing*, ESRI, Redlands, 2007, at: info@esri.com

116 Known as Reflex, this multi-agency approach brings together law enforcement, the intelligence community and government departments under a common strategy and shared objectives. It is chaired by the Director General of the National Crime Squad, the operational police organisation responsible for spearheading the fight against serious and organised crime.

117 IACP, "Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels", *IACP Intelligence Summit*, Alexandria, COPS and International Association of Chiefs of Police, 2002. "The National Criminal Intelligence Sharing Plan", The Police Chief, The Professional Voice of Law Enforcement, March 2008, at: http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_

118 See: Pino Arlacchi, *Nations Build Alliances to Stop Organized Crime*, at: http://usinfo.state.gov/journals/itgic/0801/ijge/gj08.htm

119 UN Convention Against Transnational Organised Crime, 2000, at: www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

120 The standard model of policing relies generally on a "one-size-fits all" application of reactive strategies to suppress crime and is based on the assumption that generic strategies for crime reduction can be applied throughout a jurisdiction regardless of the level and the nature of crime or other variations. Such strategies as increasing the size of police agencies, random patrols across all parts of the community, rapid response to calls for service, generally applied follow-up investigations, and generally applied intensive enforcement and arrest policies are all examples of this standard model of reactive policing. David Weisburd & John Eck, "What can police do to reduce crime, disorder, and fear?", *The Annals of the American Academy of Political and Social Science*, Vol. 593, No. 1, 2004, pp. 43-65.

121 Community policing evolved not just as response to the limitations of the standard model, but mainly as a way to re-establish police legitimacy in communities that had lost confidence and trust in the police. It is based on the belief that police should consult with the public in determining operational policing priorities, as well as collaborate with them in the search for solutions. The neighbourhood level empowerment of community officers working with local people on priorities determined by the community is certainly attractive to politicians and the media, but the lack of clear criteria for success has hampered efforts to label community policing a success. See: T. Bennett, "Community policing on the ground: developments in

Windows'[123] and *CompStat*.[124] These theories became powerful change agents for law enforcement agencies interested in providing effective, quality police services. ILP does not replace the concepts of problem-solving policing, or the community involvement and neighbourhood maintenance theories, nor the CompStat police accountability and information sharing practices. It builds on these concepts to keep pace with changes in society, technology and criminal behaviour. Incorporating research findings and advances in ICT, ILP encourages greater use of criminal intelligence, attends to offenders more than offences, and offers a more targeted, forward-thinking, multi-jurisdictional and prevention point of view to the business of policing.[125]

ILP is philosophically closest to *problem-oriented policing*, and to a degree to the accountability mechanism of CompStat, yet is distinct from both in different ways. Problem-oriented policing emphasises the tackling of underlying problems that cause crime, problems that are identified and deciphered through effective crime analysis. ILP similarly defines a strong role for analysis, establishing it as the basis for decision-making that follows. However, where problem-oriented policing is a bottom-up philosophy that places street level police officers at the forefront of problem identification and resolution, existing implementations of ILP are more hierarchical and emphasise the top-down, rank-oriented nature of law enforcement. Criminal intelligence flows up to decision-makers at the executive level, who set priorities for enforcement and prevention and pass these down to lower levels of the organisation as operational tasking.

The hierarchical nature of the intelligence flow is similar to CompStat, which also has a top-down operational structure, where senior managers hold lower ranks accountable for crime levels. ILP, however, has a more holistic view of the analysis of the criminal environment, in that it aims to include information from a wider and richer range of sources in order to better understand the context of the crime patterns often seen in CompStat meetings. ILP also attempts to seek longer-lasting solutions to complex local crime and TOC problems, and to be future oriented and strategically focussed.

Britain", in: D.P. Rosenbaum, ed., *The Challenge of Community Policing: Testing the Promise*, Thousand Oaks, Sage, 1994, pp. 224-248.

122 Herman Goldstein, "Improving policing: A problem oriented approach", *Crime & Delinquency*, No. 24, 1979, pp. 236-258, and *Problem-oriented policing*, New York, McGraw-Hill, 1990. Mike S. Scott, "Problem-Oriented Policing: Reflections on the First 20 Years", Washington D.C., COPS Office, 2000.

123 George K. Kelling & James Q. Wilson, "Broken Windows", *The Atlantic Monthly*, Washington D.C., March 1982. George K. Kelling & Catherine M. Coles, *Fixing Broken Windows, Restoring Order and Reducing Crime in Our Communities*, New York, Touchstone, 1996.

124 CompStat – short for COMParative STATistics – is a management philosophy or organisational management tool for police departments, roughly equivalent to Six Sigma or Total Quality Management (TQM). It is a multilayered dynamic approach to crime reduction, quality of life improvement, and personnel and resource management. It employs Geographic Information Systems and was intended to map crime and identify problems. William Bratton & Jack Maple, "Crime and Restoring Order: What America Can Learn from New York's Finest", 1993. Jack Maple & Chris Mitchell, *The Crime Fighter: Putting the Bad Guys Out of Business*, New York, Broadway Books, 2000.

125 The differences, advantages and disadvantages of these policing systems are well explained by Jerry H. Ratcliffe, "Intelligence-led Policing", in: Wortley R., Mazerolle L., Rombouts S., eds., *Environmental Criminology and Crime Analysis*, Cullompton, Devon, Willan Publishing, 2008.

Key dimensions of 5 policing models[126]

	Standard model of policing	Community policing	Problem-oriented policing	CompStat	Intelligence-led policing
Easily defined?	Yes	No	Fairly easy	Yes	Fairly easy, but evolving
Easily adopted?	Yes	Superficially	Difficult	Managerially challenging	Managerially challenging
Orientation?	Police admin. Units	Neighbourhoods	Problems	Police admin. Units	Criminal groups, prolific & serious offenders
Hierarchical focus?	Top down	Bottom-up	As appropriate for problem	Top down	Top down
Who determines priorities?	Police management	Community concerns/ demands	Sometimes crime analysts, but varies from problem to problem	Police management from crime analysis	Police management from crime intelligence and analysis
Target?	Offence detection	Unclear	Crime & disorder problems & other concerns for police	Crime and disorder hotspots	Prolific offenders & crime problems and other areas of concern for police
Criteria for success?	Increased detections & arrests	Satisfied community	Reduction of problems	Lower crime rates	Detection, reduction or disruption of criminal activity or problem
Expected benefit?	Increased efficiency	Increased police legitimacy	Reduced crime & other problems	Reduced crime (sometimes other problems)	Reduced crime & other problems

Both, CompStat and ILP have the goal of prevention and both bank on processes of constant raw information flow for analysis, and in both cases analysis serves as the basis for operational responses, however, a closer comparison between these 2 models shows some advantages of ILP:

CompStat	Intelligence-led Policing
• Intra-jurisdiction • Incident driven • Analysis based on known facts from reported crime data and investigations • Focuses on crime sprees and incident trends with intent to apprehend specific offenders • Relies on crime mapping, incident analysis, and modus operandi analysis • Time sensitive – 24 hour feedback/response • Predominant focus on 'street crime' – burglary, robbery, homicide, assault, theft • 'Reported criminal incidents' drive collection and analytic parameters	• Multi-jurisdiction • Threat driven • Analysis based tips, leads, suspicious activity reports and information collection • Focused on 'root causes' and conditions that contribute to serious crime and terrorism • Relies on risk analysis, commodity flow, transaction analysis, and association analysis • Strategic – inherently long-term[127] • Predominant focus on 'criminal enterprises' – terrorism, TOC, violence, etc. • 'Intelligence requirements' drive collection and analytic parameters

[126] Jerry H. Ratcliffe, "Intelligence-led Policing", in: Wortley R., Mazerolle L. & Rombouts S., eds., *Environmental Criminology and Crime Analysis*, Cullompton, Devon, Willan Publishing, 2008.

[127] Inherently strategic in that it is used for long-term resource allocation and priority-setting. But it is equally used for shorter-term operational intelligence regarding 'hot spots' in relation to both 'predatory' street crime and 'enterprise' organised crime.

3.2 Criminal Intelligence Analysis

Analysis is key to the effective use of intelligence. Criminal intelligence analysis is defined as: "The identification of and provision of insight into the relationship between crime data and other potentially relevant data with a view to police and judicial practice".[128] The central task of analysis is to help officials – the law enforcers, decision- and policymakers – to deal more effectively with uncertainty, to provide timely warning of threats, and to support operational activity by analysing crime. *Criminal intelligence analysis* is divided into *operational* – some police refer to it as *tactical* – and *strategic analysis*. The difference lies in the level of detail and the type of client to whom the products are aimed. There is debate over the meaning of the terms operational and strategic. To date, there are no commonly accepted and clearly specified definitions, despite efforts by both Interpol (in its crime analysis booklet) and Europol (in its analytical guidelines) to arrive at standardised interpretations.

Operational analysis aims to achieve a specific law enforcement outcome and usually has a more immediate benefit. This might be arrests, seizure or forfeiture of assets or money gained from criminal activities, or the disruption of a criminal group. Operational intelligence is typically of a short-term nature and provides the investigative teams with hypothesis and inferences concerning specific elements of criminal operations, criminal networks and individuals and groups involved in unlawful activities. It also concerns itself with determining specific criminal methodologies and techniques as well as capabilities, vulnerabilities, limitations and intentions. Some may argue that proximity to operations can cause an analyst's judgment to be influenced by the operational team members. Nonetheless, operational intelligence is most effective when it is undertaken as close to an operation as possible, with intelligence analysts working in conjunction with the law enforcement officers involved in the investigations.[129]

Strategic analysis is intended to inform higher level decision-making, and the benefits are realised over the longer term. It is aimed at managers and policymakers rather than investigators. The intention is to provide early warning of threats and to support senior decision-makers in setting *priorities* to prepare their organisations to be able to deal with emerging criminal issues. This might mean allocating resources to different areas of crime, increased training in a crime fighting technique or taking steps to close loopholes in a process. It typically reviews current and emerging trends to illuminate changes in the crime environment and emerging threats to public order. It draws upon a huge variety of information from both within and beyond the law enforcement universe to identify opportunities for action and likely avenues for change to policies, programmes and legislation. Though operational and strategic intelligence analysis have different aims, they are mutually dependent and cannot be carried out in isolation. Attempts to separate them, or to foster one at the expense of the other,

---

[128] The Interpol definition, agreed in June 1992 by an international group of 12 European Interpol member countries and subsequently adopted by other countries. See: www.interpol.int/Public/CIA/Default.asp

[129] Simon Robertson, "Intelligence Led Policing: a European Union View", in: Angus Smith, ed., *Intelligence Led Policing, International Perspectives on Policing in the 21st Century,* International Association of Law Enforcement Intelligence Analysts Inc., (IALEIA), Lawrenceville, September 1997.

will result in a fundamentally flawed intelligence programme and a failure to generate meaningful assessments of criminal activities.

3.3 Intelligence-led Counter-trafficking

The conceptual approach for intelligence collection, analysis and investigations directed against trafficking in human beings (THB) must reflect the geographical, structural and commercial components that make up the crime of trafficking. Geographically and structurally, these can be expressed as:

- *Country of origin* – recruitment and export
- *Country of transit* – transportation
- *Country of destination* – reception and exploitation

Within these three divisions, the *commercial characteristics* inherent in the crime of THB mean that the traffickers are compelled to become involved in one or more of the following activities at any or all of the three geographic phases listed above, irrespective of the nature of the planned exploitation: advertising; renting, buying and use of premises; transportation; communications; financial transactions, etc. The 'Achilles Heel' of THB exists in the 'trail' of evidence that will be created within these commercial imperatives. THB for any form of exploitation can only function by utilising these processes to some degree, and each one creates evidential opportunities for the investigator. More important, each of these domains affords intelligence-collection opportunities for law enforcement and all other agencies, offices or inspectorates directly or indirectly involved in the fight against THB and smuggling.

Strategic as well as operational or tactical intelligence is needed to effectively fight THB. Such intelligence is data and information on all aspects of THB and smuggling, and on the environment in which these take place, that have been subjected to the intelligence process of collection, evaluation, collation, analysis and dissemination. The purpose of such intelligence is to provide knowledge and understanding upon which strategic and operational or tactical decisions can be made by all agencies which can contribute to counter-trafficking in order to identify, prevent, pre-empt, disrupt, interdict or deter THB.[130]

Since there is a need for a broad based approach to the collection and analysis of intelligence, two important factors must be borne in mind in order to avoid adopting an approach that is too narrow: (1) All intelligence on the structure and methodology of a THB network, from beginning of the process to the end, is highly relevant to intelligence collection and analysis on, and to investigations of, THB, irrespective of whether they are done in a country of origin, transit or destination. Recalling the basic philosophy that intelligence is power, the more all those engaged in combating THB learn holistically about the subject, the greater will be their ability to counter it. (2) It is important to avoid the trap of thinking

[130] Taken in amended form from Reference Guide for Canadian Law Enforcement – Human Trafficking.

that the *sources* of intelligence are conveniently divided into the three geographical distinctions of origin, transit and destination countries. While it would be logical to assume that intelligence on recruitment could best be adduced in the country of origin, it is also possible that the highest quality information on this topic may be obtained from interviews held with cooperating victims in the country of destination. The lesson here is that intelligence sources may be found *across the spectrum of crime*, and that all those mandated with fighting THB should adopt a broad based approach to intelligence gathering, analysis and investigation.

3.3.1 Data and information needed on THB

Strategic intelligence

The objective of the collection and analysis of strategic intelligence is to conduct an overall intelligence assessment of the various strategic factors that underpin the existence of THB in a particular state or a group of states, the risks, dangers and threats they pose, and the implications for the own nation and the neighbours. A large proportion of the data used to generate a strategic overview of the situation and an overall intelligence assessment is usually derived from intelligence gathered at the operational level.

Areas of **strategic intelligence** may include:

- **Socio-economic** – Thematic data that can be gathered relating to factors such as economic hardship, unemployment, civil unrest, lack of access to healthcare facilities and medication, feminisation and juvenilisation of poverty, absence of economic opportunities, or any other relevant factors that serve to create and enlarge the supply of actual and potential victims. Thematic intelligence should equally include an understanding of all factors that impact upon the demand side of the cycle.

- **Cultural** – Thematic intelligence on cultural factors that may affect the nature of crime, and the manner in which it is perpetrated is also crucial. These may include cultural beliefs and attitudes that are used by offenders to recruit or exploit victims, or that may affect the attitude of the victims towards those who exploit them, their fears, their willingness to collaborate with authorities, or their eventual rescue, protection and repatriation.131 Common language links may also be a contributory factor as in the case of THB from Central and South America into the Iberian peninsula, from former colonies of the British Empire to the UK, from former French colonies to France, or from Albania to Italy.

- **International relations** – Thematic indicators relating to the historical, ethnic, cultural, economic or colonial connection between countries can also be relevant. This could include information about internal and international

[131] Like 'voodoo' rituals in the case of West African nationals or religious factors that may be relevant, such as the sensitive security issues involved with the repatriation of certain Islamic victims of sexual exploitation to their families in the state of origin.

conflicts; economic and trade relations and competition; military cooperation between states, the presence of foreign troops, of private military and private security companies, or of warlords, paramilitary and armed crime gangs in a state; as well as on international or national labour movements, their activities and strength; the affinity to corruption and blackmail; clans, ethnicities and languages, etc.

- **Patterns and profiles** – Intelligence on recurring crime, THB and smuggling patterns; on patterns of associations, collaboration and division of labour between TOC groups; on patterns of deception, camouflage and elusion of law enforcement control; and on transport, visa and identification requirements. Strengths and weaknesses of border management, customs, immigration, the border guard and coast guard, and other law enforcement and control measures in different parts of the region, are all useful predictors that can be applied in developing prevention and disruption initiatives and in recognising the profiles of offenders and potential victims.

Operational or tactical intelligence

Collection and analysis of operational or tactical intelligence afford immediate and timely support to counter-trafficking operations and ongoing investigations by identifying criminals, networks and gangs, and by providing advance information on their movements, activities and profits. This can lead to specific intelligence-led operations, including arrests, further investigations, prosecution and seizure of profits. And it may serve to rescue victims and to prevent secondary victimisation.

There are a number of key areas of intelligence collection and analysis activities at the operational level. While not an exhaustive list, the following domains require special attention as common elements may assist in investigations as well as in prevention measures:

- **Recruitment methods** – Use of deception, coercion, abduction or kidnapping? What is the person being recruited for?[132] Where was the person recruited from? Intermediaries?

- **Advertising media** – Internet; TV; radio; newspapers or printed media; travel and tourist office; temporary or permanent employment agency; labour unions; or 'word of mouth', etc.

- **Stolen or forged passport, travel documents and identity documentation** – Preparation; acquisition; payment methods used; location of agents or forgers; faking methods and means.

- **Immigration and visa fraud** – Preparation and acquisition; faking methods and means; by corruption or blackmail, where and how?

[132] For example: promise of legitimate work as service personnel, waitressing, domestic service, barmaid, student, au-pair, escort of VIPs, dancer, model, sweatshops, sauna & massage parlours, factory worker or agricultural plantation, etc.

- **Travel routes and means** – Routes followed; mode of travel; patterns of itinerary; ticket procurement and payment methods, etc.

- **Rentals or 'safe house' accommodation** – Location and provision; conditions and particulars of accommodation; owner or intermediaries; access and observation opportunities, etc.

- **Means of communications** – E-mail; mobile phones; fax machines; telephones; mail; dead-drops; brush passes; codes and ciphers; steganography,[133] etc.

- **Financial transactions in respect of all of the above activities** – Modes, methods, means and places used for transactions, payments and money laundering.

- **Information from visa sections, consular, customs and migration services** – All relevant personal data, particulars, conditions and addresses, phone numbers, etc.

- **Information from transportation or travel means** – Airlines; shipping companies; railway companies; trucking firms; truck, bus and car rentals; taxi services; tourist or travel agencies.

It is essential that this kind of intelligence is transmitted to those who are in a position to use it in intelligence-led operations. Expeditious transfer of intelligence is often an issue. A vital factor in effective exchange of intelligence is the speed at which the material can be transmitted to the relevant agencies or investigators, who may be in a position to respond to it. Intelligence very quickly becomes obsolete in the fast moving field of THB operations.

The skilful, focussed and well-targeted collection and analysis of strategic and operational or tactical intelligence is of critical importance in the fight against THB and smuggling, because:[134]

- It enables an accurate assessment to be made of the actual scale, methods and gravity of the crime at the local, national and international levels.

- The assessment enables decision- and policymakers to allocate appropriate levels of resources to address the problem.

---

133 Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realises there is a hidden message. By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. Today, the term steganography includes the concealment of digital information within computer files. For example, the sender might start with an ordinary-looking image file, and then adjust the colour of every 100th pixel to correspond to a letter in the alphabet – a change so subtle that no one who is not actively looking for it is likely to notice it. Steganography used in electronic communication include steganographic coding inside of a transport layer, such as an MP3 file, or a protocol, such as UDP. See: http://en.wikipedia.org/wiki/Steganography

134 See also: United Nations Office on Drug and Crime, *Toolkit to Combat Trafficking in Persons, Global Programme Against Trafficking in Human Beings*, New York, United Nations, 2006, p. 82

- It helps to raise media and public awareness of the crime which, in turn, helps to mobilise the political will to address it.
- The assessment can then serve as a basis for planning a strategic response in areas such as legislative changes, international cooperation, strategies for prevention, and educational campaigns.
- It provides the raw material and forms the basis for intelligence-led proactive, reactive and disruptive investigations of THB.
- It can be used to prevent or disrupt THB and networks in the state of origin, transit or destination, either separately or simultaneously.
- It facilitates the conduct of joint operations between and within states, and may prevent or reduce duplication of investigative efforts in different jurisdiction.
- It allows the identification of emerging future trends related to THB and smuggling, as well as the intelligence gaps which need to be addressed.
- It can lead to the rescue, protection and repatriation of victims of THB and prevent secondary victimisation.
- It can be used to enhance the credibility and relevance of training programmes and education campaigns.

3.3.2 Planning effective responses

Effective responses to TOC in general, as well as to THB and smuggling, call for collaborative, multi-agency, coordinated, long-term strategic and well-planned action. Planning for action must be based on a sound assessment of the problem and of the existing capacity to respond to it. Intelligence collection, analysis and exchange between all relevant agencies and across borders are crucial to the success of all measures taken to contain and disrupt TOC, THB and smuggling.

In a world of decentralised, adaptable criminal networks, the time available between intelligence collection, analysis and operations is dwindling quickly. Assigning these tasks to separate agencies no longer works. This is why government has to defragment i.e. to bring together the scattered efforts in order to be more effective and efficient. The external, internal and criminal intelligence service, police and law enforcement agencies, financial investigative units, border management and all other organisations mandated with fighting TOC and THB must work as closely together as possible. Even when their activities are distributed across different ministries and multiple agencies, all functions and organisations must be aligned around the same mission, must work together to achieve the same goals, and must integrate their respective information seamlessly within the requirements of privacy legislation. In this, they must aim at harmonising practices, utilising as much as possible common procedures and

standards, common risk assessment techniques, as well as select equipment and logistics that facilitate interoperability and joint operations.

Bringing together prosecutors, police, intelligence and security service personnel, auditors, accountants, economists, financial investigators, ITC specialists, social scientists and many others into tightly integrated, highly functional teams with operational latitude is a challenge, but not an insurmountable one. In the US, task forces drawn from different agencies have succeeded in dismantling TOC, THB and smuggling operations and putting away major players in the trade. An integrated view of illicit trade dictates a comprehensive integrated approach to fighting it. And there is no substitute for an integrated entity with full responsibility for this task.

3.3.3 Responses at the national level

Ever more states are forming national task forces or specialised inter-ministerial and interagency units – often under the overall leadership of the criminal intelligence service – for containing and disrupting TOC and THB. Coordination of intelligence gathering and analysis efforts, and intelligence exchange are key functions of such entities. It is important that all assess the situation requiring a response. The problem usually presents itself in a different way in each jurisdiction. Proper assessment of the situation and careful planning of an intervention are usually the hallmarks of successful responses. The best assessments are those that are based on existing effective collaboration and information sharing between the various agencies that need to be part of the response to the problem.

Countering TOC and THB requires a national strategy. However, counter-trafficking strategies based on government action alone are doomed to founder on government's inherent limitations – national frontiers and bureaucratic processes – that traffickers have so adeptly turned to their advantage. If governments cannot curb illicit trade within their own borders, they cannot do it beyond their borders. Illicit trafficking is a bigger problem than any one country, police force, border guard and intelligence service can tackle alone. Government has to be part of the answer – in fact, the most important part. Battling illicit trade calls on lawmaking and law enforcement: pure prerogatives of government. It requires legal, law enforcement and intelligence cooperation across borders. Without the legal authority and coercive power of government, the fight is lost. That makes it all the more worrisome that the illegal trade has managed to penetrate governments. And it makes it crucial that more effective ways are found to equip government for the fight. This is not just a matter of reorganising agencies or boosting budgets. It is also a matter of setting realistic goals and clear, reasonable expectations. The hardest part is never devising a strategy, but mobilising the will to make it happen. And for this it must be supported by a local willingness of the various groups and agencies involved to cooperate not only with each other but also with others at the international level. Given the complexity of the problem of TOC and THB, it

is unlikely that any real success will ever be achieved at the local or national level without ongoing international interagency collaboration.

For national and international collaboration alike, a concrete plan of action must be developed to delineate mutually agreed-upon objectives, priorities for action, and strategies, as well as the many tasks to be achieved, the resources required, and the respective responsibilities of each agency. There are a number of examples of regional, national or even local plans of action. The OSCE and the UNDP, for example, have developed handbooks and best practice manuals which provide several useful assessment tools that could be readily adapted to specific circumstances.[135]

3.3.4 Responses at the international level

International cooperation is imperative. However, working with others is never easy. Working with foreigners is even less so, particularly for governments. The arsenal of international treaties and conventions that govern illicit trade function better to enshrine global standards than to actually enable successful prosecution. Stories of international collaboration undermined by corruption, non-compliance, or absence of trust litter the headlines. But in the case of illicit trade, the alternative to international cooperation is to cede the field to traffickers, who will find ways to penetrate even those states that invest the most in patrolling their borders. Thus, the alternative is not an acceptable one. Better ways have to be found to make international cooperation against illicit trade work.

A novel approach that has shown some success is peer review. Peer review is the method that the Financial Action Task Force, the G-8 group of industrial countries' anti-money laundering and financial crime outfit, has employed. The FATF model is based on a few critical countries opting in by meeting a list of qualifications. Not every country is invited into FATF. The key to FATF's successful operation is mutual trust, which is generated the only possible way – through a careful, deliberate process. The EU makes adherence to its norms on a wide range of issues, including prevention of and the fight against illicit trade, a prerequisite for new members. The shared commitment, as well as the existence of political institutions to enforce it, means that types of collaboration at which other countries might balk are more likely to succeed among the European countries. What is needed is some degree of flexibility with regard to the concept of national sovereignty. The FATF, the EU and other multilateral organisations all limit to a degree the exercise of sovereignty by their member countries with respect to a specific set of issues. This approach in fact provides the only hope to limiting the constant and far more harmful violations of national sovereignty that illicit traffickers inflict on nation states on a daily basis. The lesson here is a difficult one for governments. The most effective forms of cooperation to curb illicit trade are also the ones that invite the most mutual scrutiny: what governments are usually quick to call 'meddling'. Yet without allowing such

[135] See: www.osce.org/documentsodihr/2004/05/2903_en.pdf and: www.undp.ro/governance/Best%20Practice%20Manuals

'meddling', it seems unlikely that governments will ever trust one another, learn from one another, and work together fast enough to keep up with the trafficking networks.

At the international level, police agencies such as Interpol and Europol produce valuable annual threat assessments and situation reports on a country-by-country basis and do useful analytical research on TOC, THB and smuggling that greatly help in the planning of effective responses. So does the UN Office on Drugs and Crime, the UNDP, the OECD, the OSCE and, in other parts of Europe, the Southeast European Cooperative Initiative (SECI Centre), the Baltic Sea Task Force and the Black Sea Economic Cooperation Initiative. But much more needs to be done to maximise reduction of THB and smuggling. In particular, more efforts need to be undertaken to provide national and international agencies with the necessary strategic and specific operational or tactical intelligence to enable them to successfully combat THB and smuggling.

3.4 The Contributions of Intelligence-led Operations to the Fight Against the Pre-eminent Threats

The main contributors are the external, internal and criminal intelligence services, different police and law enforcement agencies, financial investigative units, border management, and joint operations within the EU framework.

Strategic intelligence, consisting of clandestinely collected information on who these actors are, their intentions, capacities and potential impact, is essential to any government response to the pre-eminent threats. For the collection of strategic intelligence, and the provision of strategic analysis on these threats, governments primarily rely on their *Foreign Intelligence* and *Security Services*. Their relationships with their counterparts abroad examining these issues play a key role in their work.

3.4.1 Foreign intelligence service and security service

The main focus of the Foreign Intelligence and Security Service is on containing transnational terrorism and proliferation. Containing and disrupting organised crime is a lower priority. While Foreign Intelligence Services may occasionally conduct covert actions against some of the most notorious TOC groups abroad, they generally do not participate directly in the fight against TOC through apprehension of criminals, seizure of illicit or trafficked goods, laundered money, interruption and closing down of businesses, etc. This remains the mission of the police jointly with the judiciary, customs, the border guard and coast guard, the offices of export-import and money laundering controls, and the inspectorates of the labour, goods, health and intellectual property markets. Rather, Foreign Intelligence Services focus on exploring the influence of TOC groups and figures within selected countries, what threats this influence presents to the own national interests, and prognostications for the future.

They may be required to examine the *bona fides* of certain large commercial entities operating out of so-called 'zones of chaos' in the former USSR, Eastern Europe, parts of Asia, Africa and Latin America, seeking to do business in the own country and the region. 'Due diligence' work of this nature resulting in individual and company profiles is useful to government, economic policymakers, and those involved in counselling on commercial interests. And intelligence assessments of attempts by TOC actors to infiltrate, influence, co-opt and corrupt both foreign governments and the own are of essential interest to government. The Internal Intelligence Service does comparable work internally. But their reporting is mainly strategic and primarily serves as valuable aid to national decision-making involving national interests, policies and strategies to be pursued with regard to the subject country and for fighting TOC. In this, THB is not among their top priorities. In comparison with other crimes, terrorism and proliferation, THB is less a national security issue than a criminal, social and political issue. The criminal issue is the violation of human rights to make exploitation possible, and the illegal earnings gained by the exploitation. Foremost, this demands a rapid, vigorous, professional response on the part of the Criminal Intelligence Service together with police or law enforcement agencies at both the national and international level.

The main contribution of Foreign Intelligence and Security Services to containing the pre-eminent threats is *intelligence collection,* where they are instrumental. Foreign and Domestic Intelligence Services are able to collect in ways for which law enforcement, customs, border management, homeland defence and those offices engaged in prevention of the proliferation of WMD have neither the resources, skills, nor special access. International money laundering, for example, depends on electronic money transfers on which SIGINT of Foreign Intelligence has the monitoring facilities, the duplication of which, due to the great expenses involved, would be unaffordable for most states. Hence, they do the largest part of the collection of data and information that is needed in order to acquire the knowledge about TOC groups, their intentions, plans, organisation and activities. Some SIGINT methods are particularly useful, for example, in the investigation and prosecution of cybercrime cases where evidentiary data may be dispersed across a computer network in unknown places, far removed from where the actual search is taking place. Such knowledge is then disseminated to all agencies and organisations that are able to act on it with intelligence-led operations, but in particular to the *Criminal Intelligence Service* and to *law enforcement*.

3.4.2 Criminal intelligence service

The *Criminal Intelligence Service* – where it exists – is the main contributor, often the lead investigation agency and the overall coordinator of the fight against TOC. It uses crime analysis and criminal intelligence, collectively termed crime intelligence, in a strategic manner to determine offenders for targeting. "Crime analysis is the systematic study of crime and disorder problems, as well as other police-related issues, including socio-demographic, spatial and temporal factors, to assist the

police in criminal apprehension, crime and disorder reduction, crime prevention and evaluation".[136]

To systematically study means to inquire into, investigate, examine closely and scrutinise information. Crime analysis is not haphazard or anecdotal; rather, it involves the application of social science data collection procedures, analytical methods and statistical techniques. It uses qualitative data and methods when examining non-numeric data for the purpose of discovering underlying meanings and patterns of relationships. The qualitative methods specific to crime analysis include field research (such as observing characteristics of locations) and content analysis (such as examining police reports and calls for service). Analysts use quantitative data and methods when conducting statistical analysis of numerical or categorical data. Recent developments in criminological theory have encouraged crime analysts to focus on geographic patterns of crime, examining situations in which victims and offenders come together in time and space.[137] Improvements in IT and the availability of electronic data have facilitated a larger role for spatial analysis in crime analysis. Visual displays of crime locations and their relationship to other events and geographic features are essential to the understanding of the nature of crime and disorder. The final goal of crime analysis is to assist with the evaluation of police efforts. Such evaluations concern two main areas: (1) the level of success of programmes and initiatives implemented to control and prevent crime and disorder, and (2) how effective police organisations are run.

The *Criminal Intelligence Service* has also an important watchdog function over all intelligence collection and investigative activities of law enforcement agencies. This, because all intelligence-led, proactive investigative measures must be implemented in strict compliance with legislative and procedural requirements of the law of the country concerned. This is not just a case of legal and ethical probity, it is a simple case of professionalism. Intelligence-led, proactive techniques require resources in time, personnel and equipment to achieve their full potential, and it would be pointless to expend such resources to gather quality evidence that is then ruled as inadmissible in criminal proceedings because of non-compliance with the law or procedures attached thereto. Moreover, not only would non-compliance be pointless, it would serve to discredit the activity and professionalism of the whole national and regional counter-trafficking response, and this must be avoided at all costs.

3.4.3 Law enforcement and police[138]

The intricacies of law enforcement intelligence, analysis, the intelligence cycle and the legal, ethical and management issues arising from an intelligence function are presented and discussed in a number of venues.[139] Here, we just look at

---

136 Definition given by Rachel Boba, *Crime Analysis and Crime Mapping*, Thousand Oaks, Sage Publications, 2005, p. 6.

137 Idem., see chapter 5.

138 See: UNDP, Law Enforcement, *Manual for Fighting Against Trafficking in Human Beings*, one of the best manuals, at: www.undp.ro/governance/Best%20Practice%20Manuals/

139 See for two good examples: David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, School of Criminal Justice, Michigan State University, East Lansing,

intelligence collection and investigations while focusing on the intelligence-led proactive side. Law enforcement can use three major investigative approaches that are not mutually exclusive:

- *Reactive investigation* – victim-led;
- *Proactive investigations* – intelligence generated, police-led;
- *Disruptive investigation* – police-led option in cases where the other options are not possible.

The proactive, intelligence-led approach

The proactive option provides the means whereby law enforcement agencies can take steps to combat the traffickers without the complaint and evidence of victims. Proactive operations can be resource intensive, take time and can be expensive, but they are an effective weapon and should be considered wherever possible. Experience and best practice have shown that traffickers are particularly vulnerable to proactive, intelligence-led operations. The explanation for this can be found by considering the crime from the same commercial perspective as that used by the traffickers. These may vary their *modus operandi*, alter the routes, switch their identities, and use a range of other tactics to maximise their profits and avoid detection. But there is one feature of the crime that the traffickers cannot disassociate themselves from if their business is to be profitable: the need to market the product by advertising the availability to potential customers or buyers. This commercial imperative creates the 'Achilles Heel' that traffickers cannot escape and law enforcement can exploit. *If the victims can be located so can the traffickers.*

Once it is known where forced labour or sexual exploitation is taking place, law enforcement can identify and locate traffickers and ensure that they are effectively prosecuted by sustained efforts based on solid intelligence collection, analysis and multi-agency collaboration: by using a combination of intelligence, human and technical surveillance, undercover deployments, special investigative techniques and means.

The objective of the proactive, intelligence-led option is to use the most effective and lawful range of investigative techniques, and surreptitious entry techniques, defined as 'entry by stealth', in order to secure sufficient, sustainable evidence to arrest and successfully prosecute the trafficker, and, where possible, to identify, sequestrate and confiscate his assets.

For the attainment of this objective, the strategy to follow is to capitalise on the most promising developments already underway: such as enhancing, developing and deploying new technology. The extraordinary pace of technological innovation is beginning to yield tools with unprecedented potential to help fight illicit trade, tools that counteract the anonymity-enhancing developments and

---

November 2004, and Joseph A Schafer, ed., *Policing 2020: Exploring the Future of Crime, Communities, and Policing,* Center for the Study of Crime, Southern Illinois University, Carbondale, 2007, Chapter 8, The Future of Law Enforcement Intelligence, pp. 226-256.

border porosity of the recent past. Science as a vital arm of intelligence is here to stay. Identification, surveillance, tracing and detection are the new watchwords of R&D.[140] Most of these means are already in use:

- **Biometrics** – the use of unique physical characteristics to identify a person, has the potential to deeply disrupt the market for millions of passports that are lost or stolen around the world each year. It also has the potential to make premises and offices safer by restricting access.
- **Radio frequency identification devices** (RFID) – that overtake the familiar bare code as one of the best ways to identify an item and confirm its authenticity, register origin and date of manufacture and record its price.[141] These are also a potential tool for passports and visas.
- **Global positioning satellite location-tracking technology** (GPS) – to track humans, such as cell phones loaded with GPS software, that are popular among parents to make sure that children are going where they say they are or that they are safe. Applying radioisotopes on traffickers enables to trace these for at least 24 to 48 hours. And microchips implanted under the skin can help to locate people in the event of abduction.
- **Surveillance and eavesdropping devices** – by using existing audio[142] and video bugs, acoustic, seismic, magnetic, optical sensors, accelerometers[143] fluidics[144] or other sensors,[145] as well as the products born of the revolution in nano-technology, such as wireless micro-electromechanical sensors as small as a grain of sand in size.[146] Also radio frequency flooding of installations[147] as well as difficult-to-detect infrared links and laser techniques

---

140 For a good overview over such developments see: Robert Wallace & Keith Melton, *Spycraft. The Secret History of the CIA's Spytechs from Communism to Al-Qaeda*, New York, Dutton, 2008.

141 Radio Frequency Identification Device (RFID) is an automatic identification method, relying on storing and remotely retrieving data using tags or transponders that overtake the now familiar bar code as the best way to identify an item and confirm its authenticity, register its origin and date of manufacture, and record its price. An RFID tag is an object that can be applied to, or incorporated into, a product, animal, or person for the purpose of identification using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader. Most RFID tags contain at least 2 parts. One is an integrated circuit for storing and processing information, modulating and demodulating a (RF) signal and can also be used for other specialised functions. The second is an antenna for receiving and transmitting the signal. A technology called chipless RFID allows for discrete identification of tags without an integrated circuit, thereby allowing tags to be printed directly onto assets at lower cost than traditional tags.

142 For example, a GSM bug, which is like a miniature cellular phone – which one can ring it from thousands of km away, it answers silently and allows one to listen in on conversations. Others look like miniature phone adaptors but in fact are bugs that transmit calls.

143 Used as a specialised type of microphone, the accelerometer can pick up mechanical vibrations directly from the building structure and transmit the audio out of a facility via wire or radio transmitter.

144 Fluidics exploits the way in which acoustic energy travels with relatively low loss in liquids, or in gases if channelled. Thus, if a water pipe picks up acoustic energy, the audio signal can travel long distances within the pipe. Electric conduit or air ducts also propagate audio over substantial distances.

145 A laser beam bouncing off a window can pick up the vibrations of conversations which can then be translated into speech.

146 Scattering such 'smart dust' sensors that can detect, compute and communicate by means of 2-way-band radio THB-related activities and changes in the level of such activities, can vastly improve the gathering of intelligence. Smart dust makes it possible to track individual traffickers over great distances without detection. Dennis Gormley, "The Limits of Intelligence: Iraq's Lessons", London, IISS; *Survival*, Vol. 46, No. 3, Autumn 2004; p. 10.

147 Radio frequency flooding depends on the fact that objects, especially metal ones, vibrate slightly in response to audio in a room. A beam of microwave energy striking the metal object will be reflected from it with some weak modulation imposed by the audio vibrations. If the reflected energy can be collected and demodulated, conversations can be monitored.

can be used for eaves-dropping. Miniature video scanning can be useful for making physiological or behavioural assessments of the traffickers.

- **Other detection devices** – today, stores, building lobbies, parking garages, bank transactions, traffic intersections, streets and subway stations are permanently monitored, videoed or photographed. The combination of the Internet with digital cameras has made such monitoring a very common and inexpensive activity, even at great distances or from high up in the sky. Satellites and new scanning devices can home in on conversations and decipher certain people, vehicles, specific locations, or patters of words.

- **Other security devices** – that can identify suspect items or pick up traces of drugs, explosives and chemical, biological, nuclear and radiological (CBNR) materials far more reliably than the standard X-ray machines, traditional metal and other detectors. Backscatter scanners can contour the body to reveal any foreign items. In addition, 'puffers' which blow air on passengers and analyse the particles set loose can be used. Exploiting new parts of the spectrum, such as hyper-spectral imagery, can be used to identify effluents from buildings as well as thermal emissions by humans.

- **Computers and data-mining tools** – take detection to extraordinary new levels. Banks are spending considerable sums for implementation of anti-money laundering software in order to conform to the requirement that they will 'know their customers'. Behaviour detection applications can monitor hundreds of millions of transactions that large banks process and immediately spot events that fall into suspicious patterns. They can also identify patterns not patently obvious from individual items of information through cluster-, link- and time-series analysis. Crime fighters use similar software for 'social mapping' – logging huge numbers of transactions and interactions to establish the structure and behaviour of networks. Data-mining software can review in a matter of minutes millions of intercepted radio messages, phone calls, faxes and e-mails to find individual items of intelligence. With the proper voice recognition technology, these systems can also match voices contained in thousands of phone intercepts, even if the speaker changes phones constantly while trying to avoid detection.

- **Computer network exploitation** – attacks on information processing equipment are possible by exploiting equipment emanations and by direct or indirect access to equipment software. Easier still is network exploitation by remote access to data and databanks via Trojan horses,[148] trapdoors[149] and more sophisticated means. Keystrokes can be collected straight from the personal computer, before software encrypts the message.[150]

---

148 The *Trojan horse* is a seemingly innocent programme that conceals its primary purpose – to infiltrate a computer for illicit purposes. Emplaced in a word processor, a simple Trojan horse can make a copy of all files that the processor saves.

149 The *trapdoor* is a set of instructions that permits easy access to a computer's software or operating system. It normally bypasses the security routines so that it can be used to enter the system at any time for running tests, upgrading systems, or fixing problems. In many systems a trapdoor enables unlimited access to data in the system.

150 Using for example TEMPEST monitoring devices.

To achieve its full potential, intelligence gathering has to be conducted holistically. The potential of frontline officers 'on the beat' to gather and contribute vital intelligence must be recognised and harnessed to the more specialised work of the counter-trafficking units. Because intelligence-gathering activity cannot and should not be separated from the investigation of the crime, there will always be a degree of duplication, overlap and a blurring of the functions on the issue of when in-depth intelligence gathering become actual investigations.

Best practice recommendations bring the investigator and prosecutor closer together in the investigative process through investigator-prosecutor consultation and planning meetings. Before proactive operations are initiated, a review and planning process is needed that enables the different but interrelated skills and expertise of the specialists to be combined in the assessment of the proposal and the selection of the best legal and operational strategies and tactics to secure the objective of successfully prosecuting the trafficker. There is no point in investigators pursuing evidence-gathering tactics that may be inadmissible, or of no practical use to the prosecutor in the conduct of the trial. Equally, the prosecutor needs to be made aware of the operational difficulties that the investigators may encounter in the conduct of the tactical surveillance options, or may encounter in the seizing and securing evidential material. The intention of such meetings is to conduct a full and frank review of the options so as to identify and formulate the most effective and realistic plan for success of proactive, intelligence-led investigations.

Such meetings of investigators and prosecutors should consider the following points:

- **Operational subject and intelligence profile** – the potential subjects of the proposal and all available intelligence that has been collected and analysed or has been derived from other sources should be reviewed.
- **Operational objective** – the overall objective of the operation should be clearly identified and specified – i.e., the rescue of the victims, arrest and prosecution of suspects, identification and confiscation of assets.
- **Strategies and tactics that are going to be used to deliver the objective** – the strategy should be agreed and set out, including issues such as the scale of the operation. Whether the operation will be confined to the borders of the country concerned or whether it will require international joint operational cooperation. Whether multi-agency partners are involved, and if so, what is their role? The tactical options have to be identified that are going to be deployed, such as human and technical surveillance, interception, controlled deliveries, etc.

Once these issues have been considered and addressed, the decision can be taken as to whether the authority and implementation of the proactive investigation is justified in operational terms. If it is decided that the outline plan would justify the operation, the group will have to address the following set of issues:

Operational flagging

- Where such facilities are utilised, the 'flagging' – the method of assigning operational targets to specific investigative units - of the operation with any relevant local, regional, national and international police agencies becomes essential for 2 reasons: it reduces the risk of 'blue-on-blue' activity, and it ensures that all possible intelligence databases have been interrogated for any additional intelligence on the operational subjects.
- Moreover, it should ensure that any other law enforcement agency enquiry made in respect of those subjects during the course of the operation is brought to the attention of the operational team.
- The use of 'flags' on law enforcement databases is variable and the operational head should use the liaison officer network to ascertain whether they may apply in any particular case.

Risk assessment in respect of the victims

- The process of intelligence on advertisement, rentals, transportation, communications and financial transactions must have been completed prior to the commencement of operational activity.
- The assessment poses the question: what is the level of risk to current, outstanding and potential victims being exploited by the operational subjects and is it acceptable.
- If the answer is no, then the issue of proactive operation does not arise in any event.

Risk assessment in respect of the operation

- This process assesses any level of risk arising from the selection of the tactics.
- For example: what are the risks to the undercover or test purchase officers?
- Are the surveillance officers going to be operating in highly dangerous environments?
- Are the investigation and arrest of the subjects going to have other consequences, for example, will the investigation and arrest of the subjects lead to increased community or cultural tensions?

The risk management plan

Having identified the risks, the investigator and prosecutor should set out the risk management plan to address them. This should include clear instructions to the operational team on five issues:

- The level and type of risk that exists at the start of the operation.
- The risk management instructions, for example, surveillance monitoring of the victims for signs of injury or the lowering of victim ages or the intended transportation of under-age victims.
- Other vulnerable issues; the deployment of safety support teams for undercover or test purchase officers; and operational supervision levels.
- Instructions to the operational team should the level of risk suddenly increase, for example, where child victims are seen being placed into brothels or officers observe violence being used to a victim.
- The process of keeping the risk assessment under review – whether the risk assessment should be reviewed daily, weekly or monthly, etc., and the rank of the officer who should conduct the review.

Final go-ahead and continuity of review

If the investigator and prosecutor are satisfied that the intelligence justifies the implementation of a proactive operation, and that the tactics and risks can all be managed within the objective of securing the arrest and conviction of the subject of the operation, then the implementation of the plan should proceed.

The review process should be maintained throughout the operation. Progress should be regularly reviewed and any new developments that were not foreseen should be considered as soon as practicable. Any requisite adjustments to the strategy, tactics or risk management plan can then be made and logged as the operation progresses.

Decision logging

Since the management and authorisation of proactive operations is a complex matter involving critical decisions across a number of issues, it is very important to ensure that accurate records are maintained of these decisions and the thought processes behind them. The investigator and prosecutor should maintain a joint record of their deliberations and decisions. This record keeping process not only helps to clarify and structure the reasoning and decision-making of the investigation from the outset and as it progresses, it also serves to remind and protect them should any of the decisions be challenged at a later date, either during the trial process or from any other source.

How these logs are created is a matter for local practice. The ideal model is a separate, uniquely numbered log book in which each decision and the reason behind is entered, dated and countersigned by the parties involved in it. Where entries relate to the action and agreement of other agencies, they should be counter-signed by the representatives of those agencies. For example, if it has been agreed with immigration and customs agencies that a controlled delivery will be allowed to go ahead, the details of the plan, the parameters of it and their agreement to it should be recorded and countersigned by each agency official.[151]

[151] *Law Enforcement Manual for Fighting Against Trafficking in Human Beings – Best Practice*, UNDP Romania, Vienna 2003, Section 6, pp. 6-3 to 6-6.

3.4.4 Parallel financial investigations

The critical role of financial investigation in the successful investigation of THB cannot be overstated. The golden rule is: "Follow the money and you will find the traffickers".

The financial aspect of the crime of THB presents itself in at least two important ways:

- THB itself is all about money. In addition to the initial investment to create the infrastructure and deliver people for exploitation, the ongoing management of the proceeds of the exploitation and, finally, the laundering and movement of the profits have to become part of the activities of the traffickers.

- THB is a crime that takes time to establish and develop. This is why it often becomes a lifestyle crime. Other offender lifestyle aspects, such as the mode of travel, expenditure on luxury items such as cars and jewellery, and leisure activities will point at the illegitimate revenues of the offenders.

In transnational cases, diversity of legislation, procedure and resources can become an issue. This is especially the case with financial investigations.

A proactive, intelligence-led investigation can be conducted both during the pre-arrest and post-arrest investigative phases. When applied during the proactive pre-arrest phase, its use must be considered against the risk of disclosing the law enforcement operation. However, most versions of asset confiscation legislation contain punitive provisions for any individual or institution that discloses the fact of a financial enquiry to the account holder. This reduces the security risks that are always attached to proactive enquiries in the pre-arrest stage.[152]

3.4.5 Border management

Effective and *integrated border management services* are critical to ensuring the safety and security of citizens, promoting regional stability and facilitating trade and development. Today's border management agencies are challenged like never before. Globalisation and the pre-eminent threats have ushered in a climate that demands high performance and total responsiveness. Border management has to cope with and reconcile two opposing trends, one that pushes trade liberalisation and the opening of borders, while the other urges for *more secure borders in terms of prevention of crime and illegal trade*, and *early action*. Hence, the need for ever more efficient, rapid and open movement of travellers and goods coincides with heightened demands for more secure traveller and cargo identification before, at and within a country's borders, and this without compromising an individual's basic rights and privacy.

---

[152] Taken from: *Human Trafficking. Reference Guide for Canadian Law Enforcement*, Abbotsford, BC, University College of the Fraser Valley Press, May 2005.

There are a number of measures that states can take to make it more difficult for THB to move people across borders. These measures are included in the *Trafficking in Persons Protocol* and the *Migrants Protocol*. Under article 11 of both protocols, states parties are required to strengthen border controls to the extent possible and, in addition to measures pursuant to article 27 of the *Organised Crime Convention*, to consider strengthening cooperation between border control agencies, including by the establishment of direct channels of communication. Under article 12 of both protocols, states parties are required to ensure the integrity and security of travel documents. And under article 13, they are also required, at the request of another state party, to "verify within a reasonable time" the legitimacy and validity of documents purported to have been issued by them. In addition, there are the measures recommended by the OSCE.[153]

At its most basic, effective border management requires the identification of people and goods, the collection and analysis of relevant information, and timely dissemination of relevant information to help officers make informed admissibility decisions regarding the eligibility of travellers and cargo. For this, an integrated border management environment must be created that enables low-risk persons and cargo to move conveniently across borders, while law enforcement agencies must work together to efficiently identify and interdict higher-risk individuals and cargo.

Integrated border management requires promoting increasing cooperation at three different levels that are central to raising border management efficiency and effectiveness: (1) improving the vertical flow of information within border services from the ministry to the units working at border posts; (2) increasing horizontal cooperation between officers of the different services active at the border, as well as among the central ministries responsible for the services; and (3) international cooperation between agencies involved in border issues in different countries, which is important for confidence building and to facilitate joint action on common issues. With this, the pre-conditions can be established for: (1) an intelligence-led approach, understood as border management that relies on information that is gathered by and exchanged among all relevant agencies within a state, aimed at decision-making on resources, operations and investigations, and (2) intelligence-led cross-border cooperation via interstate intelligence sharing with emphasis on risk assessment and joint investigations, for which multinational and multi-agency cooperation are imperative to be successful.

Border guard, customs and **immigration services** are the main actors responsible for managing the movement of people and goods across borders. In every country a variety of other actors are involved in tasks related to border management. While their focus may be different – as are their objectives – they should all work towards a common goal: ensuring open but well controlled and secure borders. Achieving this balanced approach is often a complex and delicate task.

---

153 *The OSCE Action Plan to Combat Trafficking in Human Beings*, at: www.osce.org/documents/pc/2005/07/15594_en.pdf

Border guards can be a civilian or paramilitary law enforcement service. Their main objectives are: (1) preventing cross-border criminal activities and unlawful entry; (2) detecting national security threats through surveillance of all land and water borders; and (3) controlling persons and vehicles crossing the border at designated points.

Customs are a fiscal service whose responsibilities typically include: (1) ensuring that customs duties are properly paid; (2) ensuring that all goods are identified and accounted for when entering the territory of a country; and (3) enforcing restrictions on entry and exit of goods when this is justified on grounds of public policy and security; protection of the health and life of humans, animals and plants; the protection of national treasures with artistic, historic or archaeological value; or protection of industrial and commercial property.

Immigration services generally have responsibility for: (1) enforcing restrictions on the entry and exit of people on grounds of policy or security; (2) ensuring travellers have the correct and genuine documents required to cross international borders; (3) raising revenue by issuing the requisite entry/exit visas at border crossing points; (4) identifying and investigating trafficking and smuggling; and (5) identifying and assisting those in need of protection such as victims of THB, asylum seekers, refugees, and carriers of pandemics and other sicknesses.

Border management is one field of state activities that most requires an integrated approach to be effective. The wide range of national and international border management agencies with specific roles, and the close links these must entertain with law enforcement; intelligence and security services; export-import, financial and money laundering controls; migration and health services; the non-proliferation, environmental, agricultural, food, trade and intellectual property inspectors; the entities responsible for transport, communications and air traffic control; and the armed forces, etc., makes it imperative that all operate as *one enterprise* in countering THB. This is also the case for the *defence* and *military intelligence services* and the *armed forces,* which can support border management agencies with the engagement of sophisticated reconnaissance, surveillance and observation means[154] in order to improve control of land and sea borders, or in a crisis.

What is legal and what is illegal is determined by the law and implemented by state institutions. However, the standards and norms are not the same in all societies, and the level of effective implementation varies widely. When a transnational element enters crime, successful prosecution often becomes more difficult. When the criminal acts take place in different jurisdictions, the criminals can only be successfully tried if all the parts of the international investigative puzzle are laid next to each other and interlinked. This requires international police and judicial cooperation. Yet there are many obstacles to such cooperation – different legal systems, bureaucratic inertia, the pervasiveness of corruption in some law enforcement services and judiciaries, the simple lack of resources and skills, and

[154] Among others, UAVs, radars, airplanes and helicopters, infrared, ultraviolet, hyper-spectral, acoustic, magnetic and movement sensors, as well as range of MASINT means.

even linguistic incompatibility. Nonetheless, enhanced cooperation and exchange of information must stretch from *countries of origin* for THB to *countries of transit* as well as to *countries of destination*. And success requires a clearly defined *strategy* across all border management functions, the *policies* to support the strategy, and a *governance* and *leadership structure* that provides continual, *clear direction*.

3.4.6 Intelligence contribution within the framework of the EU

The EU integrated border management system

In Europe, the EU has made significant progress in developing an *integrated border management system* and for border management agencies operating as one enterprise. The EU security model goes beyond typical interstate cooperation in terms of major achievements made in reconciling the opening of borders on one side, and increasing human and state security on the other, as well as in intelligence sharing between the member states. In the EU Council's view, integrated border management consists of the following five dimensions: (1) border control (checks and surveillance) as defined in the regulation establishing the Community Code, including the necessary risk analysis and criminal intelligence; (2) investigation of cross-border crime; (3) a four-tier access control model (measures in third countries, cooperation with neighbouring countries, border control, and control measures within the area of free movement); (4) cooperation between the authorities in the field of border management at the national and international level (border control, customs and police authorities, security services and other relevant authorities); and (5) coordination and coherence of action taken by member states and institutions. The key principle is that *border management must cover all border related threats*.

At the *national level*, criminal intelligence, implemented in cooperation between police and law enforcement, the border guard, customs, the national intelligence and security services, visa, immigration and health services is 'best practice'. At the *multilateral level*, it is *joint investigations*. However, it is essential to develop not only joint operations of the EU, but also regional cooperation between border authorities. The Baltic Sea region has an effective cooperation model in use within which all states in the region – both EU member states and Russia – have been cooperating at operational level for 12 years now. A similar model has been developed for the Mediterranean in the framework of Medsea.

The Schengen system – the Community Code on the rules governing the movement of persons across borders[155] – represents an exemplary model of modern border security management as regards reconciliation of the two

[155] Relevant norms and best practices can be found in the OSCE Border Security and Management Concept, MC DOC/2/05 of 6 December 2005. EU integrated border management rules are spread across a number of legal and administrative instruments, representing a multi-layered compilation of provisions, with only the basic ones found in the formal texts such as the Treaty on the European Community or the Schengen instruments of 1985-90. Much of the rest has been adopted through informal arrangements like the *Common Manual* on external borders adopted by the Schengen Executive Committee, and the *Catalogue of Best Practices* drawn up by the Working Party of Schengen Evaluation.

opposing trends, one pushing for the opening of borders to facilitate trade and economic growth, and the other that calls for efficient prevention of the pre-eminent threats and combating TOC. The EU disposes of its own agencies for the production and exchange of intelligence: Europol for criminal and security intelligence; Joint Situation Centre – SITCEN – for external intelligence; the intelligence division of the EU military staff – INTDIV – for military intelligence; and the EU Satellite Centre – EUSC – for imagery intelligence.[156]

The Madrid terrorist attacks have given a strong impetus for further developments fighting the pre-eminent threats and put intelligence at the forefront of border security management and policy. The EU Council reached agreement on political strategic guidelines, namely on the *Integrated EU Border Management Strategy*,[157] the European Arrest Warrant,[158] on biometrics in passports, on the establishment of the European border agency FRONTEX,[159] on the exchange if information on lost and stolen passports with Interpol,[160] and on the introduction of EURODAC that prevents asylum seekers from submitting multiple asylum applications in different EU countries.[161] The European image archiving system False and Authentic Documents FADO[162] makes possible the speedy verification of documents and fast, comprehensive notification of relevant law enforcement or immigration authorities in other participating states, when misuse of a document or a fraudulent document is detected. And the capacity of the Council Secretariat has been expanded to provide analytical support to the Council as it tackles counterterrorist policy.[163] Moreover, states can prevent the use of commercial carriers as a means of transport in THB by requiring them to ascertain that all passengers possess the travel documents required for entry into the destination state.[164] Failure to do so results in appropriate sanctions, the so-called 'carrier sanctions'. Furthermore, the air transport industry has introduced and contributed interesting proposals for intelligence-led border management.[165]

Recently, the European Commission's communication on an integrated EU border management strategy presented the creation of a *European Border Surveillance System* EUROSUR,[166] with the main purpose of preventing unauthorised border crossings, reducing the number of illegal immigrants losing their life at sea, and

---

156 Björn Müller-Wille, "Building a European intelligence community in response to terrorism", *European Security Review*, No. 22, April 2004, pp. 3-4.

157 Sergio Carrera, *The EU Border Management Strategy*, CEPS Working Document No. 261, March 2007.

158 See: http://europa.eu/cgi-bin/etal.pl

159 See: www.frontex.europa.eu/

160 The number of stolen or lost travel documents recorded internationally has gone from just over 3000 in 2002 to over 10 million in 2005. This astronomical increase of more than 3000 percent is alarming. It shows not only the need for improved technological systems to detect false passports, but also for improved training of staff on how to identify counterfeit or forged documents.

161 See: www.edps.europa.eu/EDPSWEB/edps/pid/39 and http://europa.eu/scadplus/leg/en/lvb/133081.htm

162 See : http://europa.eu.int/comm/justice_home/fsj/freetravel/documents/printer/fsj_freetravel_documents_en.htm

163 European Council, "Brief Note On Counter-Terrorism", Brussels, 2004, at: http://ue.eu.int/uedocs/emsUpload/Brief_note_counter-terrorism16.12.04.pdf

164 The Council Directive (EC) 2001/51 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement OJ L187 (10 July 2001). Council Directive (EC) 2004/82 on the obligation of carriers to communicate passenger data OJ L261 (6 August 2004). Council Directive (EC) 2003/110 on assistance in cases of transit for the purposes of removal by air OJ L 321/26 (6 December 2003).

165 See for example: *Intelligence-led border management, Harnessing the power of the data in air transport industry systems*, SITA, Weyside Park, Godalming, Surrey, no date.

166 See: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/86&format=HT

increasing the internal security of the EU by contributing to the prevention of cross-border crime. EUROSUR should support the member states in reaching full situational awareness[167] at their external borders and in increasing the reaction capability of their law enforcement authorities by using new technologies such as satellites. It will provide the common technical framework for streamlining the daily cooperation and communication between member states' authorities and facilitate the use of state-of-the-art technology for border surveillance purposes.

Key operational objective should be the sharing of information, excluding personal data, between existing national and European systems. Taking into account the current migratory pressure,[168] in a first step the integrated network should be limited to the Mediterranean Sea, the southern Atlantic Ocean (Canary Islands) and the Black Sea, and focus on internal security, linking border control authorities and other authorities with security interests and responsibilities in the maritime domain together. At a later stage, this integrated network of reporting and surveillance systems could be extended to the whole maritime domain of the EU, covering not only border related aspects, but all maritime activities, such as maritime safety, protection of the marine environment, fisheries control, and law enforcement.

New tools

At the same time, the Commission's communication suggests new tools, including: (1) proposals for the introduction of an *entry/exit system*, allowing the electronic recording of the dates of entry and exit of third country nationals into and out of the EU using the *Schengen Information System* (SIS II)[169] and the *Visa Information System* (VIS);[170] (2) proposals to facilitate border crossing for *bona fide* travellers through the introduction of *automated border crossing facilities* that read the biometric data – facial image and fingerprints – in travel documents for EU citizens and certain categories of third country nationals; and (3) parameters for the possible introduction of an *Electronic System of Travel Authorisation* ESTA, and the development of common access to EU databases. In addition, the Commission wants to strengthen the role of FRONTEX by "implementing the current mandate of the Agency in full, in particular by intensifying joint operations between member states, including sea border patrols". Among others, the possibility of creating a *European Border Guard*, improved cooperation between customs and other border control authorities, and better exploitation of FRONTEX technical equipment by the recently established *Rapid Border Intervention Teams* RABITs is foreseen.[171]

---

167 See: *Public Safety and Homeland Security Situational Awareness*, An ESRI White Paper, Redlands, February 2008, at: www.esri.com and http://en.wikipedia.org/wiki/Situation_awareness

168 It is estimated that there were up to 8 million illegal immigrants within the EU in 2006.

169 See: http://europa.eu/scadplus/leg/en/lvb/133183.htm

170 See: http://europa.eu/scadplus/leg/en/lvb/114517.htm

171 See: Franco Frattini, *Providing Europe with the tools to bring its border management into the 21st century*, Ministerial Conference on the Challenges of the EU External Border Management, Brdo, Slovenia, 12 March 2008, at: www.libertysecurity.org/article1939.html

As a result, two major strands of information and intelligence exchange need to be engaged: on the one hand, the increasingly important cooperation with third countries and, on the other hand, the horizontal integration of information and intelligence sharing measures being put in place in-country and at the borders, among others, in a bid to improve cooperation between customs and other border control authorities in the fight against THB.

3.5 New Ways of Combating Organised Crime

In the US, the Customs Service and its parent ministry, the Department of the Treasury, have a long history in the fight against TOC in its many forms. Through the decades the law enforcement mission of the Treasury Department and the Customs Service in particular has expanded tremendously. Today, the Customs Service agency is tasked with an ever widening range of enforcement responsibilities ranging from traditional investigations involving drug and weapons smuggling to complicated money laundering and child pornography trafficking schemes, to the illegal movement of equipment, technology and even knowledge which can be used in the development of WMD. In all of these areas, the rapid advancement in technology and science provides both benefits and significant challenges to the law enforcement community. Today's organised criminals, proliferators and terrorist groups are making full use of easily accessible technology to further their activities. Drug smugglers are using encrypted telephones and the Skype of Internet to protect their conversations, counterfeiters are using high-powered computers and laser printers to produce currencies, child pornographers are using the Internet to communicate and trade illicit wares, and money launderers are utilising sophisticated trade transactions to disguise the movement of funds throughout the world.

When one combines these technological advances with the growing demand to open borders and governmental efforts to expedite legitimate international business and financial transactions, one can easily see the challenges ahead.

In the US, the federal government has learned that the most successful approach to combating TOC of all types is a well coordinated joint investigation bringing to bear the capabilities and strengths of the various federal, state and local law enforcement agencies. It was not until the 1980s that the US formalised this approach with the Organised Crime Drug Enforcement Task Forces. This joint or task force approach enables one to focus on all aspects of a criminal organisation. One agency may focus on financial activity; another on the individuals and potential sources of information within the organisation and another might coordinate the electronic interception of communications. Utilising the expertise of the various federal agencies, the prosecutors, as well as state and local law enforcement in this type of format has proven to be very effective.

These programmes have proven to be so successful that it has spread to the creation of Task Forces specifically targeting terrorism. The US government has created a number of Joint Terrorism Task Forces throughout the country, which

is hosted by the Federal Bureau of Investigations (FBI). The task forces require full time participation from officers of agencies such as Customs, Immigration, Alcohol Tobacco and Firearms, Secret Service, US State Department Investigators and state and local police officers. These task forces target any criminal activity of identified terrorist groups or those associated with the group. In many instances, these groups may not be planning terrorist acts but may be supporting them through financial and logistic support. The goal of the task force is to disrupt and dismantle these organisations utilising any and all means available. This may mean arresting an associate for overstaying his visa, seizing goods and funds not properly declared at the border, arresting individuals for credit card fraud, or simply issuing citations for various violations.

Future successful efforts to combat organised crime will be dependent on formal joint international law enforcement efforts as well as the utilisation of advanced technologies for information management, collection and analysis. These avenues must be aggressively pursued while still respecting the independence and sovereignty of each nation and working within the laws of each of those states. Some technical areas that should be the focus of consideration might include the automated exchange of information pertaining to international travellers, the ability to automate retrieve and exchange information related to the movement of vehicles, vessels, shipments and containers from one country to another throughout their journey, legislation to require the retention of records by Internet providers, enhanced suspicious financial activity targeting capabilities, and the sharing of intelligence for law enforcement purposes. These are the basic foundations that will lead to successes against TOC.

4. Patterns and Problems of Intelligence Cooperation

4.1 Intelligence and Law Enforcement Cooperation

Countering the pre-eminent threats requires close cooperation between law enforcement and intelligence agencies. More than ever before, intelligence and law enforcement must find new and better ways to work together to deliver integrated results for the government and the security and safety of the nation. Valuable insights can derive from close correlation of information from differing intelligence, security or law enforcement sources. The US is by far not the only country that has learned with painful clarity that failure to share, coordinate and connect available intelligence can have devastating consequences.[172] Thus, much more sharing is required – vertically and horizontally, internally and externally.

Bringing law enforcement and intelligence closer together is not without some challenges. The two communities have long-established roles and missions that are separate and based on constitutional and statutory principles. Both use the word intelligence in very different ways. For *intelligence services*, intelligence means puzzle solving[173] or mystery framing[174] that is good enough for action. The goal is policy. The context is a blizzard of uncertainty, often one that cannot be melted down into clear contours. And the standard is 'good enough to act'. By contrast, for *law enforcement,* intelligence is instrumental in another sense, not for policy but for cases. Intelligence means tips to wrongdoing or leads to wrongdoers. The goal is convictions. The context is individual cases. And the standard is that of the courtroom – to be beyond reasonable doubt.[175]

Intelligence' work is essentially forward-looking, seeking to predict and forestall emerging threats to the state and society. *Police work* usually involves collecting evidence on a case-by-case basis *after a crime has been committed* with a view to prosecute the perpetrator. Law enforcement is intentionally a reactive tool. The investigators seek to determine whether elements of a crime are present and whether they can be associated with a given suspect or a given set of facts. Law enforcement becomes proactive only when a suspect threatens to break the law. For *intelligence*, which must warn, that is simply too late. Intelligence collection seeks to understand those indications of hostile intent that may be cause for alarm.

Moreover, *police* most often want to arrest and charge criminals, while *intelligence services* want to leave them in place and see how far their networks lead and where the top bosses are. Thus, information sharing difficulties abound. Because intelligence services are careful not to reveal their sources and methods,

---

172 See: Steward Baker, *Wall Nuts: The Wall Between Intelligence and Law Enforcement is Killing*, at: http://www.newamericancentury.org/defense-20040106.htm

173 Puzzle solving is seeking answers to questions that have answers, even if these are often and long not known. Basically, puzzle solving is frustrated by a lack of information. Collecting secrets is crucial in solving puzzles.

174 Mysteries pose questions that have no definite answers because the answers are contingent, depending on a future interaction of many factors, known and unknown. A mystery cannot be answered; it can only be framed by identifying the critical factors, and applying some sense of how they have interacted in the past and might interact in the future.

175 Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge, Cambridge University Press, p. 167.

intelligence officers try hard to stay out of the chain of evidence so that they cannot be asked to testify in a court of law. As a practical matter, that means that intelligence's role is limited to tipping off other agencies.[176] *Intelligence agencies* are unwilling to let covert intelligence material be used in making a criminal case against the perpetrators of crimes, while *police* will not allow evidence crucial to an ongoing investigation to be passed outside the bounds of the investigation. True, information used in judicial proceedings is often of a different type than that usually collected by intelligence services. It is collected and stored differently, and must usually *be shared to some extent with opposing attorneys*. However, this problem may be more prevalent in the US than in Europe, where in most countries initiatives have been undertaken to enhance the usefulness of information collected by intelligence services to law enforcement agencies and vice versa.

Intelligence and *security services* have cultural and bureaucratic incentives not to share their information with each other or with those outside the service. These include a natural impulse to hoard information to protect turf, and an ingrained passion for secrecy. Security services and law enforcement on the one hand, and intelligence agencies on the other, traditionally have resisted sharing information with each other. Management of intelligence not only has to alter agency incentives and culture to require sharing, but also has to address the excessive emphasis on secrecy and classification that inhibits constructive, timely information flows, while continuing to respect the need to protect sources and methods. However, the risks of sharing information must now be balanced against the risk of not 'connecting the dots'.

A key issue is the overall direction of the effort. Law enforcement may require that some information be closely held and not shared outside the organisation or the ministry. But if law enforcement and intelligence efforts are to work more closely in dealing with the terrorist, proliferation of WMD and TOC threats, procedures will have to be in place to ensure that important information is shared. For this, a seamless system encompassing all echelons of intelligence and law enforcement agencies for storing and exchanging information in real-time on the pre-eminent threats has to be established. Most, if not all, of the technological impediments to protecting sources and methods while enabling effective information sharing have been solved. Technology has to be embraced as a key in easing the administrative burdens of sharing information. But for this, channels for transferring information must be clearly established, and close encouragement and oversight by both the executive branch and parliamentary oversight committees is required to ensure a smooth functioning of transfer arrangements.

A recurring concern reflected in reports about activities of those involved in the 9/11 attacks has been the perception that information about possible terrorist involvement of individuals may not be available to security officials of immigration, visa, border guard and coast guard, airport and transportation services – to those who encounter the individuals. Sharing between all these critical interfaces was underdeveloped, especially in the US. There have not been

[176] Ibid., pp. 167-168.

centralised databases containing intelligence by which individual names could be checked. Hence, there is a clear need to ensure that all these agencies and organisations have better access to information acquired by intelligence services about potential terrorists, proliferants, and illegal criminal and THB activities.[177]

For information sharing to succeed, there must be *trust*. Building trust requires strong leadership, clear laws and guidelines and advanced technologies to ensure that information sharing serves its important purpose and operates consistently with national values. Both communities must ensure compliance with the laws and make the commitments visible to the public.

People have a natural tendency to resist change. For this reason, leaders throughout the law enforcement and intelligence communities must consistently and repeatedly deliver the message of change and ensure that everyone understands the importance of sharing information. It is no longer enough to share intelligence: there is *a responsibility to provide it*. Moreover, the public wants and deserves collaborative intelligence and law enforcement communities effectively working together to prevent harm and destruction. Leaders must understand and nurture change that emphasises the responsibility for providing information, not just for sharing it. They must also communicate to their subordinates a willingness to accept risk in sharing data, and they *must deemphasise data ownership*. What is also needed is greater *inculcation of civic values:* that the success of others is a shared success in service to the nation and its citizens.

Effective and focused training can improve the confidence of the community members as well as the public's perception that information is being handled appropriately. The right training, coupled with good policies, clear guidelines and rules, will better enable sharing and ultimately will help *change the cultures*. These steps, along with intercommunity training, exchange of 'lessons learned' and the effective use of technology, can open doors of cooperation that have been closed for too long.

4.2 Cooperation With and Within the EU

Formal police cooperation between the member states' representatives began in 1976 with the creation of working parties known as 'Trevi groups'. It main subjects were terrorism and the organisation and training problems of police departments. By 1989 there were working parties on terrorism, police cooperation, organised crime and the free movement of persons. This system prefigured the intergovernmental structure set up by the Schengen agreements and the Treaty of Maastricht. The Schengen system set up liaison officers in the signatory states to coordinate the exchange of information on terrorism, drugs, organised crime and illegal immigration networks and introduced a right of pursuit across frontiers. The Treaty of Maastricht spelt out matters of common interest on which it sought to encourage cooperation: terrorism, drugs and other forms of international crime.

[177] See: William J. Krouse, & Raphael F. Perl, *Terrorism: Automated Lookout Systems and Border Security: Options and Issues*. Congressional Research Service; The Library of Congress, Report RL31019.

It also provided for a European Police Office – Europol – together with a system for exchanging information throughout the EU.

The Treaty of Amsterdam has given priority to preventing and curbing TOC. It defined the objectives of the member states and the relevant authorities, calling for cooperation between police forces, customs authorities and the courts to ensure a high level of safety. European police cooperation ranges from administrative and operational cooperation between police forces or through Europol to coordinated campaigns to fight organised crime and safeguard law and order. In 2000, the Council adopted an EU strategy on prevention and control of TOC, that contains a number of political guidelines, particularly with regard to establishing reliable data, protecting the public sector and the legitimate private sector, reinforcing prevention, improving legislation, backing up investigations, confiscating the proceeds of crime and increasing cooperation between the police and judicial authorities at both the national and EU level.

The European Council has named terrorism as one of the major threats to the EU's interests. In 2001 it drew up a plan of action, revised in 2004, setting out the EU's strategic objectives in the fight against terrorism. It appointed a Counter-Terrorism Coordinator who coordinates the Council's work and ensures effective monitoring of its decisions. In 2005 the Council adopted a new EU strategy aimed at combating terrorism.[178]

In the EU migration issues have dominated the political agenda since years. As early as February 1997, the Council adopted a joint action to combat THB and sexual exploitation of children.[179] A more comprehensive process was started in the Tampere European Council in October 1999. Its presidency conclusions reflect well the duality of the EU's approach. On the one hand 'it would be in contradiction with Europe's tradition to deny freedom to those whose circumstances lead them justifiably to seek access to our territory'. This liberal principle was complemented, however, by the protective one; the 'common policies of asylum and migration' must provide 'consistent control of external borders to stop illegal immigration'. The Council paid particular attention to the need to tackle illegal immigration at its source. In 2008, the Council of Europe Convention on Action against Trafficking in Human Beings came into force. It defines common guidelines for the jurisdiction, the nature of offences, penalties, and sanctions pertaining to THB.

[178] The European Council Declaration on Combating Terrorism of 25 March 2005 and the Council Declaration on the EU Response to the London Bombings of the 13 July 2005 following, respectively the Madrid and London attacks; the Plan of Action on Combating Terrorism adopted in June 2004 and revised every six months, the Commission's Communication on prevention, preparedness and response to terrorist attacks COM (2004) 698 adopted on 20 October 2004 and The Hague Programme adopted by the European Council in November 2004.

[179] 97/154/JHA.

4.2.1 Interpol

European governments have been officially working together against TOC since Interpol was founded in 1923. Today, Interpol has developed into a global body. Based in Lyon, it has 186 members worldwide, sharing information via a network of national central bureaus (NCBs). Interpol maintains databases on known criminals, lost and stolen passports, fingerprints and DNA profiles. In 2003, it rolled out a global police communications system called "I-24/7", securely connecting the NCBs to each other and to Interpol databases, widely praised as a clever solution to the problem of how to share sensitive police data electronically in a multilingual environment. In 2005, police used "I-24/7" to exchange almost 10 million messages worldwide.

One of its areas of responsibility is to maintain and develop strategic alliances with other regional and international organisations whose objectives are compatible with Interpol's stated aims. Thus, in Europe, Interpol has cooperation agreements with the Stability Pact for South Eastern Europe, the Southeast European Cooperative Initiative (SECI), the Southeast Europe Police Chiefs Association, the UN interim administration Mission in Kosovo (UNMIK), the European Union Police Mission in Bosnia and Herzegovina (EUPMBH), the Task Force on organised crime in the Baltic Sea region (BSTF), the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX), the International Law Enforcement Academy (ILEA) in Budapest, the International Centre for Migration Policy Development (ICMPD), and many others.[180] The cooperation agreement with Europol was approved by the Council of the European Union on 27 June 2001. Interpol and Europol have since implemented various joint projects, mainly on THB, money laundering and Euro counterfeiting.

4.2.2 Europol

The establishment of Europol reflected the ambition to create an integrated system of police cooperation and analysis across the EU. Europol is the EU's main tool for assisting investigations into TOC. Europol gathers and analyses intelligence on crimes ranging from THB to counterfeiting and terrorism, and produces an annual threat assessment for member states.[181] This threat assessment highlights the dangers to the EU from TOC and suggests ways member states can tackle it. Until 2003, the standard tool for assessing TOC in the EU was the annual *European Union Organised Crime Report* (OCR),[182] which had been met with quite some criticism regarding its meaningfulness, and has then be replaced by an alternative tool, the *EU Organised Crime Threat Assessment*. However, OCTA has also met with fundamental criticism.[183] Because many member states follow their

---

180 See: www.interpol.int/Public/Region/Europe/coopInitiatives.asp

181 See: *OCTA 2008 EU Organised Crime Threat Assessment*, Europol, The Hague, 2008, at: www.europol.europa.eu

182 Europol, *European Union Organised Crime Report 2003*, Luxembourg, Office for Official Publications of the European Communities, 2003.

183 Tom Vander Beken et al., *Measuring Organized Crime in Europe: A feasibility study of a risk-based methodology across the European Union*, Antwerp-Apeldoorn, Maklu, 2004. Petrus C. van Duyne & Maarten

own course, great obstacles exist for a harmonised European approach to assessing TOC, making it difficult for Europol analysts to make valid cross-European comparisons.

Europol's office is organised in a hub-and-spoke system. All member states send police officers to its headquarters in The Hague. These officers act as spokes, sharing information directly with each other as well as with a hub of Europol crime analysts. The analysts comb the combined body of European criminal intelligence for TOC trends and links that can be missed by national or regional police forces. Europol officers cannot make arrests or initiate investigations, but they can assist during investigations and be present during the questioning of suspects if required by a member state. Since 1999, Europol has focused mainly on developing analytical abilities that it needs in order to add value to national investigations. Initial sceptics among police throughout Europe have by now come to view Europol more favourably and as a potentially useful channel for coordinating the fight against TOC. But Europol has yet to become indispensable in cross-border investigations, partly due to serious bureaucratic problems that inhibit its usefulness. It has been criticised for inefficiency, cumbersome procedures and has been plagued by intra-institutional and political expediencies. But Europol can only work on the basis of data that its national contact points provide, and input from some states has been minimal.[184] Recurring lack of trust constitutes a major obstacle to the development of the agency, which is also surrounded by concerns regarding its accountability and democratic control. However, today EU governments want to give the office a greater role in supporting member states investigations aimed at putting top level criminals behind bars. And by 2010, Europol will become a full EU agency.

4.2.3 Multilateral police cooperation

Efforts to enhance police cooperation in the EU have been taking place for a number of years now. Successive legislative and constitutional developments have granted the EU competence to act in the field. Article 29 and 30 TEU and the Europol Convention provide the legal basis for EU police cooperation. Major steps have been the creation of the 3rd pillar in the Maastricht Treaty and its amendment in Amsterdam, and the incorporation of the Schengen acquis in Community law by the Amsterdam Treaty. In parallel with the Amsterdam negotiations, the member states came up with the first EU 'Action Plan' to fight TOC, which recommended the establishment of Europol, EU level action to fight money laundering, practical steps to improve cooperation between national police, customs and judiciaries, and priority areas for harmonisation of laws to fight

van Dijck, "Assessing Organized Crime: The Sad State of an Impossible Art", in: Frank Bovenkerk & Michael Levi, eds., *The Organized Crime Community: Essays in Honor of Alan A. Block*, New York, Springer, 2007, pp. 101-124. Klaus von Lampe, "Measuring organized crime; a critique of current approaches", in: Petrus C. van Duyne, M. Jager, Klaus von Lampe & J.L. Newell, eds., *Threats and phantoms of organized crime, corruption and terrorism*, Nijmegen, Wolf Legal Publishers, 2004. Klaus von Lampe, "Making the second step before the first: Assessing organized crime. The Case of Germany", *Crime, Law & Social Change*, 2004, No. 42, pp. 227-259.

[184] In 2006, while one member state contributed over 500 pages of criminal intelligence to Europol's first organised crime threat assessment, another offered only a single page.

TOC. The governments added new goals to this list in 2004, renaming it the 'Hague Programme'. This programme, and the subsequent Action Plan[185] to implement it, attempted to remedy some shortcomings by both building on existing EU initiatives and calling for the tabling of new measures at EU level.

Its most important goal has been a promise to revolutionise how European police forces share information across borders by adhering to the 'principle of availability', in effect since January 2008. The principle of availability means that throughout the EU, police forces no longer need to formally request information from each other, or rely on informal 'old boys' networks to get information. Police from one EU country now has access to police files in any other country, and the law enforcement agency in the other state which holds this information will make it available for the stated purpose, unless a good reason is given to the contrary.[186] As to cooperation between police and intelligence agencies, the Hague Programme called for particular consideration to be given to the special circumstances that apply to the working methods of intelligence and security services – including sources of information, methods of collection and confidentiality.[187]

4.2.4 Cooperation within the framework of Justice and Home Affairs

Combating TOC has also become a priority area for EU legislation and its fast-growing *Police and Judicial Co-operation Matters* (PJC), formally *Justice and Home Affairs* (JHA) – the 3rd of the three pillars of the EU. In 2004, member states agreed a radical expansion of EU powers in crime and policing, issues which cut to the bone of national sovereignty. In negotiations on the EU constitutional and reform treaties, governments agreed to drop national vetoes on decisions about crime and policing, though law enforcement will remain strictly national. They also agreed to make it easier for the EU to *initiate criminal legislation and align national court procedures*.

Interior and justice ministers now regularly meet in the EU's Council of Ministers – the JHA Council – and discuss how to implement The Hague Programme. They do so by closing legal loopholes between member states' criminal laws, and agreeing legislation and practical steps to make cross-border police investigations easier. Officials develop new proposals in an enormously complicated web of committees that make up four different levels of decision-making. These include working groups on police, customs and criminal justice cooperation, and the 'multi-disciplinary group on organised crime'. The latter is a group of national policing experts with powers to evaluate crime fighting methods throughout the EU. Officials from both the Council and the Commission help governments to draft legislation. They also give views on the effectiveness of previous EU agreements. Two most important committees are COREPER, the powerful

185 *Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union*, Council document 9778/2/05 REV2. See also the earlier Commission Communication *The Hague Programme: Ten priorities for the next five years*, COM (2005) 184 final.

186 Point 2.1, p. 27. *And Proposal for a Council Framework Decision on the exchange of information under the principle of availability*, COM (2005) 490 final, 12 October 2005.

187 Point 2.2, p. 29 and COM (2005) 695 final, 22 December 2005.

grouping of member states' ambassadors to the EU, and the committee of high-ranking interior and justice ministry officials (called CATS, after its French name Comité de l'Article Trente-Six).

4.2.5 Eurojust

A major part of the JHA Council involves replacing the slow Council of Europe procedures for police and criminal justice cooperation with faster, more efficient EU rules, such as warrants speeding up the extradition of suspects and the sharing of evidence between the member states. Euro just, a unit of senior prosecutors, judges and police officers nominated by the member states, helps with making these legal arrangements work in practice. It also has the day-to-day role of co-ordinating multi-country prosecutions in the EU. The year 2007 was an important landmark for Euro just – the historic crossing of 1000 cases handled, representing an increase of 314 cases or 41 percent over 2006.[188] It opened 71 THB cases, compared to 29 in 2006. And it aims to establish a *centre of expertise on THB*.

4.2.6 The European criminal intelligence model

In 2005, ministers of the interior agreed on a *European Criminal Intelligence Model* (ECIM),[189] a policing plan for coordinating investigations against TOC throughout the EU and *intelligence-led* policing. The idea is to get police from different countries to plan investigations together, using the best intelligence available. The ECIM sets out how the EU can achieve this by ensuring that national police forces, Europol's criminal intelligence analysts and the police chiefs' COSPOL operations work together against the same criminal threats. The model works in a number of steps. First, member state police forces share intelligence with Europol, which draws up an assessment of the overall threat facing the EU from TOC. Based on this, the Council of Ministers agrees on the law enforcement priorities that police forces should tackle together. The EU police chiefs then mount joint operations against the criminals and feed back information and 'lessons learned' into Europol, in time for the next threat assessment to be prepared.

EU member states tested this new way of working together for the first time in 2006. Based on Europol's first threat assessment, EU governments set four regional priorities in the fight against TOC in Europe. These were drug trafficking and THB by African gangs operating in the Mediterranean; Albanian gangs trafficking both heroin and women from the Balkans; commodity smuggling in the Baltic Sea region; and illegal factories for synthetic drugs in Belgium, Germany, The Netherlands and the UK. It is too soon to tell if governments or police are taking ECIM seriously enough. But the adoption of a EU law enforcement model is a significant step forward in coordination of internal security. The police model is also a subtle attempt to promote the use of *intelligence-*

188 Eurojust, *Annual Report 2007*, pp. 7 and 33.
189 See: UK Presidency of the EU 2005, *Annex – A European Criminal Intelligence Model*.

led policing methods throughout Europe. However, law enforcement cooperation across Europe as a whole has yet to match the degree of cooperation achieved by TOC. This is due to a number of basic difficulties.

4.2.7 Different police organisations

Europe's 1.2 million police officers operate in very different and, at times, incompatible ways. Ireland, Denmark and Finland each have one single national police service, centralised under a clearly designated 'chief', whereas in The Netherlands and the UK, the police are decentralised, with the UK having as many as 50 separate police forces. This means the smaller regional forces may not be able to answer requests for information or cooperation from counterparts in other countries. Moreover, in a number of countries, police have independent powers of investigation, while in others they still take their lead from national prosecutors. Police answerable to prosecutors tend to be reactive, acting only after a crime has been committed, and do less preventive work. This difference in roles means that both police officers and prosecutors from different countries divide into *proactive* and *reactive* when deciding how TOC should be tackled.[190]

4.2.8 Different rules for investigations and admissible evidence

Another problem hampering cooperation is that countries have different rules for starting investigations and gathering evidence. There are 27 legal systems in the EU, each one with its own rules for starting investigations. In the UK, for example, it is illegal to use phone taps as evidence in court, but police can and do rely of closed circuit television (CCTV). By contrast, France sees phone tapping as legitimate and human rights-compliant, but considers indiscriminate use of CCTV footage to be far more intrusive. In other EU countries, public CCTV cameras are as of yet unknown, or, as in Denmark, even banned by law.

4.2.9 Council of Europe Convention on Mutual Assistance in Criminal Matters

Police may be able to get around these differences when working informally with their foreign colleagues. But they, and the courts, still face a range of obstacles to the conduct of cross-border investigations and prosecutions. If they need a witness summons, an order to compel somebody to produce evidence, a search-and-seizure warrant or an order to freeze bank accounts, they may have to ask a court in another country to issue one. The main tool for getting this kind of work done is the 1959 *Council of Europe Convention on Mutual Assistance in Criminal Matters*, under which judges approve requests for help with investigations and prosecutions from abroad. In 2000, the Council of Europe updated the convention to include requests for *undercover operations* abroad, the *interception of phone and Internet communications across borders* and *surveillance operations* such as '*controlled deliveries*' – where authorities secretly monitor crimes such as drug

[190] Hugo Brady, *The EU and the fight against organized crime*, London, Centre for European Reform, CER, Working Paper, April 2007, at: www.cer.org.uk

trafficking to unearth a criminal network.[191] Even revamped, the convention is too complex and inflexible to provide a basis for modern crime fighting: the new changes are taking years to ratify, and requests can take weeks, months and even years to be answered. The UK, for instance, requires too much detail from countries making requests, while the Spanish bureaucracy can misplace request altogether.[192]

4.2.10 The extra powers of police forces from Schengen countries

Aside from the pitfalls of formal legal cooperation, European governments have made efforts to boost operational cooperation among police. This is particularly true in the now passport-free zone of the EU: the 'old' EU minus Britain and Ireland, with the addition of Norway, Iceland and Switzerland, and the exception of Cyprus. Police forces from Schengen countries have extra powers to pursue crimes with a cross-border dimension. For example, Dutch officers can carry out surveillance on suspects in Belgium, with or without prior notification. Italian policemen can follow suspected criminals in 'hot pursuit' into Austria – until the local police arrive. This thanks to a patchwork of bilateral and multilateral agreements. Cooperation is most sophisticated where countries share land borders, have similar legal systems and face common threats from the same TOC groups or terrorists. Police in the Benelux countries assist each other in every day law and order matters. The Nordic countries have been running joint patrols and police stations in sparsely populated border regions for years. So too have the Spanish with their French counterparts.

4.2.11 The headway made by the Treaty of Prom

In 2005, Austria, the Benelux countries, France, Germany and Spain formed an information sharing *avant-garde* outside the EU by concluding the *Treaty of Prom*. It aimed to further the development of European cooperation, to play a pioneering role in establishing the highest possible standard of cooperation, especially by means of a much speedier exchange of information, particularly in combating TOC, terrorism and illegal migration, while leaving participation in such cooperation open to all EU members. The extended security cooperation measures comprise among other things: sharing of DNA and fingerprint data, common rules on flight security, vehicle registration databases, and cross-border 'hot pursuit' of officers without prior consent of the convention parties in urgent situations.

Some observers feared the convention would undermine efforts to facilitate sharing of information in the EU as a whole, since it involved only a handful of countries, ignored related initiatives by the European Commission, and created a new hierarchy within the EU and a new form of the Schengen process. But it turned out that the Prüm Treaty was the best way to encourage wider information

191 Idem.
192 Eurojust, *Annual Report 2005*, p. 46.

sharing. Its members have acted as a 'laboratory', working out the complicated technical arrangements for querying each others' police databases quickly and effectively in a small group.[193] The rapid progress has encouraged the rest of the EU to adopt the Prüm system and, in February 2007, the member states agreed to incorporate the information sharing bits of the treaty into the EU' legal order. If this agreement is implemented on time, every EU member state will have automatic access to others' DNA, fingerprint and vehicle registration databases by 2009, a "quantum leap in cross-border sharing of information".[194] The challenge for the future is to make the Prüm information sharing arrangements work well with 27 countries. Overall, the Prüm experience is an important case study for the future of police cooperation in the EU.

4.2.12 The outlook ahead

Any reform of national policing structures must be based on the constitutional order of each country and its specific traditions. Not all countries will want to follow Britain in setting up a powerful separate agency, such as the *Serious and Organised Crime Agency* (SOCA), which integrates several police organisations devoted to gathering criminal intelligence, as well as law enforcement parts of the UK Customs and Immigration Services.[195] But all member states should at least have *common platforms* like the French *Section Centrale de Coopération Opérationelle de Police* (SCCOPOL) in Paris, where representatives from the different law enforcement agencies work together, and are on hand to coordinate investigations with colleagues abroad. In Italy, a similar unit in Rome maintains such a platform, where representatives from all six Italian police forces work on TOC.

Another aspect urgently needing improvement for rendering the fight against TOC more effective and efficient in Europe is that representatives to both Europol and Eurojust need to have *equivalent powers* if either organisation is to function properly. The obvious way to overcome such challenges would be to merge both Europol and Eurojust to form a single European law enforcement coordination body, incorporating also the police chiefs' task force. A single body could underpin a uniform level of cooperation across the EU whatever the national law enforcement structures. It would also prevent duplication in intelligence gathering and analysis and ensure better follow-through from investigation to prosecution in cross-border cases.

Furthermore, as Brady convincingly pointed out: "One of the most useful things the EU does for improving cooperation against TOC is also one of the most

---

193 Austrian and German police claim that adopting the Prüm procedures produced over 1,500 new leads in unsolved cases.

194 *Justice and home affairs Council, press release*, 15 February 2007. at: www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/92800.pdf

195 SOCA has powers to use phone tapping, undercover officers and new surveillance techniques to make sure that previously convicted criminals do not re-establish their networks. SOCA handles all international cooperation between Britain's assorted police forces and their counterparts abroad. It deals directly with Interpol and Europol, and cooperates with Schengen area countries on behalf of all UK police. An interesting aspect of SOCA is that it has adopted a 'harm reduction' rather than 'law enforcement' model for its work. It is perhaps too early to judge what its impact has been but it is clear that it has given it some legitimacy problems as some of its members who were police have expressed considerable frustration.

basic: it helps the member states to copy each others' *best practice*. EU officials carry out *'peer evaluation' of police methods* in each member state and draw up recommendations for improving their law enforcement systems based on *best practice*. If member states aligned their investigative methods, technology and training, they would benefit far more from cross-border cooperation. The JHA Council should give more weight to these evaluations. It should agree on 'headline' goals for the use of ICT and modern police equipment, as well as for the adoption of modern policing methods, including procedures for seizing criminal assets and conducting financial investigations".[196]

[196] Hugo Brady, op. cit., p. 30.

5. Intelligence-led Operations and Democratic Oversight

5.1 The Need for Tighter Democratic Control, Supervision and Oversight

Maintenance of internal and external security of the state is vital and essential for the protection of the population, the critical national infrastructures, the national interests and other values of the state. Only a strong state can counter threats from abroad, ensure a satisfactory level of law and order, and the full protection of human rights internally. However, with the advent of the pre-eminent threats, predominantly by non-state actors of the unholy trinity of transnational terrorism, proliferation of WMD and TOC, external and internal security merge and become indistinguishable, with the concomitant accentuation and prevalence of threats coming from within: clandestine, often unknown terrorist networks and shadowy TOC groups operating at the heart of our societies. This is why intelligence has become the main weapon of the state in the struggle against these threats. In order to protect itself against, and to anticipate, prevent, deter and pre-empt these and other threats to national security, a state needs a strong security sector with more effective security and intelligence services, and with police, border management and all other agencies mandated with fighting these threats being capable of conducting *intelligence-led operations*. All these are, and must be, equipped with considerable technological tools and enjoy exceptional powers. Intelligence has thus become an inescapable necessity for modern governments.

An effective security sector is one where all security sector elements operate with professionalism within a democratic system of civilian control and oversight that ensures accountability and transparency. A professional security sector is one that understands not only its intelligence, law enforcement, border management and financial control duties, but also its proper relationship and responsibilities to society at large. A democratic system of civilian control and oversight can vary in its design but serves the critical function of ensuring that the security sector is held accountable to the needs and priorities of the public. Regardless of the particular form of control adopted in democracies, most relevant democratic control of the intelligence services and of the activities of all agencies that conduct intelligence-led operations must be exercised by executive, legislative, judicial and also by independent entities. Every element plays its specific role within the whole package of control, supervision, oversight and accountability. The purpose is to provide assurance of legality, proportionality and propriety for all collection activities that are necessarily conducted in secret.

There are enough manuals of best practices available on how democratic control, supervision and oversight should be modelled, can best be established and handled in the security sector, and for democratic control of intelligence and security services in particular.[197] There is neither need nor room here to repeat

[197] For the latter see: Hans Born, Loch K. Johnson & Ian Leigh, eds., *Who's Watching the Spies?, Establishing Intelligence Service Accountability*, Dulles, Potomac Books, 2005, also Hans Born & Marina Caparini, eds., *Democratic Control of Intelligence Services. Containing Rogue Elephants*, Aldershot, Ashgate Publishing Ltd., 2007. See also: the Council of Europe Venice Commission, *Report on the Democratic Oversight of the Security*

what has been so well and thoroughly explained in these works. What we will look into are the changes that have taken place since the advent of the pre-eminent threats, and the implications these changes may have for democratic control, supervision and oversight.

In short, these changes are enormous. External, internal and criminal intelligence services, as well as all the security sector agencies that conduct *intelligence-led operations*, have to collect as much information as possible on threats to the state. However, wherever this involves intelligence collection on individual members of the state – nationals as well as foreign residents – there is the danger that collection activities *impinge on individual, human and privacy rights of the persons*. This danger is greater today because the new threats require a transnational and network-based response from the state that involves proactive and closer operational collaboration between intelligence and security agencies, police, customs, immigration, border guard, export-import, financial and money laundering control authorities and other state bodies. The problems of control and oversight are aggravated yet further by the incorporation of the corporate sector into these multi-agency networks. Such an integrated multi-agency effort can only be successful with greatly enhanced inter-agency communication, collaboration and intelligence sharing at the national and international level. Operating as one enterprise, aligned around the same mission and working together to achieve the same goals while integrating their information and intelligence seamlessly, makes democratic control, supervision and oversight more difficult. Control, even by government, is made more difficult by the very nature of secret intelligence collection, where government becomes more dependent on the specialist knowledge of the experts.

Physical and administrative capacities may previously have set some limits on the extend to which intelligence could interfere with people's freedoms, privacy and human rights. However, major technological advances in data-mining, collection, processing, analysis and surveillance activities have dramatically increased intelligence collection capacities. Moreover, intelligence is now used in more varied ways, for example for security screening and in relation to decisions on entry into a country, to grant citizenship or to deport aliens. It is therefore essential that there be internal and external limits to intelligence collection activities. Furthermore, individuals must be better protected against an abusive or illegitimate use of the information collected about them. This is why there is a need for tighter democratic control, supervision, oversight and accountability, and also for a different kind of control.

Services, Adopted at the 71st Plenary Session, June 2007, at: www.venice.coe.int/docs/2007/CDL-AD(2007)016-e.asp

5.2 The Problems Accruing to Democratic Control, Oversight and Accountability

The starting point of difficult problems accruing to democratic control, supervision, oversight and accountability is the *increased intelligence collection capacities*. These increased capacities are brought about by the need that all agencies mandated with fighting the pre-eminent threats apply *intelligence-led operations* in order to become more effective, and by the major technological advances that enhance intelligence collection quantitatively, if not in all circumstances also qualitatively. Collecting information on individuals immediately raises the issue of respect for civil liberties, individual rights and freedom. Increased intelligence collection capacities enhance the damage intelligence can do to the vital values of democratic societies, in particular, to human rights, the enjoyment of the rights of freedom of expression, association, privacy and to personal integrity.

The EU is founded on the rule of law and the respect of international conventions, and its member states are to respect the right to life (article 2), the ban on torture and on inhumane or degrading sentences or treatments (article 4), the right to protection in case of displacement, expulsion or extradition (article 19), the right to an effective appeal and a fair tribunal (article 47), and should actively protect these rights if a third country infringes on them. And within the EU, the personal data of an individual belongs to this individual and not to the service that has collected it. No treaty contrary to this principle can be adopted; consequently, it is up to a potential partner to change its legislation shall an agreement be reached. Comprehensive precautionary measures against such violations have to be established.

The vulnerability of democratic societies, combined with the diffuse nature of the pre-eminent threats against them, means that intelligence is wanted on everything which is, or can become, a danger. Unless some limits are imposed, and continually re-imposed, then the natural tendency on all agencies engaged in the fight against the pre-eminent threats is to over-collect information. While good internal controls and professional staff should set limits on the collection of data and information, internal limits may not suffice. Because it is not the staff of an intelligence agency, or of the agencies conducting intelligence-led operations that can make a decision on the delicate balance between national security and the damage which over-collection of intelligence can do to the vital values of democratic societies, such limits have to be set by law – in the mandate of these organisations.

Moreover, it is obviously not simply a question of collecting intelligence. Intelligence is collected to be used in a number of ways, which leads to a number of additional problems, particularly for the collaboration of agencies that operate at the intersection of law enforcement and intelligence gathering. If the intelligence is intended to lead to prosecutions and convictions, it must be of a different quality – be beyond reasonable doubt – compared with, for instance, intelligence intended for warning purposes or for helping to prevent security threats from materialising. But 'hard' data – purely factual information – is mostly

insufficient for a security agency or, for that matter, any law enforcement organisation. They also need to gather *speculative intelligence* in order to determine which people are, or are probably or possibly, a threat to security and safety. Such information can be obtained in different ways. A large proportion of classified source information comes from informants. Like factual information, such 'soft intelligence' can and must – if the agencies do their job properly – be collated to produce a personality profile of a suspect or an analysis of a suspected activity. This means that the filing system must be constructed in such a way as to facilitate linking of information on the same subject matter filed often after some time, as well as allowing synthesis of apparently unrelated information, for example, to discern patterns of activity.

Furthermore, all entries must be graded to indicate the *reliability of the source* and the *credibility of the information*, and the grading must be periodically re-assessed. The data system must also allow all operators to obtain quick overviews of large quantities of data. Basically, however, security and intelligence officials, and also crime analysts, make a value judgment on the available information as to whether a particular person is a security risk, and if so, what exactly he or she is up to. It is thus a question of *risk assessment*, and this inevitably involves a *large degree of subjectivity*. Obviously, it takes a long time for any external monitoring body to penetrate the arcane world of intelligence to understand what is a reliable and credible intelligence assessment, and why this is so. But unless and until they are in a position to make a reasonably informed 'second assessment', a monitoring body is not a real safeguard against the violation of human rights, privacy and personal integrity.

This problem is extended by the fact that all intelligence and security services and all agencies that conduct intelligence-led operations have to work as one enterprise to be successful, hence have to share and exchange information. That also means that law enforcement and intelligence communities converge. From the perspective of effectiveness, barriers to intelligence sharing and cooperation are difficult to justify and should be dismantled. But the concept of information, which lies at the heart of the notion of information exchange, is deeply affected by the sharing of information if these are coming from many more diverse sources of different reliability and accuracy. Indeed, the different pieces of information do not always confirm one another and often may add just 'noise' to real information.

While there is convergence between law enforcement and intelligence, combining domestic and foreign intelligence functions creates the possibility and danger that domestic law enforcement will be infected by the secrecy, deception and ruthlessness that international espionage requires. If the distinction between intelligence and law enforcement grows too artificial, the judiciary could cripple intelligence surveillance by demanding that it conform to the same standards as law enforcement. And if intelligence agencies succeed in providing the kind of case-oriented 'tactical' intelligence that law enforcement values most, the

distinction between intelligence and law enforcement will erode more.[198] All this must be avoided. The wall of separation between intelligence and law enforcement should largely be maintained. Hence, intelligence agencies should not be asked routinely to use their intelligence-gathering authority to help law enforcement agencies bust criminals.

International cooperation is exacerbating the problem. Existing control mechanisms not only tend to be institutional, focussing on single agencies, but are nationally limited, as each state looks exclusively at its own agencies, and none look at the international network of cooperation as a whole. The transnational nature of the pre-eminent threats in fact increases the risk for a 'state within a state' mentality: in order to obtain information which is in the hands of foreign agencies, a national agency will have to cooperate with foreign agencies in information exchange. The administrative need for good relations with powerful foreign friendly agencies carries with it a number of risks and dangers, notably that of the agency disobeying the will of the government of the day, or of the agency harming the interests of citizens or residents of the state by transferring information on them to foreign agencies. The recent problems in connection with extraordinary renditions are a clear example of how international cooperation in intelligence operations may negatively affect human rights protection.[199]

In addition, there is a blurring of the distinction between the guilty and the suspect that leads to an erosion of the principle of presumption of innocence. The judicial and police systems tend to adapt to the logics of intelligence instead of 'judicialising' the latter. This general trend has been observed by the court judges in most of the countries concerned by it. Even conservative judges have reacted on this aspect that concerns their own sphere of competence. Moreover, the questions raised in relation to fundamental rights and civil liberties are all linked to this tendency. What is at stake is thus the very foundations of democracy and its difficult relation to the state, as well as the issue of the efficiency of the government apparatus. Issues of habeas corpus, presumption of innocence, fair trial, and freedom of opinion are at the heart of the topic, and reach far beyond the crucial question of the protection of personal data.

Intelligence is fundamental to limit the possibility that clandestine organisations might be able to pursue their criminal projects. However, it cannot guarantee absolute security. There will always remain margins of uncertainty. The necessary intelligence is the one that enables to unveil a guilty person, not one that generalises suspicion. International collaboration between intelligence services must thus be encouraged between democracies, but *within well defined frames*. The importance of this collaboration should in no way justify that one of the partners may act with impunity either in the use made of information exchanged or on the territory and in the airspace of another partner. The intrusive conception of intelligence, extending the principle of suspicion to an ever-growing group of

---

198 Stewart A. Baker, "Should Spies be Cops?", *Foreign Policy*, No. 97, Winter 1994-95, pp. 37, 46, 48, at: http://www.jstor.org/stable/1149438

199 See also Canada's Arar Inquiry and other problems connected with Security Of Information Agreements, or SOIAs, existing between partner services. Alasdair Roberts, *Blacked Out - Government Secrecy in the Information Age*, Cambridge, Cambridge University Press, 2006, chapter "Opaque Networks", pp. 127-149.

individuals on the basis of information of dubious accuracy weakens the rule of law at the domestic and international levels.

Solutions for all these problems must be found. This can be done: (1) by a clear redefinition of accountability of all intelligence services and all agencies that conduct intelligence-led operations; (2) by tighter executive control and supervision; (3) by the reinforcement of checking mechanisms outside the executive and strengthening expert accountability; and (4) by improved complaints mechanisms. In addition, there is a degree of international accountability to international and supranational monitoring mechanism, such as the European Court of Human Rights.

5.3 Clear Redefinition of Accountability

There are five basic principles all organisations that engage in intelligence collection and conduct intelligence-led operations must follow: (1) to provide effective intelligence essential to the security of the nation; (2) to have an adequate legal framework; (3) to have an effective management and tasking system; (4) to be effectively accountable; and (5) to be open to internal and external review, supervision and control, and to parliamentary oversight.

Sensitive accountability structures attempt to insulate all organisations that engage in intelligence collection and intelligence-led operations from political abuse without isolating them from executive governance. On the whole, the solutions adopted by democratic states deal with this paradox in two ways: (1) by balancing rights and responsibilities between these organisations and their political masters and (2) creating checking mechanisms outside the executive branch, the most important of which is legislative oversight by parliament or special parliamentary committees.

Accountability is the obligation to demonstrate, and be responsible for, performance in the light of agreed expectations. The prerequisites for accountability are: (1) clear and agreed roles and responsibilities; (2) clear and agreed expectations of what is to be done and how, what is not to be done, and what is to be achieved; (3) performance expectations that are balanced by the relevant capacities of each party – authorities, skills and also resources; (4) timely and credible reporting of performance achieved in the light of the expectations; and (5) review and feedback on the performance reported, such that achievements are recognised and necessary corrections made. All organisations that engage in intelligence collection and intelligence-led operations must be made statutorily accountable, which is "being liable to be required to give an account or explanation of actions and, where appropriate, to suffer the consequences, take the blame or undertake to put matters right, if it should appear that errors have been made". It is greatly preferable that the primary rules be in statute form. It is essential, at any rate, that the norms concerning intelligence services are as clear and concise as possible, and that they are kept secret only to the extent that it is absolutely necessary.

Accountability must exist *ex ante* (authorisation or control), during the operations (control or monitoring of the activities) and *ex post* (review of the activities). It can concern general operations or specific acts. Accountability can have different modes. It can be backward looking, to apportion responsibility, or it can be forward looking, to encourage learning. The executive is better placed to exercise *ex ante* oversight whereas parliamentary and independent oversight bodies as well as the judiciary are generally better placed to deal with *ex post* oversight. Depending on a number of factors, in particular the constitutional structure and the history of the state and its legal and political culture, there can be overlaps or gaps in the types of accountability exercised by the different branches of government, both of which must be excluded. But making secret services accountable presents special problems. A high degree of secrecy must accompany national security policy and operations, which increases government control at the expense of the legislative power, and insulates the former from criticism.

To be truly democratic, political control must involve accountability to democratically elected representative – that is to parliament.[200] The legislature is elected to represent the people and to ensure government by the people under the constitution. It does this by balancing security and liberty, in part by providing a national forum for public consideration of issues, by passing legislation, and by scrutinizing and overseeing executive action. In all aspects of government, and the expenditure of public money, parliaments have an essential role in monitoring and scrutinizing policy and budgets. The budget represents the culmination of intelligence requirements and, at the same time, it represents the contribution required from the taxpayer – the electorate at large to whom parliamentarians are most directly responsible. Though legislative oversight is policy-related and, in theory, unlimited, the choice is not between executive or legislative sovereignty over intelligence and intelligence-led operations. The challenge is to use the best attributes of both branches in the service of the nation's security. The role that parliament can play in the development and implementation of national security policy can be grouped to four tasks: (1) oversight; (2) giving a second opinion; (3) ensuring transparency, and (4) providing a link between intelligence and society at large.

Monitoring the implementation of legislation goes to the heart of the oversight role. However, oversight is a process, not an event. It should be both proactive and reactive: proactive in anticipating issues; reactive to initiate hearings and inquiries when problems or scandals occur, and to determine whether legislation is effective and having the desired results. As a general rule, under such procedures as the president or the prime minister may establish (including those conferred by law upon the executive, legislature and judiciary to protect sources and methods), intelligence services and all agencies conducting intelligence-led operations against the pre-eminent threats should:

---

[200] Assembly of Western European Union , *Report: Parliamentary oversight of the intelligence services in the WEU countries - current situation and prospects for reform,* Paris: WEU, Document A/1801, 4 December 2002.

- Keep the oversight committees fully and currently informed of their intelligence activities, including all significant anticipated activities;

- Upon request, provide the oversight committees with any information or document in the possession, custody or control of the services or agencies; and

- Report information relating to intelligence activities that are illegal or improper, and corrective actions that are taken or planned to the oversight committees in a timely fashion.

Ideally, the committees should bring a perspective to the oversight function that is not replicated by the control and review bodies within the executive branch. Furthermore, oversight should not become so burdensome and intrusive that it has a negative effect on intelligence-led operations. Since all too often legislative oversight tends towards micromanagement of executive decisions, the parliament's oversight committees must not have the authority to direct the intelligence services and the agencies conducting intelligence-led operations to initiate certain investigations or to pursue certain cases. The question of which persons, groups, events and activities to investigate is an executive branch decision. Moreover, the committees are political bodies, subject to political expediency and to overreact. Thus, the members should hold the responsibility of avoiding overreaction in times of crisis, and the intelligence services and the agencies conducting intelligence-led operations should have the responsibility of retaining their focus on their missions and not letting the committees push them into following new objectives.

5.4 Executive Control and Supervision

However necessary it may be, secrecy needed for intelligence activities creates a scenario for potential or perceived abuse of intrusive powers by all entities engaged in intelligence activities, as well as the perception that inadequate attention may be given to obtaining value for the money spent. To gain the benefits and avoid the risks of intelligence activities, control and accountability arrangements must be balanced, and be seen to balance the need to protect and promote national interests with the need to safeguard individual rights and freedoms. At the same time, these arrangements need to ensure an appropriate focus on achieving their desired results.

Control, in the narrowest sense, means ensuring that specific procedures are followed. In the broadest sense, it means creating the conditions that lead to the achievement of agreed standards of performance, including the desired results as well as compliance with law and policy. Control may be exercised by both formal and informal means. In general, formal means are used to ensure conformity of intelligence activities with policy and procedures, proper authorisations, funding, audit and review, while informal means focus on ethics, values and leadership, etc.

International cooperation between intelligence agencies is increasingly necessary to fight the pre-eminent threats, but often involves even more secrecy, thus raising issues of accountability. Hence measures must be established by the executive that international exchanges of intelligence and intelligence cooperation cannot escape national mechanisms of control. Engaging in international networking of intelligence and security agencies is certainly the adequate response to the pre-eminent threats. However, it is necessary to create a legal framework in which cooperation with foreign agencies is only permissible according to principles established by law, including human rights safeguards, authorised according to strict routines, with proper paper trails, and controlled or supervised by independent expert bodies. The government has to consider the need for parallel transnational supervision and how that might be developed, for example, through international networking between national overseers and supranational institutions such as the Council of Europe.

The most important aspect of executive control is the need for competent political guidance of all organisations engaged in intelligence activities from the people they serve.[201] Thus, policymaker direction must be both the foundation and the catalyst for intelligence work. If all those engaged in intelligence activities do not receive direction, the chances of resources being misdirected and wasted increase. Intelligence services and those agencies conducting intelligence-led operations need to know what information to collect, and when it is needed. They need to know if their products are useful and how they may be improved to better serve policymakers and policy. Hence, policymakers need to appreciate what intelligence can offer them to a much greater extent, and become more directly involved in the ways in which intelligence capabilities are used.

Executive control and supervision play the decisive role. Guidance must come from the very top. The higher the echelon of executive control and supervision, and the greater the seriousness with which its tasks are executed, the lesser the likelihood of problems accruing to the government from judicial supervision and legislative oversight. It is the executive which is fully responsible for the proper controls and auditing of intelligence and security services, thus creating the necessary base for transparency and parliamentary oversight. The tasks of executive control and supervision are to make sure that intelligence services and all agencies that conduct intelligence-led operations: (1) function properly; (2) collect the right information; (3) satisfy the needs of decision- and policymakers; (4) are rigorous in analysis and reporting; and (5) have on hand the necessary operational capabilities and means. Of particular importance for executive control is to identify intelligence failures, and to take action to prevent these from occurring in the future.

As an arm of the government, intelligence and security services must act according to the policies of the government of the day and in pursuit of objectives relevant to these policies. However, if too close a link between policy and intelligence exists, that is when intelligence becomes policy-driven or when there is political

[201] Jack Davis, "A Policymaker's Perspective on Intelligence Analysis", *Studies in Intelligence*, Vol. 38, No. 5, 1995, pp. 7-15., at: www.cia.gov/csi/studies/95unclass/Davis.html

interference in operational activities,[202] intelligence and security services may become susceptible to being used by political actors as a tool to retain power or to undermine or discredit opponents. Thus, the misuse of intelligence and security services with their extraordinary powers by an elected government for its own political ends must be excluded. To this end, intelligence and security services should be at arms length from policymakers, should not be affiliated with any party, and they must be neutral and depoliticised.

5.5 Reinforcing the Checking Mechanisms Outside the Executive

The source of executive control should be either the president or the prime minister since they are ultimately responsible for the integrity and security of the state and for related intelligence matters. There are practical reasons why these, the ministers responsible or the National Security Council might not be able to give full attention to all of the control, supervisory and accountability tasks. Hence, governments in democracies will normally appoint individuals or establish committees or boards mandated with control and supervision of intelligence activities.[203] Individuals can be appointed as Inspector General, Controller or Efficiency Advisor, who report to the president, the prime minister or minister. Best practice is to have an independent statutory Inspector General for each of the intelligence services and all the agencies which conduct intelligence-led operations, who may also be required to make reports to the legislative oversight committees.

Committees or boards can be established, sometimes with jurisdiction extending across the entire intelligence or law enforcement community, who ideally report to the president, the prime minister or the ministers responsible, or alternatively to the National Security Council. These can be composed of members from outside the government, employed on the basis of their ability, knowledge, diversity of background and experience. However, no member should have any personal interest in, or any relationship with, any intelligence agency or agencies that conduct intelligence-led operations. These can be united in a *National Intelligence Council* and a *National Law Enforcement Council,* mandated with coordination and control. Some countries have separate committees for intelligence supervision and for policy review to scrutinise performance and policy of intelligence and security services. Independent intelligence expert or review bodies exist in Canada, The Netherlands, Norway and Belgium. These are truly outside the executive, whereas all bodies whose members are appointed by the executive cannot be viewed as truly outside or independent of the executive.

Audit is another important part of executive control. An external audit serves three purposes in terms of accountability: First, to assess compliance with the law, ensuring that those given executive authority exercise this authority in accordance with their assigned responsibilities. This involves reviewing behaviour, identifying

---

202 Robert M. Gates, "Guarding Against Politicization", *Studies in Intelligence*, Vol. 36, No. 5, 1992, pp. 5-13.
203 Mark M. Lowenthal, *Intelligence. From Secrets to Policy*, Washington D.C., CQPress, 2003, pp. 153-155.

poor administration and those who should be held accountable. The second purpose of auditing is to assess performance in public management in order to contribute to organisational learning. The third purpose is compliance auditing, which involves scrutinising accounts to see if money has been spent as allocated, and to assess the efficiency and effectiveness of financial allocations. In democracies, an external audit of accounts is normally done by the Auditor General or the National Audit Agency.

Expert bodies can replace or supplement a parliamentary body or judicial accountability. Such bodies can allow for greater expertise and time to be devoted to oversight and do not present the same risks of political division as a parliamentary body. However, they do not have the same legitimacy as a parliamentary body. Different methods exist for strengthening their legitimacy.

Their mandate can be agency-specific or field-specific (e.g. only over databanks or surveillance). However, nowadays the integrated approach to security issues means that such specific forms of oversight miss other important parts of the security spectrum. Like parliamentary bodies, the focus can be on different things. They can supervise certain aspects of the security work (legality, efficacy, efficiency, budgeting, conformity with human rights, policy), or certain activities (as regards e.g. security of databanks). Such bodies can also be given certain control functions, for example, as regards approving surveillance.

Their members should be legally trained if the mandate is review of legality, or a more varied background if the mandate is broader. Expert bodies need the trust of parliament and the public. Parliament involvement is thus necessary in establishing the expert body, in choosing its membership and in receiving its reports. An alternative to a purely expert body which combines expertise with legitimacy is to have part of the membership consist of serving or retired politicians, a 'hybrid body'. Expert bodies should be able to present special reports as well as an annual report. As regards the content of the report, different methods exist for reconciling government concerns for secrecy with the need for the expert body to provide plausible reassurance to parliament and the public. However, the government should not normally be able to control whether a report is published at all, and when it is published.

5.6 Improved Complaints Mechanisms

It is clearly necessary for individuals who claim to have been adversely affected by intelligence services, or agencies that conduct intelligence-led operations, to have avenues of redress before an independent body. This strengthens accountability and leads to improved performance through highlighting administrative failings.

The capacity of ordinary courts to serve as an adequate remedy in intelligence fields is limited. Alternative, specialist tribunal or ombudsman-like systems exist in some states. In some cases, parliamentary bodies also deal with individual complaints. The ECHR requires that control and remedies functions are performed by different bodies.

6. Key Recommendations

1. In view of generally restricted budgets, governments must give their security sector goals that can be achieved with the resources available. For this, another approach is needed – one which starts with the recognition that some of the illicit trades need to become licit. This does not mean decriminalisation of THB and exploitation of its victims. It means that the resources now wasted enforcing the prohibition of marijuana or of temporary illegal workers should be redeployed in the fight against more dangerous and harmful illicit trades. Research helps to better understand the economic incentives to illicit trade, and measure its economic and social costs as well as those of proposed alternatives. As Naím pointed out, two principles are vital to these decisions and are best applied together. The first is *value reduction*. As with any other economic activity, the more illicit trade grows the more value its participants derive from it. Driving out value from an illicit economic activity, its prevalence will diminish accordingly. The second principle is *harm reduction*. This means measuring the *social harm* that an illicit trade activity causes and comparing ways to fight it by the extent that they lower this harm.[204] Thus, deregulation, decriminalisation and legalisation have to be *policy options*, subject to the test that they reduce the value to illicit traders *and* the harm to society.

2. More effective ways to counter terrorists, proliferants, TOC and THB have to be found; the starting point of which begins with the recognition that *intelligence is the prerequisite for more effective measures of all agencies* that aim at the disruption, suppression, pre-emption, mitigation and prevention of the pre-eminent threats.

3. The *raison d'être* of intelligence is knowledge of intentions, capabilities, methods and means. And its essence is information plus insights derived from subject matter knowledge. Hence, intelligence provides a sound basis from which inferences can be drawn to guide strategic decisions on better use of resources, as well as for operational or tactical activities and investigations.

4. Countering the pre-eminent threats from multiplying non-state actors requires not only security and intelligence services. These threats can be effectively counteracted, disrupted, pre-empted and finally deterred and prevented only when the operations of all the security sector organisations mandated to deal with them are intelligence-led.

5. Intelligence-led operations are needed for improvement and expansion of the fight against the pre-eminent threats in a more effective and tailored way. All law enforcement agencies have to shift their modus operandi to intelligence-led policing. Switching to intelligence-led operations is equally

[204] Moisés Naím, *Illicit – How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*, New York, Doubleday, 2005, pp. 251-252.

necessary for border management and all other agencies fighting the pre-eminent threats.

6. This requires a radical new approach of more close collaboration, interaction and information exchange of all these organisations with the agencies of the intelligence community. And it calls for the establishment of an intelligence function that produces operational and tactical intelligence in all organisations where it is absent.

7. Foremost, these intelligence cells should do an analysis of what is seen, heard and reported by the personnel of their own organisation, from open sources and from intelligence reports exchanged, so that they can accomplish their missions in smarter ways, with more agility, more effectively and efficiently, particularly by all those agencies that suffer from a lack of resources.

8. The increasing sophistication of TOC makes it imperative to disrupt and demolish network structures instead of merely arresting individual criminals. But attempts to break up criminal networks will never be effective until all available information is developed and transformed into intelligence for use by all government agencies involved in countering the pre-eminent threats.

9. The more holistic the intelligence collection approach, and the more accurate and timely the intelligence analysis and assessments on terrorism, proliferation of WMD, TOC and THB activities and actors, the more this will allow for limited resources to be effectively applied to achieve the national security goals of countering the pre-eminent threats.

10. Intelligence-led policing is synonymous with greater integration of criminal intelligence and crime analysis. Criminal intelligence provides information on prolific TOC offenders, while crime analysis provides the environmental crime context in which they offend. Both are essential for a full understanding of the crime problems and prerequisites for effective crime reduction.[205]

11. Intelligence collection, analysis and investigations must reflect the geographic, structural and commercial components that make up the crime of THB, thus must cover the countries of origin, transit and destination as well as all the commercial THB activities of advertising, renting and use of premises, transportation, communications and financial transactions, etc.[206]

---

[205] Jerry H. Ratcliffe, "Intelligence-led Policing", in: Wortley R., Mazerolle L., Rombouts S., eds., *Environmental Criminology and Crime Analysis*, Cullompton, Devon, Willan Publishing, 2008. *Intelligence-Led Policing: The Integration of Community Policing and Law Enforcement Intelligence*, Austin, Texas Police Department, no date; *Intelligence Led Policing: Getting Started*, *Professionalizing Analysis Worldwide*, International Association of Law Enforcement Analysts, IALEIA, Richmond, 3rd edition, January 2005; *Practice Advice Introduction to Intelligence-Led Policing*, National Centre for Policing Excellence, Wyboston, Bedfordshire, 2007.

[206] *Law Enforcement Manual for Fighting Against Trafficking in Human Beings – Best Practice*, UNDP Romania, Vienna 2003, Section 2, pp. 2-1 to 2-10. *OSCE Action Plan to Combat Trafficking in Human Beings*, Decision No. 557/Rev.1, PCED557/Rev.1, 7 July 2005, at: www.osce.org/documents/pc/2005/07/15594_en.pdf United Nations Office on Drug and Crime, *Toolkit to Combat Trafficking in Persons, Global Programme Against*

12. Strategic and operational or tactical intelligence is needed to effectively fight THB. Strategic intelligence serves for an overall assessment of the various strategic factors that underpin the existence of THB, while operational or tactical intelligence must enable specific intelligence-led operations that lead to arrests, further investigations, prosecution and seizure of profits.[207]

13. Main contributors to combating the pre-eminent threats are the external and internal intelligence services doing much of strategic intelligence collection, whereas the criminal intelligence service, often the lead investigation agency against TOC, and law enforcement, financial investigative units and border management do investigations, and joint operations within the EU framework.

14. As to investigations by law enforcement agencies, experience and best practice show that THB is particularly vulnerable to proactive, intelligence-led operations. The commercial imperative to market the product creates the 'Achilles Heel' that THB cannot escape and law enforcement can fully exploit. If the victims can be located so can the THB actors.[208]

15. The objective of the proactive, intelligence-led option is to use the most effective and lawful investigative techniques in order to secure sufficient, sustainable evidence for arrests and prosecutions. The collection strategy to follow is to capitalise on the technological innovation that yields high-tech tools with unprecedented potential to help fight illicit trade and THB.[209]

16. Best practice for investigations is to bring the investigator and prosecutor closer together in the investigative process in consultation, planning and risk assessment meetings, so as to avoid the investigator pursuing evidence gathering tactics that may be inadmissible or of no use to the prosecutor in the trial, and to acquaint the prosecutor with operational difficulties.[210]

17. Such meetings of investigators and prosecutors serve to decide on the operational subject and intelligence profile, the operational objective, and on strategies and tactics to be used to deliver the objective. They also serve to

---

Trafficking in Human Beings, New York, United Nations, 2006, pp. 81-84. *Human Trafficking: Reference Guide for Canadian Law Enforcement*, University College of the Fraser Valley Press, Abbotsford, BC, May 2005, pp. 31-34.

207 *Human Trafficking: Reference Guide for Canadian Law Enforcement*, University College of the Fraser Valley Press, Abbotsford, BC, May 2005, pp. 32-34. Rachel Boba, *Crime Analysis and Crime Mapping*, Thousand Oaks, Sage, 2005, Part III, Tactical Crime Analysis, pp. 111-164, Part IV, Strategic Crime Analysis, pp. 165-240.

208 *Law Enforcement Manual for Fighting Against Trafficking in Human Beings – Best Practice*, UNDP Romania, Vienna 2003, Section 4, pp. 4-1 to 4-9, Section 6, pp. 6-1 to 6-3. *Human Trafficking: Reference Guide for Canadian Law Enforcement*, University College of the Fraser Valley Press, Abbotsford, BC, May 2005, Appendix 1, pp. 63-68. United Nations Office on Drug and Crime, *Toolkit to Combat Trafficking in Persons, Global Programme Against Trafficking in Human Beings*, New York, United Nations, 2006, pp. 70-71.

209 *Law Enforcement Manual for Fighting Against Trafficking in Human Beings – Best Practice*, UNDP Romania, Vienna 2003, Section 2, pp. 2-1 to 2-10, Section 6, pp. 6-1 to 6-3.

210 Idem., Section 6, pp. 6-1 to 6-6. United Nations Office on Drug and Crime, *Toolkit to Combat Trafficking in Persons, Global Programme Against Trafficking in Human Beings*, New York, United Nations, 2006, pp. 77-81.

make rigorous risk assessment in respect of victims and the operation, to establish a risk management plan, and for proper decision logging.[211]

18. Intelligence sharing and exchange have to be clearly regulated both nationally and internationally. Recording, retention, classification, evaluation and dissemination of all intelligence material must be in strict accordance with the relevant laws on data protection and confidentiality. In addition, a system for 'flagging' or labelling the intelligence into categories should be established.[212]

19. Though there is convergence between law enforcement and intelligence since they have to collaborate ever more closely, some walls of separation should be maintained in order to prevent the infection of domestic law enforcement by foreign intelligence methods. Moreover, foreign intelligence should not be routinely asked to help law enforcement bust criminals.

20. Increased intelligence collection capacities enhance the problems accruing to democratic control, supervision, oversight and accountability. In order to minimise the damage that intelligence can cause to civil rights and liberties, accountability must be redefined, executive control and outside checking mechanisms must be reinforced, and the complaints mechanisms must be improved.

[211] *Law Enforcement Manual for Fighting Against Trafficking in Human Beings – Best Practice*, UNDP Romania, Vienna 2003, Section 6, pp. 6-4 to 6-6.
[212] Idem., Section 4, pp. 4-9 to 4-17.

7. Select Bibliography

United Nations

UN Treaty Collection, Overview, at: http://untreaty.un.org/English/overview.asp

UN Security Council Resolution 1373 (2001), adopted 28 September 2001.

UN Security Council Resolution 1540 (2004), adopted 28 April 2004.

UN, A more secure world: Our shared responsibility. Report of the Secretary-General's High-level Panel on Threats, Challenges and Change. 2004.

UN, Report of the Secretary-General on the Status of the Implementation of the Special Commission's Plan for the Ongoing Monitoring and Verification of Iraq's Compliance with Relevant Parts of Section of Security Council Resolution 687 (1991), 11 October 1995, at: www.un.org/Depts/unscom/sres95-864.htm

UN, Report of the United Nations Scientific Committee on the effects of atomic radiation to the General Assembly, generally referred to as UNSCEAR 2000 Report.

World Health Organization: Department of Communicable Disease, Surveillance and Response. Global Outbreak Alert and Response. *Report of a WHO Meeting, Geneva, 26-28 April 2000. WHO/CDS/CSR/2000.3.*, at:
http://www.who.int/csr/resources/publications/surveillance/whocdscsr2003.pdf

Department of Communicable Disease, Surveillance and Response, Strengthening national preparedness and response to biological weapons. *Report of a WHO consultation with the participation of the Food and Agricultural Organization of the UN and the Office International des Epizooties*. Rome, Italy, 6-8 March 2002. WHO/CDS/CSR/EPH/ 2002/ 18, at: http://www.who.int/csr/delibepidemics/preparednessromemeeting/en

Fifty-fifth World Health Assembly. *Report by the Secretariat. Deliberate use of biological and chemical agents to cause harm. Public Health response*. A55/20, 16 April 2002, at: http://www.who.int/gb/ebwha/pdf_files/WHO55/ea5520.pdf

Public Health response to biological and chemical weapons: WHO guidance, 2004, at: http://www.who.int/csr/delibepidemics/biochemguide/en/print.html

Implementation of resolution WHA55.16 on global public health response to natural occurrence, accidental release or deliberate use of biological and chemical agents or radio-nuclear material that affect health. *Report by the Secretariat to the Executive Board*, EB116/9, 4 May 2005, at: http://www.who.int/gb/ebwha/pdf_files/EB116/B116_9-en.pdf

Laboratory Biosafety Manual, 3rd edition, 2004, at: www.who.int/csr/resources/publications/biosafety/WHO_CDS_CSR_LYO_2004_II/en/index.html

Statement of the Director General IAEA, *Security Today: Challenges and Opportunities*, Basel, Nobel Laureate Lecture, Biozentrum, University of Basel, February 14, 2007, at: www.iaea.org/NewsCenter/Statements/2007/ebsp2007n003.html

Organization for the Prohibition of Chemical Weapons, Inspection Activity, URL, at: www.opcw.org

European Union

A Secure Europe in a Better World, Brussels, 12 November 2003, at:
http://ue.eu.int/uedocs/cmsUpload/78367.pdf

Declaration on Combating Terrorism, Brussels, 25 March 2004, at:
http://ue.eu.int/uedocs/csmUpload/79635.pdf

European Union, *Factsheet: the EU and the Fight Against Terrorism*, at:
http://ue.eu.int/uedocs/cmsUpload/europa.pdf

European Union, *Factsheet, EU Strategy against the Proliferation of Weapons of Mass Destruction,* European Commission and Secretariat General of the Council of the EU, EU-US Summit, Dromoland Castle, Ireland, 26 June 2004.

EU-US Declaration on Combating Terrorism, Dromoland Castle, 26 June 2004, at:
http://ue.eu.int/uedocs/cmsUpload/10760EU_US26.06.04.pdf

European Council Declaration on Combating Terrorism, May 2004.

Council and Commission Action Plan on implementing the Hague Programme on strengthening freedom, security and justice in the European Union, at:
http://ue.eu.int/uedocs/cmsUpload/web097781.en.pdf

Commission of the European Communities. Commission Staff Working Paper. *Report of the R&D Expert Group on countering the effects of biological and chemical terrorism*. Brussels, 3 June 2002. SEC (2002)698.

Commission of the European Communities. Communication from the Commission to the Council and the European Parliament on Cooperation in the European Union on Preparedness and Response to Biological and Chemical Agent Attacks. Brussels, 2.6.2003, COM(2003)320 final, at:
http://europa.eu/eurlex/en/com/cnc/2003/com2003_0320en01.pdf

Schengen Catalogue of Best Practices on External Borders Control, Removal and Re-admission: *Recommendations and Best Practices of February 2002*, at:
http://ue.eu.int/uedocs/cmsUpload/catalogue20.pdf

Council of the European Union from Presidency. *Integrated Border Management, Strategy deliberations*, Brussels, 21 November 2006, 13926/3/06 REV 3.

Commission of the European Communities. Communications from the Commission to the Council. Reinforcing the management of the European Union's Southern Maritime Borders. Brussels, 30.11.2006, COM(2006)733 final.

NATO

The NATO Nuclear, Biological and Chemical Defence Initiatives, 2002, at:
http://www.nato.int/docu/comm/2002/0211-prague/exhibition/nnbcdi.pdf

Departments of the Army, Navy, and Air Force. *NATO Handbook on the Medical Aspects of NBC Defensive Operations*, Washington D.C., Defense Department, 1996, PAP-DIB at:
http://www.nato.int/ducu/basictxt/b040607e.htm

Joseph F. Pilat & David S. Yost, eds., *NATO and the Future of the Nuclear Non-Proliferation Treaty,* Rome, NATO Defense College, Academic Research Branch, May 2007, at:
http://www.ndc.nato.int

G8

G8 Action Plan on Nonproliferation, 2004, at:
http://www.fco.gov.uk/Files/kfile/PostG8_Gleneagles_CounterProliferation.pdf

Gleneagles Statement on Non-Proliferation, 2005, at:
http://www.fco.gov.uk/Files/kfile/PostG8_Gleneagles_CounterProliferation.pdf

OECD

OECD DAC Handbook on Security System Reform, Supporting Security and Justice, Paris, OECD, 2007, p. 252.

Security System Reform and Governance, Policy and Practice, DAC Guidelines and Reference Series, Paris, OECD, 2004.

OSCE

http://www.osce.org/publications/spmu/2007/01/23086_795_en.pdf

Victor-Yves Ghebali & Alexandre Lambert: *The OSCE Code of Conduct on Politico-Military Aspects of Security. Anatomy and Implementation,* Leiden and Boston, Martinus Nijhoff Publishers, 2005, p. 428.

ICRC

Appeal on Biotechnology, Weapons and Humanity. ICRC's appeal to the political and military authorities and to the scientific and medical communities, industry and civil society on the potentially dangerous developments in biotechnology. Geneva, 25 September 2002, at: http://www.icrc.org/Web/eng/siteengo.nsf/html/5EAMTT?OpenDocument

Christopher B. Harland & Angela Woodward, 2002: *A Model Law*: *The Biological and Toxin Weapons Crimes Act*. An act to implement obligations under the 1972 Bio-logical and Toxin Weapons Convention and the 1925 Geneva Protocol, Geneva, 30 September 2005, at:
http://www.icrc.org/Web/eng/siteengo.nsf/htmlall/review-859-p573/$File/irrc_859_Harland_Woodward.pdf

Christoph Wirz & Emmanuel Egger, "Use of nuclear and radiological weapons by terrorists?", *International Review of the Red Cross*, Vol. 87, No. 859, September 2005, p. 499.

Germany

Deutscher Bundestag, 2003. *Entwicklung eines Gesamtkonzepts zur Abwehr bio-terroristischer Gefahren*. Antwort der Bundesregierung, 16. Oktober 2003, Druck-sache 15/1748.

Deutscher Bundestag, 2005. Organisation des Katastrophenschutzes im Gross-schadensfall mit biologischen oder chemischen Schadstoffen. Antwort der Bundesregierung, 6. Mai 2005, Drucksache 15/5433.

Deutscher Bundestag, 2005. Ausrüstung und Vorbereitung für einen Grossschadens-fall mit biologischen und chemischen Schadstoffen. Antwort der Bundesregierung, 20. Juni 2005, Drucksache 15/5794.

New Zealand

Tumuaki o te Mana Arotake, *Managing Threats to Domestic Security*, Report of the Controller and Auditor-General, Wellington, The Audit Office, October 2003, at: www.oag.govt.nz

Russia

Government Resolution No. 303. On the Division of Authority among Federal Agencies in the Sphere of Biological and Chemical Security of the Russian Federation, 16 May 2005, at: http://www.government.ru/data/news_text.html?he_id=103&news_id=17471

Biological Science and Biotechnology in Russia. *Controlling Diseases and Enhancing Security - Development, Security and Cooperation*, 2005, at: http://books.nap.edu/books/0309097045/html

Russia: Nonproliferation of Weapons of Mass Destruction, CEP20060702347001, Official website of the government of the Russian Federation, at: www.government.ru, in Russian, 21 June 2006.

White Book: The Russian Federation and the Situation in the Area of Non-proliferation of Weapons of Mass Destruction and Means of Delivery Thereof: Threats, Assessments, Tasks and Ways of Carrying Them Out.

United Kingdom

Foreign Affairs Committee, 2002, The Biological Weapons Green Paper, at: http://www.publications.parliament.uk/pa/cm200203/cmselect/cmfaff/150/150.pdf

Emergency Planning College, 2005, *Emergency Response and Recovery*, at: http://www.ukresilience.info/ccact/emergresponse.pdf

United States

U.S. Congress, House, Committee on Armed Services, *Army Transformation*, Hearing, 108th Congress, 2nd session, July 15, 2004, Washington D.C., GPO, 2005, 200 p.

U.S. Congress, *Technologies Underlying Weapons of Mass Destruction*, OTA-BP-ICS-119, Washington D.C., US Government Printing Office, December 1993.

Government Accountability Office, Nuclear Non-proliferation: DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium in Civilian Research Reactors, GAO-04-807, Washington D.C., GAO, 2004.

Government Accountability Office, U.S. and International Assistance Efforts to Control Sealed Radioactive Sources Need Strengthening, GAO-03-638, August 2003.

The National Security Strategy of the United States of America, Washington D.C., March 2006, at: www.whitehouse.gov/nss/2006

The National Security Strategy of the United States of America, Washington D.C., September 2002, at: www.whitehouse.gov/nsc/nss.html

Homeland Security: Information Sharing Activities Face Continued Management Challenges; GAO-02-1122T, Report No. A05205, Washington D.C., 1 October 2002.

The White House, "Biodefense for the 21st Century", 28 April 2004, at: http://www.whitehouse.gov/homeland/20040430.html

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President*, Washington D.C., WMD Commission, 31 March 2005, at: www.wmd.gov/report

National Strategy to Combat Weapons of Mass Destruction, Washington D.C., December 2002, at: http://www.state.gov/documents/organization/16092.pdf

Ballistic Missiles. Delivery Systems for Weapons of Mass Destruction, Washington D.C., U.S. Government Publication, 2nd Edition, August 2006, p. 111.

Cruise Missiles. Potential Delivery Systems for Weapons of Mass Destruction, Washington D.C., U.S. Government Publication, April 2000, p. 53.

For a primer on ballistic missile defenses, see: the Missile Defense Agency missile defense system booklet at: www.acq.osd.mil/bmdo/bmdolink/pdf/bmdsbook.pdf

National Strategy for Combating Terrorism, Washington D.C., February 2003.

National Strategy for Combating Terrorism, Washington D.C., September 2006.

National Military Strategy to Combat Weapons of Mass Destruction, Washington D.C., Chairman of the Joint Chiefs of Staff, 13 February 2006.

Public Health Emergency Response Guide for State, Local, and Tribal Public Health Directors, Department of Health and Human Services, Center for Disease Control, at: http://www.bt.cdc.gov/planning/pdf/cdcresponseguide.pdf

The National Intelligence Strategy of the United States of America, Transformation through Integration and Innovation, Office of the Director of National Intelligence, Washington D.C., October 2005, at: www.odni.gov

Joint Vision 2020, Washington D.C., Joint Staff, June 2000.

The National Counterintelligence Strategy of the United States of America, the National Counterintelligence Policy Board, Chaired by the National Counter-intelligence Executive, Washington D.C., 2007.

Military Transformation, A Strategic Approach, Washington D.C., U.S. Department of Defense, 2003.

Defense Transformation for the 21st Century: Act of 2003, at: http://www.govexec.com/pdfs/transformation.pdf

WMD

Weapons of Terror. Freeing the World of Nuclear, Biological and Chemical Arms, WMDC, the Weapons of Mass Destruction Commission, Final Report, Stockholm, EO Grafiska, 2006, at: www.wmdcommission.org

SIPRI Yearbook 2006, Armaments, Disarmament and International Security, Stockholm International Peace Research Institute, New York, Oxford University Press Inc., 2006.

SIPRI Yearbook 2007, Armaments, Disarmament and International Security, Stockholm International Peace Research Institute, New York, Oxford University Press Inc., 2007.

"Weapons of Mass Destruction Verification and Compliance: The State of Play, Challenges, and Responses", *International Security Bureau, Department of Foreign Affairs*, Ottawa, Canada, January 2005.

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, Washington D.C., The National Academies Press, Committee on Science and Technology for Countering Terrorism, National Research Council, National Academies Press, 2002, p. 440, at: http://www.nap.edu/catalog/10415.html

Andreas Persbo & Angela Woodward, National Measures to Implement WMD; *Treaties and Norms: The Need for International Standards and Technical Assistance*, WMDC, Stockholm, The Weapons of Mass Destruction Commission, Verification Research, Training and Information Centre (VERTIC), May 2005.

D. Smith, *Establishing a Global Quarantine against Weapons of Mass Destruction*, at: http://history.sandiego.edu/gen/text/us/fdr1937.html

Nuclear Weapons and Warfare

David Albright & Kimberly Kramer, "Civil HEU Watch: Tracking Inventories of Civil Highly Enriched Uranium", *Global Stocks of Nuclear Explosive Materials*, Washing-ton D.C., Institute for Science and International Security, 2005, at: www.isis-online.org/global_stocks/end2003/tableofcontents.html

David Albright, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents", *Special Forum 47*, Berkeley, Nautilus Institute, 6 November 2002.

David Albright, Kathryn Buehler & Holly Higgins, "Bin Laden and the Bomb", *Bulletin of Atomic Scientists*, Vol. 58, No. 1, January/February 2002.

Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed., New York, Times Books/Henry Holt, 2004.

Graham Allison, "How to Stop Nuclear Terror", *Foreign Affairs*, January/February 2004.

Gunnar Arbman & Charles Thornton, *Russia's Tactical Nuclear Weapons, Part II: Technical Issues and Policy Recommendations*, Stockholm, Swedish Defence Re-search Agency, Report ISSN 1650-1942, February 2005.

Matthew Bunn & Anthony Wier, *Securing the Bomb 2006*, Cambridge, Project on Managing the Atom, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, Commissioned by the Nuclear Threat Initiative, July 2006.

John P. Holden & Matthew Bunn, "Technical Background: A Tutorial on Nuclear Weapons and Nuclear-Explosive Materials", *Nuclear Threat Initiative Research Library: Securing the Bomb*, Cambridge, and Washington D.C., Project on Managing the Atom, Harvard University and Nuclear Threat Initiative, 2002, at:
www.nti.org/e_research/cnwm/overview/technical.asp

Anna M. Pluta & Peter D. Zimmerman, "Nuclear Terrorism: A Disheartening Dissent", *Survival* 48, No. 2, Summer 2006.

NTI, Research Library, *Securing Nuclear Warheads and Materials. Global Nuclear Security Standards*, at: www.nti.org/e_research/cnwm/securing/standards.asp.

Anthony Wier, "Interactive Budget Database", in *Nuclear Threat Initiative Re-search Library: Securing the Bomb*, Cambridge and Washington D.C., Project on Managing the

Atom, Harvard University, and Nuclear Threat Initiative, 2006, at:
http://www.nti.org/e_research/cnwm/overview/funding.asp.

Chemical and Biological Weapons and Warfare

Frederick R. Sidell, Ernest T. Takafuji & David R. Franz, eds., *Medical Aspects of Chemical and Biological Warfare*, at:
www.nbcmed.org/SiteContent/HomePage/WhatsNew/MedAspects/contents.html

Frederick R. Sidell, Ernest J. Takafuji & David R. Franz, eds., *Textbook of Military Medicine: Medical Aspects of Chemical and Biological Warfare, Part I: Warfare, Weaponry, and the Casualty*, Washington D.C., Surgeon General, U.S. Department of the Army, 1997.

Margaret E. Kosal, "The Basics of Biological and Chemical Weapons Detectors", *Center for Non-proliferation Studies*, Research Story of the Week, 23 November 2003, at: http://cns.miis.edu/pubs/week/031124.htm

Chemical Weapons and Warfare

P. A. D'Agostino & C. L. Chenier, Analysis of Chemical Warfare Agents: General Overview, LC-MS Review, IN-House LC-ESI-MS Methods and Open Literature Bibliography, Defense Research and Development Canada, Technical Report DRDC Suffield TR 2006-022, March 2006.

Sergey Batsanov, "Viewpoint. Approaching the 10th Anniversary of the Chemical Weapons Convention, A Plan for Future Progress", Non-proliferation Review, Routledge, The Monterey Institute of International Studies, Vol. 13, No. 2, July 2006, p. 341.

Biological Weapons and Warfare

Michael J. Ainscough, "Next Generation Bioweapons: Genetic Engineering and Bio-logical Warfare", in: Jim A. Davis & Barry R. Schneider, eds., *The Gathering Bio-logical Warfare Storm*, Westport, Connecticut, Praeger, 2004.

Ken Alibek & Stephen Handelman, Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World -Told from Inside by the Man Who Ran it, New York, Delta, 1999.

Brian Bernett, *U.S. Biodefense and Homeland Security: Toward Detection and Attribution*, Thesis, Monterey, Naval Postgraduate School, December 2006.

Sergio Bonin, *International Biodefense Handbook 2007*, Zürich, Center for Security Studies, ETH Zürich, 2007, p. 434, at: www.crn.ethz.ch

Sheldon H. Harris, Factories of Death: Japanese Biological Warfare 1932-45 and the American Cover-up, New York, Routledge, 1994.

Milton Leitenberg, *The Problem with Biological Weapons*, Stockholm, The Swedish National Defence College, 2004, 68 p.

Coleen K. Martinez, *Biodefense Research Supporting the DoD: A new Strategic Vision*, Carlisle, Strategic Studies Institute, U.S. Army War College, March 2007, at: http://www.StrategicStudiesInstitute.army.mil/

Olive Meier, "Aerial Surveillance and BWC Compliance Monitoring", *Research Group for Biological Arms Control*, Occasional Paper 2, November 2006, at:
http://www.biological-armscontrol.org/download/aerial%20surveillance_web.pdf

Judith Miller, Stephen Engelberg & William Broad, *Germs, Biological Weapons and America's Secret War*, New York, Simon & Schuster, 2001, p. 382.

"Biological Weapons: Research, Development and Use from the Middle Ages to 1845", in *SIPRI Chemical and Biological Warfare Studies*, No. 18, Erhard Geissler & John Ellis van Courtland Moon, eds., Oxford, Oxford University Press, 1999.

National Institute of Allergy and Infectious Diseases, *NIAID Biodefense Research Agenda for Category B and C Priority Pathogens*, NIH Publication No. 03-5315, January 2003.

L.D. Rotz et al., "Public health assessment of potential biological terrorism agents", *Emerging Infectious Diseases*, Vol. 8, No. 2, 2002, pp. 225-230.

John Steinbruner, Elisa D. Harris, Nancy Gallagher & Stay Okutani, *Controlling Dangerous Pathogens: A Prototype Protective Oversight System*, Center for Inter-national and Security Studies, University of Maryland, December 2005.

Elizabeth L. Stone Bahr, *Biological Weapons Attribution: A Primer*, Thesis, Monterey, Naval Postgraduate School, June 2007.

G.F. Webb, "A Silent Bomb: The Risk of Anthrax as a Weapon of Mass Destruction", *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 100, No. 8, 15 April 2003.

Health Aspects of Chemical and Biological Weapons, Geneva, World Health Organization, 1970.

Radiological Weapons

Cleanup After a Radiological Attack: U.S. Prepares Guidance, Center for Non-proliferation Studies, at: http://cns.miis.edu/pubs/npr/vol11/113toc.htm

Commercial Radioactive Sources, Center for Non-proliferation Studies, at:
http://cns.miis.edu/pubs/opapers/op11/

Fact Sheet on Dirty Bombs, U.S. Nuclear Regulatory Commission, at:
www.au.af.mil/au/awc/awcgate/nrc/dirty-bombs.htm

Radiological Weapons as Means of Attack, Center for Strategic and International Studies at:
http://www.csis.org/burke/hd/reports/radiological.pdf

Robert Johnston, *Dirty Bombs and Other Radiological Weapons*, at:
www.johnstonsarchive.net/nuclear/dirtybomb.html

Fred Burton, "Dirty Bombs: Weapons of Mass Disruption", *Stratfor*, Predictive, Insightful, Global Intelligence, 4 October 2006, at:
www.stratfor.com/products/premium/print.php?storyId=277090

"British Terrorist Dhiren Barot's Research on Radiological Weapons", *Global Terrorism Analysis*, The Jamestown Foundation, at:
http://jamestown.org/terrorism/news/article.php?articleid=2370201

"Radiological Dispersion Weapons: Health, Social, and Environmental Effects", a Briefing Paper from International Physicians for the Prevention of Nuclear War, *Global Health Watch Report*, 1996.

Export Controls

Michael Beck, Cassidy Craft, Seema Gahlaut & Scott Jones, *Strengthening Multilateral Export Controls, A Non-proliferation Priority*, Athens, The University of Georgia, CITS, Center for International Trade and Security, September 2002, at: www.uga.edu/cits

Terrorism

Caleb Carr, *The Lessons of Terror*, New York, Random House, 2002.

Ken Booth & Tim Dunne, eds., Worlds in Collision: Terror and the Future of Global Order, New York, Palgrave, 2002.

Charles D. Ferguson & William C. Potter, *The Four Faces of Nuclear Terrorism*, 2005.

Lawrence Friedman, ed., *Superterrorism: Policy Responses*, Oxford, Blackwell, 2002.

Harry Henderson, *Global Terrorism - The Complete Reference Guide*, New York, Checkmark Books, 2001.

Brian Jenkins, *Terrorism: Current and Long-Term Threats*, Santa Monica, Rand, 2001.

Brian Jenkins, *Protecting Public Surface Transportation against Terrorism and Serious Crime: An Executive Overview*, Report No. MTI-01-14, Norman Y. Mineta Institute for Surface Transportation Policy Studies, San Jose, San Jose State University, 2001.

Walter Laqueur, "Post-modern Terrorism", *Foreign Affairs*, September/October 1996.

Walter Laqueur, The New Terrorism. Fanaticism and the Arms of Mass Destruction, London, Phoenix Press, 2001.

Organised Crime

Klaus von Lampe, *The Use of Models in the Study of Organized Crime*, Paper presented at the 2003 Conference of the European Consortium for Political Research (ECPR), Marburg, 19 September 2003, p. 11.

Thomas Land, "Islamic terrorists and the Russian Mafia, Nuclear weapons-free zone in Central Asia", *Contemporary Review*, January 2003.

Louise I. Shelley, "Trafficking in Nuclear Materials: Criminals and Terrorists", in *Global Crime*, Routledge, Volume 7, No. 3-4, August-November 2006, pp. 544-56.

Phil Williams & Roy Godson, "Anticipating organized and transnational crime", *Crime, Law and Social Change*, Vol. 37, No. 4, June 2002, pp. 311-355.

Lyudmila Zaitseva, "Organized Crime, Terrorism and Nuclear Trafficking", Conference: *Terrorism, Transnational Networks and WMD Proliferation: Indications and Warning in an Era of Globalization*, Monterey, Defense Threat Reduction Agency's Advanced System Concepts Office, Naval Postgraduate School, 25-27 July 2006.

Police

David H. Bayley, *Democratizing the Police Abroad: What to Do and How to Do It*, Washington, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, NCJ 188742, June 2001.

David Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies,* Office of Community Oriented Policing Services, COPS, Michigan State University, November 2004.

Frank Gregory, The UK's Domestic Response to Global Terrorism: Strategy, Structure and Implementation with Special Reference to the Role of Police, Madrid, Real Instituto Elcano, Documento de Trabajo, 18 June 2007, at: www.realinstitutoelcano.org

Anita Hazenburg, "Target Areas of Police Reform", in: Kadar, Andras, ed., *Police in Transition*, Budapest, Central European University Press, 2001, pp. 177-186.

Gary T. Marx, *Police and Democracy*, in: M. Amir & S. Einstein, eds., *Policing, Security and Democracy: Theory and Practice*, at: http://www.mit.edu/gtmarx/www/dempol.html

Jerry H. Ratcliffe, *Intelligence-led Policing*, Trends and Issues in Crime and Criminal Intelligence, Australian Institute of Criminology, No. 248, April 2003 at: www.aic.gov.au

Jerry H. Ratcliffe, Integrated Intelligence and Crime Analysis, Enhanced Information Management for Law Enforcement Leaders, Police Foundation, COPS, U.S. Department of Justice, Washington D.C., August 2007.

Overview of the Law Enforcement Strategy to Combat International Organized Crime. U.S. Department of Justice, Washington D.C., April 2008.

Rachel Boba, *Crime Analysis and Crime Mapping*, Thousand Oaks, Sage Publications, 2005.

Colleen McCue, Data Mining and Predictive Analysis, Intelligence Gathering and Crime Analysis, Elsevier Inc., Burlington, 2007.

Steven David Brown, ed., *Combating International Crime, The Longer Arm of the Law*, Routledge-Cavendish, June 2008.

Border guards

European Agency for the Management of Operational Cooperation at the External Borders of the Member States, Brussels, at:
http://europa.eu.int/scadplus/leg/en/lvb/133216.htm

Ian Anthony, Aline Dewaele, Rory Keane & Anna Wetter, *Strengthening WMD-related border security management assistance*, Stockholm, SIPRI, Stockholm International Peace Research Institute, Background paper No. 7, September 2005.

United Nations Office on Drugs and Crime, Afghanistan, Iran and Pakistan - Border Management Cooperation in Drug Control, Outline Action Plan, April 2008.

Transforming global border management, Facilitating trade, travel and security to achieve high performance, Accenture, Consulting, Technology, Outsourcing, 2005, at: www.accenture.com

Franco Frattini, *Providing Europe with the tools to bring its border management into the 21st century,* Ministerial Conference on the Challenges of the EU External Border Management, 31 March 2008, at: www.libertysecurity.org/article1939.html

Peter Hobbing, *Integrated Border Management at the EU Level*, Centre for European Policy Studies, CEPS Working Document No. 227, August 2005, at: http://www.ceps.be

William J. Krouse & Raphael F. Perl, *Terrorism: Automated Lookout Systems and Border Security: Options and Issues*. Washington D.C., Congressional Research Service, The Library of Congress, Report RL31019.

FRONTEX Annual Report 2006, p. 29.

FRONTEX, BORTEC, Study on technical feasibility of establishing a surveillance system, (European Surveillance System), Warsaw, December 2006.

Armed Forces

John Arquilla & David Ronfeldt, *Swarming and the Future of Conflict*, Santa Monica, RAND, AB-372-OSD, 2000.

John Arquilla & David Ronfeldt, eds., *Networks and Netwars*, Santa Monica, RAND Corporation, 2001.

James J. Carafano, *A Congressional Guide to Defense Transformation: Issues and Answers*, Washington D.C., Heritage Foundation, 2005, Heritage Foundation Back-grounder No. 1847.

David E. Chesser, Transformational Leadership: An Imperative for Army Reserve Readiness in the 21st Century, Carlisle Barracks, PA, Army War College, March 2006.

Alan M. Dershowitz, *Pre-emption. A Knife that Cuts both Ways*, New York, W.W. Norton & Company, Inc., 2006, 348 p.

Sean J.A. Edwards, *Swarming on the Battlefield: Past, Present, and Future*, Santa Monica, RAND, MR-1100-OSD, 2000.

Colin S. Gray, *The Implications of Pre-emptive and Preventive War Doctrines: A Re-consideration*, Carlisle Barracks, US Army War College, July 2007, at: http://www.StrategicStudiesInstitute.army.mil/

Rupert Smith, *The Utility of Force: The Art of War in the Modern World*, New York, Alfred A. Knopf, 2007, p. 448.

Transforming Defense. National Security in the 21st Century. *A Transformation Strategy*, Report of the National Defense Panel, December 1997, at: http://www.fas.org/man/docs/ndp/part05.htm

Security Sector Reform

A Beginner's Guide to Security Sector Reform (SSR), Birmingham, GFN-SSR, global facilitation network for security sector reform, DFID Department for International Development, March 2007, at: www.ssrnetwork.net

Alan Bryden & Heiner Hänggi, eds., *Security Governance in Post-Conflict Peace-building*, Geneva, Geneva Centre for the Democratic Control of Armed Forces (DCAF), New Brunswick and London, Transaction Publishers, 2005, p. 282.

Intelligence

Jason D. Ellis & Geoffrey D. Kiefer, *Combating Proliferation, Strategic Intelligence and Security Policy*, Baltimore and London, The Johns Hopkins University Press, 2004.

Dennis Gormley, "The Limits of Intelligence: Iraq's Lessons", London, IISS; *Survival*, Vol. 46, No. 3, Autumn 2004.

Alexander Kouzminov, Biological Espionage. Special Operations of the Soviet and Russian Foreign Intelligence Services in the West, London, Greenhill Books, Mechanics-burg, Stackpole Books, 2005.

Jeffrey T. Richelson, "MASINT: The New Kid in Town", *International Journal of Intelligence and Counterintelligence*, Vol. 14, No. 2; 2001, p. 152.

Jeffrey T. Richelson, Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea, New York, W.W. Norton, 2006.

George Tenet, *At the Center of the Storm, My Years at the CIA*, New York, Harper Collins, 2007, 832 p.

Gregory Treverton, *Reshaping National Intelligence for an Age of Information*. New York, Cambridge University Press, 2001.

Phil Williams, Intelligence Requirements for Transnational Threats: New Ways of Thinking, Alternative Methods of Analysis, Innovative Organizational Structures, Paper, University of Pittsburgh, 2006.

Useful websites

TOC Convention and Protocols: www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

Legislative Guide for TOC Convention and Protocols:
www.unodc.org/unodc/en/organized_crime_convention_legislative_guides.html

UN Global Programme Against Trafficking:
www.unodc.org/unodc/en/trafficking_programme_outline.html

International Centre for Migration Policy Development:
www.icmpd.org/traffickinginhumanbeingsgene/html

U.K. Crime Reduction Toolkits, Trafficking of People:
www.crimereduction.homeoffice.gov.uk/toolkits/tp00.htm

Guides/manuals/handbooks/practical tools

Law Enforcement Manual for Fighting against Trafficking in Human Beings - Best Practice, User's Guide and Trainer's Guide, UNDP Romania, Vienna, 2003.

OSCE Action Plan to Combat Trafficking in Human Beings, Decision No. 557/Rev.1, PCED557/Rev.1, 7 July 2005,

United Nations Office on Drug and Crime, Toolkit to Combat Trafficking in Persons, Global Programme Against Trafficking in Human Beings, New York, United Nations, 2006.

Recommended Principles and Guidelines on Human Rights and Human Trafficking, United Nations High Commissioner For Human Rights, E/2002/68/Add.1, 2002.

Human Trafficking: Reference Guide for Canadian Law Enforcement, University College of the Fraser Valley Press, Abbotsford, BC, May 2005.

National Referral Mechanisms - Joining Efforts to Protect the Rights of Trafficked Persons: A Practical Handbook, OSCD–ODIHR, Warsaw, 2004.

The IOM Handbook on Direct Assistance for Victims of Trafficking, International Organization for Migration, IOM, Geneva, 2007.

Comprehensive Anti-Trafficking Training Strategy for Law Enforcement Officials in South Eastern Europe, UNDP, ICMPD, October 2003.

Anti-Trafficking Training Material for Judges and Prosecutors: Background Reader, International Centre for Migration Policy Development, ICMPD, Vienna, 2006.

Anti-Trafficking Training Material for Judges and Prosecutors: Curriculum Training Guide, International Centre for Migration Policy Development, ICMPD, Vienna, 2006.

Anti-Trafficking Training Material for Judges and Prosecutors: Handbook, Inter-national Centre for Migration Policy Development, ICMPD, Vienna, 2006.

Strengthening Law Enforcement Capacities for Fighting Human Trafficking in South-Eastern Europe - Joint ICMPD/UNDP Romania Follow-up on Regional Training, Training Guide for Police, Border Guards and Customs Officials in EU Member States, Accession and Candidate Countries, International Centre for Migration Policy Development, ICMPD, Vienna, 2005.

Anti-Trafficking Training for Frontline Law Enforcement Officers, International Centre for Migration Policy Development, ICMPD, Vienna, 2006.

Combating the Forced Labour Outcomes of Human Trafficking, International Centre for Migration Policy Development, ICMPD, Vienna, 2005.

OCTA - EU Organised Crime Threat Assessment 2007, Europol, The Hague, June 2007, and OCTA - EU Organised Crime Threat Assessment 2008, Europol, The Hague, 2008.

Democratic Oversight of Police Forces, Mechanisms for Accountability and Community Policing, The National Democratic Institute for International Affairs, Rights Consortium, Rule of Law Series Paper, Washington D.C., 2005.

Handbook for Parliamentarians, The Council of Europe Convention on Action against Trafficking in Human Beings, Parliamentary Assembly of the Council of Europe, Strasbourg Cedex, Reprinted June 2007, at: http://assembly.coe.int

Practice Advice - Introduction to Intelligence-led Policing, National Centre for Policing Excellence, Produced on behalf of the Association of Chief Police Officers, CENTREX, Wyboston, Bedfordshire, 2007.

Geneva Centre for the Democratic Control of Armed Forces (DCAF)

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is one of the world's leading institutions in the areas of security sector reform and security sector governance. DCAF provides in-country advisory support and practical assistance programmes, develops and promotes appropriate democratic norms at the international and national levels, advocates good practices and conducts policy-related research to ensure effective democratic governance of the security sector.

DCAF Geneva
P.O. Box 1360
1211 Geneva 1
Switzerland
Tel: +41 (22) 741 77 00
Fax: +41 (22) 741 77 05

DCAF Brussels
Place du Congrès 1
1000 Brussels
Belgium
Tel: +32 (2) 229 39 66
Fax: +32 (2) 229 00 35

DCAF Ljubljana
Kotnikova 8
1000 Ljubljana
Slovenia
Tel: + 386 (3) 896 5 330
Fax: + 386 (3) 896 5 333

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine
Tel: +972 (2) 295 6297
Fax: +972(2)295 6295

www.dcaf.ch

ISBN 978-92-9222-099-0