

A Publication of the

Global Futures Partnership of the Sherman Kent School for Intelligence Analysis
Link Campus University of Malta
Gino Germani Center for Comparative Studies of Modernization and Development

NEW FRONTIERS OF INTELLIGENCE ANALYSIS

Papers presented at the conference on "*New Frontiers of Intelligence
Analysis: Shared Threats, Diverse Perspectives, New Communities*"
Rome, Italy, 31 March-2 April 2004

All statements of fact, opinion, or analysis expressed in these collected papers are those of the authors. They do not necessarily reflect the official positions or views of the Global Futures Partnership of the Sherman Kent School for Intelligence Analysis, of the Link Campus University of Malta, or of the Gino Germani Center for the Comparative Study of Modernization and Development. The papers in this publication have been published with the consent of the authors.

This volume has been edited by the New Frontiers conference co-directors.

Comments and queries are welcome and may be directed to New Frontiers conference co-director Dr. L. S. Germani : l.germani@unilink.it

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the publishers and the authors of the papers.

CONTENTS

PREFACE	5
<i>Vincenzo Scotti</i>	
INTRODUCTION	9
<i>Carol Dumaine and L. Sergio Germani</i>	
Part I - INTRODUCTORY REMARKS TO THE CONFERENCE	
1 - INTRODUCTORY REMARKS	15
<i>Gianfranco Fini</i>	
2 - INTRODUCTORY REMARKS	17
<i>Nicolò Pollari</i>	
Part II – PAPERS PRESENTED AT THE CONFERENCE	
3 - LOOKING OVER THE HORIZON: STRATEGIC CHOICES, INTELLIGENCE CHALLENGES	23
<i>Robert L. Hutchings</i>	
4- EMERGING TRENDS IN THE THREAT ENVIRONMENT: AN ASIAN PERSPECTIVE	29
<i>Peter Ho</i>	
5- INTELLIGENCE REQUIREMENTS FOR TRANSNATIONAL THREATS: NEW WAYS OF THINKING, ALTERNATIVE METHODS OF ANALYSIS AND INNOVATIVE ORGANIZATIONAL STRUCTURES	35
<i>Phil Williams</i>	

6- HISTORICAL ATTENTION SPAN DEFICIT DISORDER: WHY INTELLIGENCE ANALYSIS NEEDS TO LOOK BACK BEFORE LOOKING FORWARD <i>Christopher Andrew</i>	63
7- NEW AND EMERGING CHALLENGES FOR INTELLIGENCE ANALYSIS <i>Markus Ederer</i>	81
8- EVOLVING APPROACHES TO ANALYZING TRANSNATIONAL THREATS: KEY CHALLENGES AND POTENTIAL PARTNERSHIPS <i>David Gordon</i>	87
9- THE FUTURE OF INTELLIGENCE ANALYSIS <i>Greg Fyffe</i>	91
10 - ANALYZING TRANSNATIONAL INTELLIGENCE <i>Michael Wesley</i>	97
11 - ADAPTING TO THE ANALYSIS OF TRANSNATIONAL THREATS. CHALLENGES FOR A SMALL INTELLIGENCE SERVICE <i>Christian Jenny</i>	105
12 - THE BUDDHA AS AN INTELLIGENCE ANALYST <i>David Chuter</i>	111
13 - TOOLS, TECHNIQUES AND TEAMS FOR ANALYSIS <i>Gilman Louie</i>	127
14 - INTEGRATING METHODOLOGISTS INTO TEAMS OF SUBSTANTIVE EXPERTS <i>Rob Johnston</i>	137
15 - INTELLIGENT LEARNING <i>Max Boisot</i>	153
APPENDIX	
Appendix A “New Frontiers of Intelligence Analysis” conference program	169
ACKNOWLEDGEMENTS	179

Preface

*Vincenzo Scotti**

Unimaginable and unexpected social and political events, on the one hand, and the dramatic impact of technological innovations, on the other, have radically changed the contents and methods of strategic research in the field of intelligence. Analyses and scenarios that had been consolidated over the course of half a century have quickly become obsolete.

An eminent physicist once used the following metaphor to describe the work of contemporary scientists: “Imagine sailors out to sea who are trying to transform their clunky, bulky ship into a more streamlined one. To modify the hull of their ship they decide to use wooden beams found floating in the ocean along with beams from their old ship. However, they can’t put their boat in dry dock to rebuild it from scratch. So they set to work inside their old ship, constantly fighting against violent storms and rough waves.” This in fact is our own destiny. Although the metaphor refers to the work of the scientist in the contemporary world, it can easily apply to the work of today’s intelligence community.

Intelligence must rethink its objectives and methods. It must achieve a higher degree of transnational integration. At the same time, it must respond to the demands of decision-makers and maintain its credibility in the eyes of the public. This is the challenge laid before us by two symbolic events: the fall of the Berlin Wall in the now seemingly distant 1989, and the attack on the Twin Towers in September 2001.

The fall of the Berlin Wall was an event that, in the eighties, was impossible to imagine happening in the near future. It became the turning point at which the analyses and scenarios we had developed for interpreting the bipolar world needed to be critically re-examined and changed, along with our methods for assessing the global balance of power and regional conflicts.

In the changed global environment ushered in by the collapse of the bipolar order, intelligence communities experienced increasing difficulties in under-

* Prof. Vincenzo Scotti is President of Link Campus University of Malta, Rome.

standing the new scenarios that were taking shape. It was also difficult for them to assess the new threats to peace and security originating from actors and geographical regions of which little was known – threats which were often misinterpreted because of the continued influence of the bipolar view of the world.

The intelligence community perceived that a profound change had taken place but nonetheless found itself in a difficult situation: it had to radically rethink the work of intelligence and at the same time respond in a timely manner to the new intelligence requirements of policy-makers that had to deal with pressing new events.

A re-examination of events in the Balkans after the end of the Cold War – starting with the disintegration of Yugoslavia – can shed light on delays and errors in intelligence analysis and assessment as well as in strategy.

The attack on the Twin Towers in 2001, even more unexpected and unforeseen than the fall of the Berlin Wall, dealt a serious blow to intelligence communities, raising serious questions about their capacity to correctly interpret and assess the vast amounts of information collected. The 9/11 “intelligence failure” brought to the fore the problem of integrating the analytical efforts and partial analyses of different intelligence services into a comprehensive view of the situation.

The performance of the intelligence community overall was inadequate in three critical areas deemed particularly important for counterterrorist strategy: the threat of Islamic fundamentalism; the growth of terrorism in the Middle and Far East and the organizational structures of terrorist networks and their relationship to “rogue states.”

As a result, the intelligence community initiated a critical re-examination of its mission and methods. It began to place special emphasis on the need to fight transnational terrorist networks with transnational intelligence networks.

Transnational intelligence through networking is now a real possibility thanks to the enormous contribution of information technology and new techniques of analysis and integration of information deriving from both open and clandestine sources. Nevertheless, increased awareness and a new professionalism of the intelligence analyst are still required.

For several years now, the Link Campus University – the Italian branch of the University of Malta – has sought to make a contribution to the rethinking of intelligence by promoting conferences and seminars between academics, non-governmental research centers and government officials. The underlying theme of these meetings is a critical examination of the tasks and responsibilities of the intelligence community in the new century through a wide-ranging reflection on the nature of emerging threats and on new analytical instruments and methods. The innovative ideas developed in the United States by the Global Futures Partnership of the Sherman Kent School for Intelligence Analysis has provided crucial inspiration for our efforts.

The “New Frontiers of Intelligence Analysis” conference in 2004 gave us the opportunity to work together with the Global Futures Partnership. The conference was the result of a two-year collaborative effort between the Global Futures Partnership, the Link Campus University of Malta in Rome and the Gino Germani Center for the Study of Modernization and Development.

The papers presented at this conference are now published in this volume, which is available not only to experts and scholars, but also to policy-makers and the general public. We hope that it will contribute to the development of a new “culture of intelligence.”

Dramatic events have highlighted the need for effective intelligence structures. However, when these events become distant over time it is easy to lose sight of the need to earmark resources that will guarantee the maintenance of an effective infrastructure and ensure the training of personnel so they are well-prepared to handle the new tasks at hand.

In numerous countries, with the United States in the forefront, a discussion is under way on the need for profound changes in the organization of intelligence and national security systems, and drastic decisions are often taken in an attempt to stir into action the organizations responsible for intelligence activities.

In Italy the discussion on intelligence reform seems to drag on indefinitely, and various commissions and bills have not yet led to a definite decision that takes into account the new challenges and the need to use all the most advanced technologies that are available to us today.

The Link Campus University intends to continue to cooperate with other academic institutions and research centers in order to enhance dialogue between government officials, academics and private sector experts on key issues of intelligence reform and global security.

Introduction

New Frontiers Conference co-directors

It is our pleasure to introduce this original collection of diverse insights provided by senior security officials as well as academics and non-government specialists from around the world on how intelligence analysis can adapt to deal more effectively and creatively with the changing strategic environment of the 21st century.

The present book is an outcome of the “New Frontiers of Intelligence Analysis” conference held in Rome at the Istituto Superiore di Polizia on 31 March - 2 April 2004. The “New Frontiers of Intelligence Analysis” conference was organized by the Global Futures Partnership of the Sherman Kent School for Intelligence Analysis, the Link Campus University of Malta in Rome and the Gino Germani Center in Rome, with the support of the Presidency of the Council of Ministers of Italy.

In this brief introduction, we wish to provide some background and description about the conference from which the papers making up this book were derived. We also highlight below some of the recurrent themes and recommendations from the conference attendees.

For three days in the spring of 2004 more than 200 government intelligence analysts, security professionals, academics, business leaders, and non-government specialists from around the world met in Rome to share perspectives on the profession of intelligence analysis in the 21st century.

These professionals, in most cases meeting each other for the first time, worked together in breakout groups to discuss new pressures on and implications for the profession of intelligence analysis. They pointed to ongoing efforts and specific new actions that could be taken in order to enhance and modernize analytic capabilities. Although speakers and participants came from nearly 30 countries, many in Europe but also a few Latin American, Middle Eastern and Asian countries, there were common refrains throughout the three days. Some of the common themes and observations that emerged both from the papers presented at the meeting and the breakout group discussions include the following:

- The profession of intelligence analysis faces major challenges deriving from a rapidly changing security and intelligence environment. The key characteristics of this new environment include complexity, and boundary-less and adaptive adversaries that have harnessed advanced technologies and distributed, decentralized networks.
- In this environment of rapid change and easy access to open information, intelligence organizations face intensified public scrutiny and demands for nearly real-time and in-depth analysis.
- Traditional, evidence-based approaches to intelligence analysis are inadequate in an environment characterized by logarithmic and unpredictable change.
- Intelligence analysis is in a learning race to refine traditional and develop new analytic tools, techniques and ways of thinking in order to meet current and upcoming analytic challenges. We cannot rely exclusively on known facts nor depend on familiar analytic conceptual tools.
- Analysts must constantly question their assumptions, recognize their mindsets, and look for deeper contextual understanding. Without such vigilance, particularly in a complex security environment, cognitive and cultural biases pose growing risks.
- It is the responsibility of intelligence organizations to create an environment that provides access to traditional and new analytic tools, fosters effective and rapid learning, rewards innovation, and promotes divergent thinking.
- Intelligence agencies need to take a close look at what must remain secret and declassify information that can be released more widely for greater input and debate. Intelligence organizations and consumers must not automatically value secrets over open information.
- Sharing information is not enough. Insights must be shared across organizational, jurisdictional, and national boundaries.
- It takes a network to fight a network. Network-centric thinking and collaboration within intelligence agencies, the national intelligence communities, and the international intelligence world is essential.
- Sustained organizational commitment is necessary in order to move forward on the ideas and innovations proposed at the conference. Collective action will help all parties progress more quickly.

One recurrent theme that emerged from the plenary and breakout discussions emphasized tighter connectivity between policy makers and analysts that would enable frequent updating of analysts' understanding of intelligence consumer needs and expectations. Such feedback mechanisms also would sensitize the policy maker better to limitations in available data and analytic methods, as well as the assumptions behind analysis. Suggestions for ways to improve connectivity include:

- Broadening analysts' responsibilities from providing written products to include also advisory services for policymakers.
- Empowering the intelligence organizations to be the futures groups of governments, involving policy makers or their staffs in some of the analytic work.
- Educating and enabling policy makers to understand how the complex security environment affects analytic tradecraft, so that policy makers become public advocates of intelligence.
- Viewing strategic and tactical intelligence as complementary and providing analysts with the training and the opportunities to do both.

The participants had numerous ideas and recommendations for enhanced organizational support for analysts. These ranged across technological, methodological, and personnel policy-related fields. Suggestions included:

- Employing advanced technological tools, including an envisioned "Google-like" search capability for classified data bases, to improve the effectiveness of analysts' targeted online searches.
- Emphasizing analytic training in new tools and techniques including multiple conceptual frameworks, multiplayer gaming, interdisciplinary studies, complexity science and networked systems behaviors, creative thinking and "sense-making" methods.
- Cycling individuals from the public and private sectors through positions in the intelligence community.
- Mixing subject experts and interdisciplinary generalists, as well as team players and individualists, in analytic teams
- Hiring a culturally-diverse, technologically-savvy cadre of analysts and leveraging their capabilities

Finally, and perhaps unsurprisingly given the international diversity of the participants, there was considerable support for enhanced cross-boundary linkages and communication between analysts. For instance, participants recommended:

- Forming a multinational intelligence analysis structure in which participating states and non-government organizations could send their analysts and products for joint study and undertake joint assessment projects.
- Expanding international cooperation on intelligence issues through trust-building exercises.
- Creating global standards or guidelines for sharing information transnationally, across jurisdictions, disciplines, and government/nongovernment boundaries.

- Expanding outreach programs and partnerships with actors from outside government intelligence communities,
- Incorporating “citizen observers” into the intelligence process via blogging (web logs) and online reporting.

The participants acknowledged that collaboration does not come without risks. There are valid reasons behind some of the existing barriers to information sharing. Finally, some noted, the largest barrier of all to improving information sharing is the need to devise strict rules or “gentlemen’s agreements” that collaborators will not target their partners in information sharing arrangements: without such agreements, there can be little cooperation.

Participants shared ideas enthusiastically and most expressed interest in future opportunities to develop concepts and relationships established at the conference. Several participants and speakers commented in plenary discussions on the sense of urgency regarding the need to update analytic techniques and organizational conventions for an increasingly complex and unpredictable security environment.

Conference organizers continue to hear these sentiments more than a year after the New Frontiers conference.

Carol Dumaine* and Luigi Sergio Germani**

* Ms. Carol Dumaine is Chief, Global Futures Partnership of the Sherman Kent School of Intelligence Analysis, Washington D.C.

** Prof. Luigi Sergio Germani is Director, Gino Germani Center for Comparative Studies of Modernization and Development, Rome, and Academic Director of the Link Campus University of Malta Master of Arts Program in Intelligence and Security Studies (Rome).

PART I

Introductory remarks to the Conference

Introductory remarks

Gianfranco Fini*

When I accepted the invitation to participate in this conference, the horrific events that left Madrid stained in blood – and that struck at the heart of the entire civilized world – had yet to unfold. The urgency of the topics to be discussed over the next few days is as pressing as ever. In Europe, the need to focus attention and efforts on preventing and counteracting the terrorist phenomenon tops our list of priorities. While intelligence is not employed exclusively in the fight against terrorism, there is no question that nowadays combating terrorism has become a number one concern.

Governments are the primary users of intelligence services. Effective intelligence analysis is crucial if political decision-makers are to carry out their function of serving the national community. No matter who is responsible for laying down the lines of action for both national and foreign policies, as well as the lines of conduct for international organizations, it is the intelligence community – widely represented here today – that is expected to provide a consistent and reliable information base. This is essential for making appropriate decisions in as timely a manner as possible.

In our era, the problem of information concerning security is two-fold:

a) *To have correct and well-synthesised information.* It merely takes a quick search on the Internet to understand what “excess of information” means. The painful lesson learned from 11 September 2001 is that an excess of information can seriously hinder the decision-making process just as much as the lack of information.

b) *To have timely information,* that is, before a threat has the chance to be transformed into irreparable damage. This has particular relevance in times like ours when threats turn into reality, shooting along slim fiber optics at the speed of light. The biblical saying “If the master of the house knew at what hour the

* On. Dott. Gianfranco Fini is Deputy Prime Minister of Italy.

thief would come, he would watch, and not suffer his house to be broken into” might be updated to say “If the master of the house knew at what hour the thief was to leave his own house...” or even “If the master of the house knew that the thief had gone to buy a picklock.”

It goes without saying that loyalty and a willingness for close collaboration between intelligence services is of the utmost importance. Protection of the interests of national communities depends heavily on the readiness to share information, since the threats we are called to fight against reach far beyond the borders of individual states and will never be effectively overcome without the full cooperation of the entire international community. With this in mind, I sincerely hope that this conference will help to make a useful contribution to enhancing knowledge and strengthening mutual trust.

In light of the above considerations, the Italian Government will closely follow your work at this event and your ideas and reflections on the topic of intelligence.

It is my most wholehearted desire that during the conference you will succeed in deepening our understanding of issues that are of increasing significance for the security of our citizens.

Introductory Remarks

Nicolò Pollari*

It is a great pleasure for me to welcome all our illustrious guests to our country. I am especially delighted that this event will allow us to bring together in a single place many of the most distinguished officials in the national and international intelligence community to reflect together on the new frontiers of intelligence analysis, particularly in light of their growing strategic relevance.

The dramatic events in Madrid this month have heightened our awareness of the urgent need to strengthen international intelligence cooperation to the highest degree possible, and to seize every opportunity to determine which measures are the most appropriate in the fight against the escalation of the terrorist phenomenon.

It is evident that only constant dialogue between all the forces involved in preventing and counteracting such threats will make it possible to achieve an effective synergy geared to the successful protection of our collective security.

It is clear that Islamic terrorism has a destabilizing impact on a global level, and that it has not hesitated to strike defenceless civilians with unprecedented violence and unpredictable acts spread over time and perpetrated in the most diverse geographical contexts.

I thus believe that our common priorities must be, on the one hand, to achieve a better understanding of this complex phenomenon by means of an extensive analysis of its cultural foundations, social motivations and ideological principles and, on the other hand, to identify the most effective methods to fight adversaries who have the capacity to camouflage themselves and their intentions in the very communities they intend to destroy.

In the 12 years following the fall of the Berlin Wall up to the tragedy of September 11th, the Intelligence Services of NATO countries have had to deal with a fundamental change in the nature of threats, which have become more and more globalized.

* Gen. C.A. Prof. Nicolò Pollari is director of SISMI.

We now live in a world that enjoys more freedom, is more dynamic and more interconnected, but is undoubtedly more unpredictable. In this environment Islamic terrorism has developed gradually, alongside the threats of transnational organised crime and the proliferation of nuclear, biological and chemical weapons. The phenomenon of Islamic terrorism has characteristics very different from past forms of terrorism.

The Usama bin Lādin network was born as a platform to unify Salafites, Wahabites and the Muslim Brotherhood by offering, in the language of modern school of business administration, a strategic vision, a way of thinking, business techniques, and a common culture to hundreds of veterans from the anti-Soviet Afghan resistance and to thousands of Muslims disaffected by moderate Islamic regimes.

After Enduring Freedom, bin Lādin's network further improved its terrorism franchising techniques by providing inspiration, financial resources and specialized personnel in order to carry out new forms of attack. This network exemplifies a new variety of terrorism that has freed itself from the rules typical of the older forms of terror. It is decentralized, privatized and therefore perfectly capable of disguising itself inside the darker side of globalization.

We are already aware that neutralizing the top terrorist leadership, although important, is not enough to guarantee success, precisely because this variety of terrorism has adopted the flexibility and compactness of modern "clan" organisations – less cumbersome but just as efficient as the old hierarchical structures.

Since September 11th, more intense cooperation between intelligence services has enhanced our knowledge of the morphology and dynamics of this phenomenon, thus making it possible to sharpen the effectiveness of the techniques for countering the threat.

The road ahead of us is still long and full of dangers, especially if we consider the complexity of this phenomenon and of the environment that provides a fertile terrain for its growth: enormous political, social and economic problems, combined with ethnic demands, religious intolerance and ideological fanaticism.

The intelligence services of the third millenium can successfully respond to these challenges by developing new analytical strengths. This will constitute a decisive step forward.

Intelligence analysis will undoubtedly have to be carried out in an interdisciplinary context. Right now, the analytical process requires more than a simple synoptic and symptomatic interpretation of single pieces of information, collected and analyzed by discovering relationships between micro-data. It also requires the capacity to understand the macro-trends of present-day realities by interpreting new and complex phenomena, organizational models and instruments of propaganda that are rooted in the specific socio-cultural environments from which terrorists emerge.

Terrorism's asymmetric war is also fuelled by the simplifications of those

who, on the opposite front, are unwilling or simply unable, due to the limitations of their conceptual models, to perceive the distinctive nature of this terrorist phenomenon.

Therefore, it is necessary to acquire a new dimension of insight into cultures remote from our own, so that we may deal more flexibly and effectively with these terrorist phenomena as well as understand the environment and social context that favors their growth and spread.

In order to respond to these major challenges, intelligence must constantly adapt its technological and organizational infrastructures and update its professional culture. This is necessary to avoid the danger of being surpassed by the sudden development of new, and potentially destabilizing, instruments and means of terrorist aggression.

Consider, for instance, the intelligence community's growing interest in the "network," in all its forms and applications, and in particular in the Internet as a vehicle for new forms of communication among terrorist groups and as an instrument for creating consensus among groups with different ideologies.

Particularly significant with regard to this issue is the skilful strategy of communication conducted by al-Qa'ida, and by groups affiliated with it, which systematically uses the multimedia circuit to send out threats in messages that praise the "Holy War," exploiting the power of the media in order to spread fear and deterrence.

Intelligence therefore requires an overall process of renewal so that our security agencies, regardless of their distinctive characteristics, become less "isolated" from the outside world and more integrated with the different actors that, on both a national and an international level, guarantee the protection of our citizens and their democratic freedom.

In this conference we will have the opportunity to draw on our varied experiences in order to explore new areas of action and shared effort.

The challenge that Islamic terrorism poses to our democracies is undoubtedly a great one. It is essential that we do not waver in our collective effort to understand its underlying logic and to detect its tendencies and strategies as these emerge.

I wish to stress once again the growing importance of strengthening international intelligence cooperation to the highest possible level: comparing and sharing information, analytical techniques and methodologies, all of which are essential for the protection of our institutions and of a peaceful civil order.

PART II

Papers presented at the Conference

Looking over the Horizon: Strategic Choices, Intelligence Challenges

Robert L. Hutchings*

I would like to offer a broad-gauged look at the kind of challenges we will be facing over the next 10-20 years and how these will affect the work of intelligence. I will speak mainly from an American perspective, but many of these observations may apply to your countries as well.

In that vein, let me preview one of my conclusions: namely, that this kind of international gathering will be critical to building the intelligence coalitions we will all need to meet the challenges that lie ahead.

A World in Flux

My starting point is that we are facing a more fluid and complicated set of international alignments than anything we have seen since the formation of the Western alliance system in 1949. I would attribute the current flux to three chief factors:

- *First*, it is a commonplace but nonetheless true assertion that with the end of the Cold War and the collapse of the Soviet empire we lost the galvanizing element that held together that system. The bipolar world of the Cold War has been replaced by a unipolar global system – to which the world is still adjusting.
- *Second*, 9/11 was a turning point. Because those attacks were directed at the United States and carried out on American soil, we were uniquely affected. Our friends and allies offered sympathy and support, of course, but they did not and do not feel the same sense of urgency that we do, so the international consensus of the previous era has eroded.

* Ambassador Robert L. Hutchings is Chairman of the U.S. National Intelligence Council.

- *Third*, the breakdown of consensus over Iraq reflected a fundamental restructuring of the international system. I would add that it wasn't just because of this particular incident: that would be too simplistic an historical judgment. If the clash hadn't occurred over Iraq, it would have occurred over something else.

We are facing major flux in all the areas of the world that we have traditionally considered vital. And we are simultaneously waging a global struggle against terrorism, which can take us into countries and regions traditionally low on our list of priorities.

Challenges Facing the Intelligence Community

All of this adds up to a new set of challenges and demands on intelligence. Let me highlight just a few of them.

1. Strategic Surprise

During the Cold War, there was very little that we didn't know about the Soviet Union – at least within the universe of things we needed to know. There was a defined threat, which focused our collection and analysis. We even knew the Warsaw Pact's battle plan.

After the Cuban missile crisis, there was an increasing recognition on both sides that a certain amount of transparency was stabilizing. Each side allowed the other a degree of unfettered intelligence collection, in order to reduce the danger of miscalculation and misunderstanding.

Needless to say, that degree of maturity doesn't exist among our present-day adversaries – some of which do not even occupy a defined territory. And unlike the single massive threat of the Cold War, we must now worry about threats emanating from almost anywhere.

Even as the threat posed by state sponsors of terrorism has receded, threats from non-state actors have increased. These terrorist groups operate outside the traditional state system – beyond the reach of demarches, sanctions, deterrence, or coercive diplomacy.

To have a chance of prevailing in this environment – as CIA Director Tenet said just last week in his Congressional testimony – we must build coalitions of intelligence services to detect, monitor, disrupt, and defeat terrorist threats.

2. Denial and Deception

The threats we worry about most come from adversaries who are practiced in denial and deception (D&D) – that is, from closed, authoritarian systems that

deny access to their weapons program and develop elaborate programs to deceive outside weapons inspectors as to what their activities really signify.

We obviously faced this with respect to the Iraqi regime, which built D&D into its entire WMD program – and refined its D&D capacities over by a dozen years of international scrutiny.

In the NIE (National Intelligence Estimate) on Iraqi WMD we were aiming at a particularly hard target. Every Iraqi program had “dual-use” built in that provided a plausible cover story: this was the game of hide-and-seek that Iraq had been playing with UN inspectors since 1991.

We are facing a similar situation now in North Korea. We are applying the most sophisticated technical systems and best interpretive and analytic capabilities – and still can’t be sure. This isn’t an intelligence “failure” in the making; this is just the way it is.

3. Smaller, More Mobile Targets

We have gone from an era in which we were looking for large things in more or less fixed locations – armored divisions, missile silos, etc. – to one in which we are looking for small things on the move. This is true in the war against terrorism and in counter-proliferation efforts, and it is also true of our support to war fighters.

During Operation Iraqi Freedom, we needed to direct special operations units to individual buildings in which a key leader was known to have arrived an hour before – and then to tell them which door to enter. This requires ever more sophisticated technical means as well as improved human intelligence – and synergistic use of all the sources of intelligence from overhead imagery to communications intercepts.

Now and in the future, intelligence and military operations will be fused, from the battlefield to the national level. During Operation Iraqi Freedom, we held daily teleconferences with Centcom. This was real-time information-sharing calling for quick turn-around assessments, coordinated throughout the intelligence community. Obviously, this level of direct support to war-fighters stretches the intelligence community thin for other tasks.

4. Technological Acceleration

Technological change – information technology, biotechnology, and nanotechnology – continues to accelerate. Computer processing power per unit cost doubles every 18 months, with no end in sight. Coming advances in biotech and nanotech promise to be as sweeping.

A decade ago, we spoke about the information revolution in terms of the “CNN effect” – of intelligence and policy trying to play catch-up to the rapid dissemination of breaking news via CNN and other networks. Now the concept sounds pos-

itively quaint, having been overtaken by the “PDA effect” or “hand-held effect” in which news travels nearly instantaneously via cell phones, Blackberries, and other devices without passing through any filters whatever.

Technological innovation is by its nature unpredictable, so the impact of some of the emerging technologies on the work of intelligence is hard to forecast. But let me tick off a few trends, some positive, some negative:

On the plus side:

- Breakthroughs in biometrics and materials science – including “smart dust” – could make it possible to track individual terrorists over great distances without detection.
- New techniques in “data mining” will make it possible to extract signatures – to connect the dots, if you will – from a vast array of data.

On the negative:

- One could envision a genetically modified virus that could put mass destructive power in the hands of small groups or a single individual.
- The vulnerability of cyber-systems will grow, because the attackers are getting faster while the defenders (because of the complexity of the systems they must protect) are getting slower.

As a general proposition, our technical edge continues to shrink, as the rapidity with which information flows makes it possible for adversaries to learn our vulnerabilities – and our defenses – and adapt to them. Speed and agility become more critical than the inherent robustness of our capabilities.

5. The Challenge of Global Coverage

Let me conclude, as I began, with some broad observations about the intelligence challenges of the early 21st century. (Or, as one of my students at Princeton wrote, the challenges “for the next millennium *and beyond*”!)

The threats and issues we now face are dispersed and global, and they grow out of complex cultural roots. This means that both the breadth *and the depth* of our coverage has to be correspondingly greater.

Let me mention a few ways in which we are trying to meet these new strategic challenges. Within the NIC (National Intelligence Council), we have just created a new NIO (National Intelligence Officer) account to deal with transnational threats, including terrorism – not to duplicate the work of the many organizations dealing with day-to-day counter-terrorist work, but to look over the horizon at broader trends that day-to-day operators may miss.

On these and many other issues, we must look outside government to find the expertise on which we must draw. Here the NIC plays a critical bridging role between outside experts and policy makers.

In addition to calling on outside experts to review all of our estimates, we maintain regular contacts with hundreds of academics and other experts.

Over the past year, we have engaged a group of international relations theorists in a series of conferences to examine strategic responses to American pre-eminence – how other countries are reacting to U.S. power.

And we have launched broad-gauged studies on a wide range of issues:

- The geopolitics of energy
- New approaches to counter-proliferation
- The changing nature of warfare – technological and normative issues
- Technology and power
- China's emerging role as a regional and global power
- The sources of terrorist conduct

Finally, we have launched an ambitious, year-long project called *NIC 2020*, which will explore the forces that will shape the world of 2020 through a series of dialogues and conferences with experts from around the world.

We have held several conferences in Washington involving prominent “futurists” – the head of Shell's scenarios project, the head of the UN's millennium project, and the director of RAND's center for the study of the future – as well as regional experts and specialists on biotechnology, information technology, demography, ethnicity, and energy.

Now we are organizing workshops on five continents, drawing on experts from academia, business, governments, foundations, and the scientific community, so that this effort will be truly global and interdisciplinary.

We commissioned local partners to convene these affairs, but our role is limited to facilitation – so that regional experts may speak for themselves in identifying key “drivers” of change and a range of future scenarios.

As the 2020 project unfolds, we will be posting discussion papers, conference reports, and other material on our unclassified website, so I encourage you to follow the project as it unfolds over the coming year.

Conclusion

It may seem somewhat self-indulgent to engage in such futurology, but I see this as integral to our work. If we are entering a period of major flux, as I believe we are, it is important to take a longer-term strategic review.

We are accustomed to seeing linear change, but sometimes change is logarithmic: it builds up gradually, with nothing much seeming to happen, but then major change occurs suddenly and unexpectedly.

- The collapse of the Soviet empire is one example.
- The growing pressures on China may also produce a sudden, dramatic transformation that cannot be understood by linear analysis.

As I used to say to my students, linear analysis will get you a much-changed caterpillar, but it won't get you a butterfly. For that you need a leap of imagination. I'm hoping that the 2020 project will help us make that leap, not to *predict* the world of 2020 – that is clearly beyond our capacity – but to *prepare* for the kinds of changes that may lie ahead.

Emerging Trends in the Threat Environment: An Asian Perspective

*Peter Ho**

I am delighted to join you at this conference, and to participate in this dialogue on some of the most pressing challenges facing defense and intelligence communities around the world today. For my presentation, I would like to offer my perspective on two key security challenges facing Southeast Asia today – challenges which are also faced by many of the countries represented here.

Terrorism

The first is terrorism. With its global reach and transnational nature, and the capability and even intent to cause catastrophic damage, terrorism has become the biggest and most immediate security challenge for many countries. That is certainly the case in Southeast Asia, where the threat is very real and present. There have been two massive terrorist attacks – the Bali bombings in October 2002 and the Jakarta Marriott bombing in August 2003. There have been numerous less spectacular ones – in the southern Philippines, various parts of Indonesia, and most recently in southern Thailand, where there appears to be a sophisticated and coordinated campaign in progress.

This situation has been a long time in the making. The moderate and syncretic form of Islam that long characterized Southeast Asia began to be influenced by the fundamentalist, literal approach to Islamic doctrines of the Wahhabi school from the late 19th century, gathering momentum as large numbers of pilgrims went on the *hajj* and more and more Muslim clerics attended *madrasas* (or Islamic schools) in Saudi Arabia.

However, the catalyst for radicalisation was participation – and victory – in the *jihad* (or holy war) in Afghanistan against the Soviet Union from 1979 to

* Mr. Peter Ho is Permanent Secretary of Defence, Singapore.

1989. That gave the Southeast Asian men who answered the call, possibly numbering in the thousands, access to training, contacts and ideology. In Afghanistan, al-Qa'ida taught these *mujāhidīn* (or fighters) terrorist tradecraft. When they returned home, they were fired up to start their own militant Islamist groups and they turned their sights to *jihād* closer to home. At the same time, a constant supply of new recruits was and continues to be provided by radical *madrasas* in Pakistan and increasingly by Wahhabi-funded *madrasas* in Southeast Asia.

Militant groups in Southeast Asia are part of a much wider, tangled web of transnational terrorism. Even before September 11th, al-Qa'ida had already extended its tentacles into Southeast Asia. It provided funds and training to the Abu Sayyaf Group and the Moro Islamic Liberation Front, or MILF, in the southern Philippines. In Malaysia, al-Qa'ida has links with the Kumpulan Militan Malaysia, or KMM; and in Indonesia, with the Jemaah Islamiyah, or JI, the Laskar Jihad, and the Majelis Mujahidin Indonesia.

These al-Qa'ida affiliates, in turn, have training and operational ties that extend beyond their local support bases. For instance, Laskar Jihad in Ambon, Indonesia, was until recently thought of as a local separatist movement fuelling Muslim-Christian violence in the Moluccan islands. However, the logic of the *ummah* (or universal Muslim community) unites militant Islamist groups in their goal of Islamising the societies – or indeed the world – around them. Right at the centre of this web of militant Islam in Southeast Asia is the JI network. Its aim is to establish a pan-Islamic entity encompassing Indonesia, Malaysia, Singapore, Brunei, the Philippines and southern Thailand. It was responsible for the bombings in Bali and Jakarta, as well as others in various parts of the Philippines and Indonesia. It had planned but was unable to carry out an attack on the APEC Summit meeting in Bangkok in October last year.

The Singapore security authorities uncovered the JI group in Singapore shortly after the September 11th attacks. We found that they had plans to attack foreign assets in Singapore, such as Western embassies, commercial buildings housing Western firms; our international airport at Changi; chemical plants; the Ministry of Defence; the Ministry of Education; and the water pipelines between Singapore and Malaysia. Our investigations revealed that the JI terrorist operation to be a multinational enterprise. In Singapore, they had used local JI members to conduct the reconnaissance of potential targets. A regional expert would then be brought in to build the bombs, and yet other foreign experts from the Middle East would be brought in to carry out the attack. Since the uncovering of the network, the Singapore authorities have detained 37 persons with links to the JI and MILF.

Over the past year, the security authorities in the region have shown resolve in cracking down on JI militancy. About 200 JI members, including key operatives, and radicals with links to JI, have been arrested throughout Southeast Asia

– in Indonesia, Malaysia, the Philippines, Thailand, Singapore and recently even in Cambodia. While this has disrupted the JI network, the organization as a whole still poses a very serious threat. There are indications that the JI has successfully regenerated its leadership, thanks to its resilient networked organizational structure, similar to al-Qa’ida’s, and its transnational, symbiotic links with other militant Islamist groups. New terrorist plots are regularly being uncovered, such as the plans for attacks in Jakarta and West Java during the Christmas season last year.

Just as the terrorist enterprise is multinational, the authorities’ response has also to be multinational. Cooperation among the regional governments and their security agencies, especially in the form of intelligence sharing, has been critical in enabling the arrest of JI members in various countries throughout Southeast Asia and in emasculating parts of the network. Besides such cooperation, governments in the regional countries would also need to demonstrate political will to confront the threat. In this regard, there is concern that upcoming elections in the region could be a distracting factor, as political parties pander to the demands of the Islamists. For instance, the jail sentence for the JI’s spiritual leader Abu Bakar Baashir was recently halved from three years to 18 months – a development which many took to be a result of the influence of politics in the current heated climate in Indonesia.

The radical Islamists, the terrorists, see this as an ideological battle. They are able to exploit the global trend of increasing religiosity in the Muslim world, and find cover in the growing politicization of Islam in Southeast Asia. Clearly, it is a battle that will take many years, and perhaps several generations. For every terrorist neutralised, the charismatic preachers and leaders who are the *queen bees*, men like Abu Bakar Baashir, can produce dozens and hundreds more in radical religious schools that are propagating an uncompromising brand of Islam. The war against terrorism is also a battle for the hearts and minds of Muslims. Ultimately, only Muslims themselves – those who strive for a peaceful, moderate Islam compatible with the modern world – can effectively counter the ideology that has been twisted out of a perverted interpretation of Islam.

In the meantime, governments can – and must – take preventive and protective measures to effectively counter the threat of terrorism. They will have to improve cooperation with one another, and work more closely together to counter this common enemy. Security and intelligence agencies could cooperate to identify groups that do not have direct links to known militant groups but that, nonetheless, play a central role in recruiting susceptible young people to the extremist cause. These include *madrasas* and grassroots organizations that have been infiltrated by foreign Wahhabist elements, which poison the minds of moderate Muslims and help produce foot soldiers for the militant cause.

Maritime Security

The transnational terrorist threat in Southeast Asia also poses a real and present danger for maritime security – which is the second security concern I would like to address. Maritime security has always been an issue of critical importance even before 9-11, as sea-borne trade is a critical element for our region's prosperity. Singapore, for instance, sits on one of the world's most important sea lines of communication, with over a quarter of the world's trade and half its oil passing through.

In the past, sea-borne threats generally took the form of piracy and armed robbery against ships. But these days, piracy is only one aspect of maritime security that we need to be concerned about. Post September 11th, maritime targets are obviously lucrative ones, more so after the hardening of land and aviation targets. The disruption of sea-borne commerce would have a serious impact on the international economy, with not just economic but also strategic repercussions for the whole world. The challenge of securing ships and ports from attack, and ensuring the freedom of navigation, is an enormous one. We know that the terrorists have been studying maritime targets across the region. For example, when we cracked down on the JI network in 2002, we found preliminary plans for suicide attacks on US naval vessels calling at Singapore. Terrorists could also resort to pirate tactics to hijack supertankers, LPG or chemical carriers to turn them into floating bombs.

Another challenge for maritime security is the need to counter the proliferation of weapons of mass destruction at sea. The use of shipping for conveying WMD components and materials means that proliferation over the seas has serious implications for global security and the global trading system. More immediately and directly, more frightening, is the prospect of these two huge threats being combined. In the event of a successful attack, the catastrophic consequences would not just hit the target country but also the maritime trade system and global trade in general.

Cooperation among the multiple stakeholders is key. This includes governments and their agencies as well as our commercial partners. Good intelligence sharing among like-minded countries is an important prerequisite for effective maritime security. For example, with over 18 million containers passing through Singapore's ports each year, it is not possible or economically feasible to open every container for inspection. Good and comprehensive intelligence is therefore indispensable. Containers must be profiled, through the comprehensive tracking of their movements, and that information must be efficiently disseminated so that ports all over the world can pick up suspicious cases for closer inspection. In the case of transshipments, some of which never leave their ships, developing the international ability to comprehensively track and profile these vessels is also vital. Finally, initiatives for tracking and building up maritime situa-

tional awareness would further have to be complemented by a system to operationalize the interdiction of suspicious vessels.

As a maritime nation and the world's busiest transshipment port, maritime security is naturally a vital component of Singapore's national security efforts. Not only have we stepped up efforts to enhance the security of our waters, Singapore also actively plays our part in contributing to the international efforts to bolster maritime security. We were the first Asian port to implement the Container Security Initiative and have recently become a core group member of the Proliferation Security Initiative.

Conclusion

This brief sketch of two immediate security challenges, which I have outlined today, affirms the indispensability of international cooperation and intelligence sharing. Good intelligence is a pre-requisite to the early identification and tackling of these security challenges. At the same time, having good intelligence is, like having all the pieces of a jigsaw puzzle, necessary but not sufficient. The further challenge is to connect the many pieces on the table. That is, to develop an information-sharing mechanism that collates, systematises and connects the pieces of intelligence and makes it available to those who need it. This requires the coordination of local intelligence with global initiatives. Given the complex transnational links between various militant groups in the Southeast Asian region alone, which we still have an imperfect understanding of, the conclusion is that we cannot systematically root out the networks that fuel and perpetrate international terror without effective international collaboration. I trust that this conference will go some way towards exploring avenues to this end.

Intelligence Requirements for Transnational Threats: New Ways of Thinking, Alternative Methods of Analysis, and Innovative Organizational Structures

*Phil Williams**

Introduction

The terrorists attacks on Sept. 11 2001 demonstrated the urgent need for the US government to use insights from “complexity science” to better understand our interconnected world... Policymakers and analysts need a new way of thinking, and new models for analysis and reporting that reflect the complex, nonlinear, and dynamic realities of the world in which we live. (T. Irene Sanders)¹

The strategy we have recommended is elaborate...To implement it will require a government better organized than the one that exists today, with its national security institutions designed half a century ago to win the Cold War. Americans should not settle for incremental, ad hoc adjustments to a system created a generation ago for a world that no longer exists. (9/11 Commission Report)²

Events since the end of the Cold War have confounded many analysts of global politics, piling one surprise on top of another. The United States intelligence community has been no exception, failing as it did to anticipate the difficulties – largely caused by organized crime – in the transition of the states of the Former Soviet Union from authoritarianism and command economies to liberal democracies and free markets, the Asian financial crisis, which both stemmed from and created contagion effects, the rise of Islamist terrorism and the attacks of September 11, 2001, the outbreak and spread of SARS, the spread of WMD technologies through the illegal diffusion networks of Pakistani nuclear scientist,

* Prof. Phil Williams is Professor of International Security at the Graduate School of Public and International Affairs, University of Pittsburgh.

¹ See T. Irene Sanders, “US must invest in science of dot-connecting,” *Christian Science Monitor*, 17 June 2004.

² *Final Report of the National Commission on Terrorist Attacks Upon the United States: Executive Summary* (Washington DC.: July 2004), p.20.

A Q. Khan, and what, somewhat ironically, might be described as weapons of mass disappearance in Iraq.

The litany of surprise is even more substantial than these examples suggest. It is also particularly embarrassing for United States intelligence agencies charged with the responsibility for anticipating future events and providing warning to policy-makers. So too is the report of the 9/11 Commission, which concluded that prior to September 11, 2001 the intelligence and policy communities had displayed failures of imagination.³ Even more ominously, the report noted that “al-Qa’ida’s new brand of terrorism presented challenges to U.S. governmental institutions that they were not well-designed to meet”⁴ while contending that “the missed opportunities to thwart the 9/11 plot were also symptoms of a broader inability to adapt the way government manages problems to the new challenges of the twenty-first century.”⁵ The Commission’s assessment was very damning of both ways of thinking and organizational structures and processes.

The 9/11 Commission’s recommendations, however, focused mainly on structural reform emphasizing, among other things, the need for a new Director of Intelligence and the creation of a National Counterterrorism Center. In making these recommendations, the Commission has added its voice to the widespread demand for reforms designed to enhance the performance of the intelligence agencies and to minimize the prospects for future surprise. Proposals have ranged from the creation of an intelligence czar with real budgetary authority over the multiplicity of agencies that make up the intelligence community in the United States to the establishment of a new body for domestic intelligence along the lines of Britain’s MI5.

While some of these proposals for reform offer little more than organizational tinkering, others seek to dismantle permanently the barriers that have inhibited real sharing of information, especially between traditional national security intelligence agencies on the one side and law enforcement agencies on the other. Such dismantling is essential to a new environment in which the intelligence space is borderless and many threats are transnational in character. Progress has already been made in this direction through the Terrorist Threat Integration Center, and the creation of a National Counterterrorism Center would both consolidate and enhance the gains that have been made.

It is arguable, however, that the problems are not simply those of architecture or structural design. In fact, the shortcomings of the intelligence process go much deeper, and involve: (1) traditional and, in many cases, obsolete ways of thinking about a threat environment that is novel and unprecedented in its com-

³ Ibid., p.9.

⁴ Ibid., p.9.

⁵ Ibid., p.10.

plexity; (2) methods of analysis based in large part on notions of scientific inquiry that are increasingly, if often tacitly, called into question by an important segment of the scientific community; and (3) organizational structures well-suited to the relative stability of the Cold War but which are totally inadequate in a world where the threats are transnational, networked, distributed, and highly adaptable.

Against this background, this paper seeks to offer a set of prescriptions and recommendations for rethinking the challenges facing intelligence and for reorienting the intelligence community in ways that go well beyond organizational tinkering. Indeed, the recommendations enunciated below involve changes – some modest and some more radical – in the ways we think about transnational threats, the ways we analyze these threats, and the ways we structure the institutions within which this thinking and analysis is carried out. Starting from the assumption that the change in the threat environment has been profound, the paper contends that equally profound changes are required in intelligence thinking and intelligence analysis, as well as in structures and processes, if the prospects for catastrophic surprise are to be reduced and an in-depth understanding of the twenty-first century world is to be acquired.

A radical approach to intelligence in the new security environment is essential. Anything less will be little more than a palliative and, although it might silence domestic criticism temporarily, it will do little to enhance the analytic process or to avoid surprise. At the same time, the baby must not be thrown out with the bath water. Although it is crucial to move beyond traditional assumptions that were appropriate to state-based threats but are less relevant and useful when the main threats and challenges come predominantly from non-state or “sovereignty-free” actors, it also has to be acknowledged that traditional state threats have not disappeared.⁶ Consequently, some of the old ways of thinking about threats cannot simply be discarded: a paradigm shift in intelligence is required; yet there are components of the old paradigm that must be retained, if only as a hedging strategy. The twenty first century threat environment involves not only new, unorthodox, unfamiliar, and poorly understood threats, but also the potential for the re-emergence of more traditional, familiar, and well-understood threats emanating from great powers challenging United States hegemony. Traditional geopolitics and transnational forces are not alternative lenses on the world but overlays that need to be placed on top of one another for a more complete picture.

If traditional geopolitical threats have not disappeared, however, they have diminished significantly, and do not need to be given the level of attention and resources they received in the past. The need for caution, therefore, is not an ex-

⁶ The term “sovereignty free actors” was coined by James N. Rosenau. See his *Turbulence in World Politics* (Princeton: Princeton University Press, 1989).

cuse for inaction: efforts must be made to make sense of the new security environment and the challenges that typically arise within it. The major proposition here is that the security environment has undergone the equivalent of a shift in tectonic plates, with the result that only shifts of an equivalent magnitude in the way we think about this environment and analyze the new security threats will provide an adequate basis for good intelligence and sound decision-making in the first few decades of the twenty first century.

Paradigm Shifts and Complexity Theory

Some of the keys to the necessary paradigm shifts are provided in the work of David Snowden, whose focus is primarily on management and information science but whose insights about the acquisition and management of knowledge are enormously relevant to the world of intelligence analysis.⁷ According to Snowden “the conceptual changes required for both academics and management are substantial, effectively bounding or restricting over a hundred years of management science in a similar way to the bounding of Newtonian science by the discoveries and conceptual insights of quantum mechanics et al. in the middle of the last century. These changes are not incremental, but require a phase shift in thinking that appears problematic, but once made reveals a new simplicity without the simplistic and formulaic solutions of too much practice in this domain.”⁸ Such comments are equally relevant for intelligence analysts and managers.

The key development underlining the need for this paradigm change or conceptual shift is the shift from known and knowable environments where there is order to environments in which there is “un-order” characterized by complexity or by chaos. These four domains – along with the approaches required to respond to or cope with each one of them – are explored and elucidated by Snowden.⁹ They are highlighted in the following figure taken directly from his analysis.

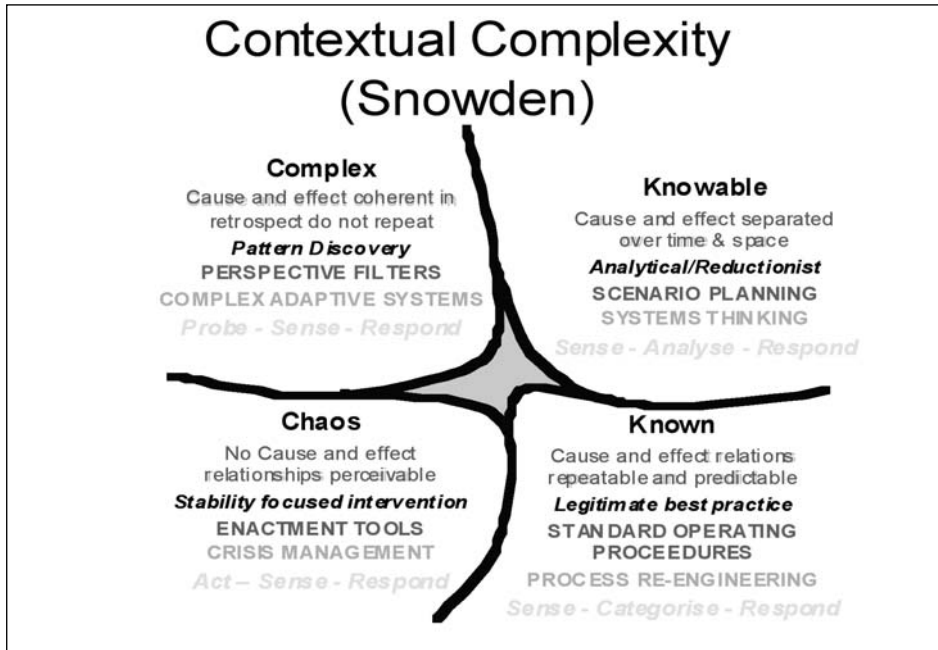
In Snowden’s judgment, both the known and knowable domains are analytically tractable. Surprise can certainly occur, especially in the knowable domain where many things are still undiscovered and there is a natural tendency to assume that existing, well understood, and precisely delineated, patterns of behavior will continue into the future – without sufficient consideration of change or novelty within the domain itself. With caution and care, however, the potential

⁷ David Snowden, “Complex Acts of Knowing: Paradox and Descriptive Self-Awareness,” in *Journal of Knowledge Management*, Vol. 6., No. 2 (May 2002).

⁸ *Ibid.*, p.2.

⁹ *Ibid.*, p. 5.

Figure 1



for surprise can be minimized. Intelligence analysts can be expected to perform like quarterbacks where an exceptionally high completion rating (80 percent) is necessary for induction into the hall of fame. The analysts can be expected to get it right most of the time. This was certainly the case for much of the Cold War in which United States intelligence developed a set of indicators and warnings that were sensitive to even small changes in Soviet force deployments and alert levels. Moreover, apart from the introduction of Soviet missiles in Cuba in 1962, the Soviet Union proved a relatively cautious and predictable adversary and the United States record of predicting its behavior – although not always its capabilities – was a very respectable one.

When the domains shift to complex and chaotic, however, the difficulties of forecasting or anticipating become immensely more difficult. It is the difference between predicting Soviet strategic behavior during the Cold War and predicting the collapse of the Soviet Union and the end of the Cold War. The dynamics of political and economic collapse were not well understood, and even when there were hints of Soviet weakness and decay, they ran up against 50 years of countering an enemy which was as formidable as it was implacable. With the focus on the monolith itself, the cracks in the foundation were given little attention. Yet, this should not really be surprising. State or system collapse is a highly complex phenomenon and complexity can be difficult both to comprehend and to navigate.

In a complex system, for example, cause and effect are not readily distinguished, independent and dependent variables merge into interdependent variables, and it is only in retrospect that a coherent picture can be determined – a phenomenon that Snowden terms “retrospective coherence.”¹⁰ At the same time, it is possible in such systems to identify and even influence interactions – partly through what Snowden terms probing behavior – and discern emergent patterns. As Snowden put it: “in a complex space we cannot sense and respond, but must first probe the space to stimulate pattern understanding or formation, then sense the patterns and respond accordingly.”¹¹

In the chaotic domain, however, patterns do not emerge naturally through interaction, nor are they discernible simply through probing behavior. Instead, they have to be imposed as a result of crisis management behavior. Again in Snowden’s words, “in the chaotic domain the most important thing is to act, then we can sense and respond.”¹² Intelligence analysis in both the complex and chaotic domains is particularly difficult, more like a baseball batter than a quarterback, where a relatively low percentage of strikes (30 percent) if sustained will guarantee entry into the baseball hall of fame. Even if the focus is on the complex rather than the chaotic, the intelligence challenges are both formidable and forbidding. The shift from the known and knowable domains imposes formidable requirements and new challenges.

If the threat environment has indeed moved from the knowable into the complex, simply recognizing this, and changing ways of thinking about and analyzing threats will go a long way towards enhancing intelligence. Complexity has certain patterns associated with it, and once these patterns are discerned and understood then they can provide considerable insight into possible developments and manifestations of threat.

Understanding complexity guarantees neither highly effective intelligence analysis nor an absence of surprise, but it will increase the prospects for good analysis that offers insight and, on occasion, might even provide a degree of warning that would otherwise be absent. If this does not seem particularly upbeat, it is perhaps the most that can be achieved in an era characterized by Eliot Cohen as the “age of surprises.”¹³ Yet even achieving this will be no small task.

Changing ways of thinking, established assumptions, existing preconceptions, and familiar techniques and methods of analysis is not easy. It requires that analysts make explicit efforts to move beyond the comfortable familiarity of the known to a kind of intellectual terra incognita. This is particularly important when the existing preconceptions about the threat are not only irrelevant and

¹⁰ Ibid., p.7.

¹¹ Ibid., p.8.

¹² Ibid., p.9.

¹³ Eliot A. Cohen, “A Tale of Two Secretaries,” in *Foreign Affairs* (May/June 2002).

misleading but actually inhibit understanding of the ways in which analysts need to view and analyze transnational threats.

Against this background, this paper seeks to identify those characteristics of complexity and complexity theory which, it is argued, are particularly important in relation to intelligence analysis for transnational threats. These range from the notion of holistic analysis, which requires an understanding that a system (whether an eco-system or a threat system) is much more than the sum of its parts, to the idea of emergent behavior.

Extracting key themes from something as sophisticated as complexity theory is a potentially dangerous activity, particularly for the non-specialist, and especially when the various components of complexity are themselves inextricably inter-connected. Nevertheless, it is essential to highlight themes and ideas with significant implications both for thinking about threats in a complex environment and for analyzing these threats. Only after this brief elucidation of complexity is it possible to consider the implications for intelligence. Complexity itself is best understood as the space or domain between chaos and order and can move in either direction, often as a result of small changes. This is why complexity is sometimes described as being located at the “edge of chaos” or as the zone between chaos and order and capable of moving in either direction.¹⁴

- A key theme in complexity theory is that the system as a whole has to be the focus of considerable attention. As Baruch Blumberg noted, “for nonlinear systems the whole is greater than the sum of the parts, and they can only be understood by examining ‘global’ behaviors in addition to the individual agents of which they are comprised.”¹⁵ This is sometimes termed the macroscopic level, and it suggests that a holistic perspective is essential.¹⁶
- A complex system is also a non-linear system in which “small inputs can lead to dramatically large consequences,” something that is often summarized as the butterfly effect.¹⁷ Moreover, these effects can differ very dramatically since “very slight differences in initial conditions produce very different outcomes. That’s the basis of their unpredictability.”¹⁸ Outcomes depend critically on the context or the initial conditions surrounding the starting point.
- The transition from complexity to chaos or order can also be understood as the equivalent of what scientists often refer to as a “phase transition” between

¹⁴ See Roger Lewin, *Complexity: Life at the Edge of Chaos* (Chicago: Chicago University Press, 1999).

¹⁵ Quoted in Peter Coveney and Roger Highfield, *Frontiers of Complexity* (New York: Fawcett Columbine, 1995), p. xi.

¹⁶ The idea of macroscopic is discussed in *Ibid.*, p. 7.

¹⁷ Lewin, p.11.

¹⁸ *Ibid.*.

solids, liquids and gases.¹⁹ As one complexity theorist noted, “as you approach the boundary and cross it, you suddenly get a phase change.”²⁰ Another way of describing the same phenomenon is in terms of a “tipping point.” This is a notion popularized by Malcolm Gladwell in a study that seeks to explain a variety of phenomena ranging from epidemics to fashion trends which can be understood as a form of social contagion involving imitative behavior.²¹ Gladwell emphasizes that little changes can have big effects and can tip the system from one condition to another.

- Complex systems involve self-organization and emergent behavior. Self-organization involves tacit rather than explicit coordination and does not require leadership or top-down hierarchical structures. The notion of emergent behavior also contains the idea of the learning organization. Emergent systems create a complex global order out of very simple decision rules, but as the order evolves the decision rules can become more sophisticated. The idea of adaptability and, in the context of organizations, the notion of organizational learning is critical – and highly relevant to the understanding of transnational threats.
- A corollary of the idea of adaptation is that of coevolution, a phenomenon that is ubiquitous in nature. As Mark C. Taylor has written, “Since complex systems are adaptive, their evolution tends to be coevolution. When systems as well as networks adapt to systems and networks that are adapting to them, change is necessarily correlative.”²² Examples of this are “parasites, symbionts and tightly coupled dances” such as that between the parasite and the milkweed.²³
- A closely related feature of complexity is the notion of inter-connectedness. This manifests itself largely through networks, which can be understood as one form of emergent system. Indeed, the notion that networks are a sub-component of complexity theory has been most fully articulated by Barabasi, who in the last few years has provided some very illuminating analyses of the topologies of networks and how some kinds of topology are more resilient than others in the face of attacks on the network.²⁴

¹⁹ Mark C. Taylor, *The Moment of Complexity: Emerging Network Culture* (Chicago: Chicago University Press, 2001), p. 25.

²⁰ Chris Langton, quoted in Lewin, p.17.

²¹ Malcolm Gladwell, *The Tipping Point* (Boston: Little, Brown 2000).

²² Taylor, pp. 188-189.

²³ Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World* (Cambridge, MA: Perseus, 1994), p.75 and p.76.

²⁴ A.L. Barabasi, *Linked: The New Science of Networks* (Cambridge, MA: Perseus, 2002).

- Yet another concept in complexity theory relevant to the tasks of intelligence is the notion of a fitness landscape and fitness peaks. “A fitness landscape is a mountainous terrain showing transition locations of the global maximum (highest peak of fitness) and global minimum (lowest valley). Fitness is a biological concept which describes the relative ‘success’ of a species in relation to others in its environment.”²⁵ The height of a feature becomes a measure of its fitness.

This is a greatly simplified summary of the ideas of complexity and, as such, it omits concepts such as attractors and autopoiesis (“the process by which living creatures constantly recreate and maintain themselves and their own identity”²⁶), while greatly over-simplifying others.²⁷ Nevertheless, even a crude summary of this kind can assist us in the way we think about transnational threats. Complexity theory can be helpful both indirectly as a heuristic device and as a direct way of understanding transnational threats, whether terrorism, transnational organized crime, or infectious diseases. It can not only help us to identify some of the characteristics of transnational threats, but also suggests ways in which these threats can be analyzed.

Understanding the Transnational Threat Environment

Unlike traditional threats to national security stemming from rival nation-states, transnational threats are more difficult to anticipate, to assess, and to combat. These threats can be understood in several ways: they are global; they emerge from ecologies of malevolence; they are networked and distributed; they are emergent in form; they adapt and evolve (or co-evolve) as states adapt by developing strategies to combat them; and they become more or less serious depending on the direction in which they tip. Consequently, this analysis focuses on several aspects of the threat environment.

1. The Global Borderless Intelligence Space

In thinking about transnational threats, it is important to keep in mind that they are global. This is certainly compatible with the notion of the macro-level of complexity and the need to consider the system as a whole. The implication for intelligence is that it is necessary to think in terms of a global borderless intelligence space. Indeed, the old distinction between domestic and international

²⁵ Arthur Battram, *Navigating Complexity* (London: The Industrial Society, 1999), p.210.

²⁶ *Ibid.*, p.225.

²⁷ For a fuller discussion of some of these concepts see T. Irene Sanders, *Strategic Thinking and the New Science* (New York: Free Press, 1998).

has broken down in relation to threats that can as easily be embedded in our own society as in other societies. Moreover, transnational threats have a nomadic quality: they are highly mobile and although they occasionally touch down – sometimes for extended periods – in particular localities, countries or regions, as discussed below, they can also have a presence in multiple places simultaneously. The other implication here, of course, that in many respects the world has become borderless. Diseases spread across borders as easily as they spread within countries – as was evident in the way SARS moved from Hong Kong to Toronto. Similarly, for criminal organizations and terrorists, national borders have become no more than inconveniences, at least offensively (while they sometimes try to use national sovereignty as a defensive measure).

The implication of the global borderless intelligence space, therefore, is that analysts focusing on transnational threats need to combine specific geographic expertise with a global vision. Moreover, because of the geographic diversity of transnational threats, teams which combine functional expertise on particular threats with combinations of country and regional expertise are likely to prove particularly valuable.

2. The Context: Ecologies of Malevolence

Since September 11, some critics of the United States war on terrorism have argued that the military response needs to be accompanied by greater understanding of the “root causes” of terrorism. Often implicit in this contention is the notion that the United States is one of the root causes. Partly because of this and partly because of the continued efforts to deal with the present threat from al-Qa’ida little attention has been devoted to this aspect of the problem. Yet, as suggested above, in considering complexity, context is very important and cannot be neglected in any effort to understand emergent behavior.

One way of looking at the context for transnational threats is in terms of what can be described as ecologies of malevolence – a combination of factors that together breed instability, crime, terrorism and disease. Resulting from poor governance often combined with poverty and repression and demographic trends leading to a “youth bulge,” these ecologies have become deeply entrenched in parts of the world such as Afghanistan, Central Asia, and much of West Africa. For a variety of reasons these regions incubate resentments that can lead to efforts to get even with the developed world (through terrorism) or to get rich through rule-breaking behavior (organized crime and corruption). Because of the prevailing conditions, they also tend to be breeding grounds for disease. Not surprisingly, they also exhibit signs of contagion, with crime being exported from these regions and terrorist networks moving into the region, either in search of money-making schemes or safe havens.

It is not a single factor, however, but the interaction of multiple parts that creates the environment in which violence, terrorism, organized crime and disease

– all contemporary threats to security – flourish, and from which they are exported. Significantly, there is no single set of conditions that acts as an incubator of terrorism, organized crime and disease. Rather there are various combinations of factors that lead to these phenomena. Terrorism and organized crime, for example, can emerge from rural areas and from massive urban conurbations, as well as from radicalism that can be bred by poverty or religion, or by a potent combination of both. Disease can arise as a result of a mix of deforestation, poor living conditions, and the lack of basic health care and so on. One omnipresent condition, however, is poor governance which in some cases results from lack of state capacity and in other cases stems from the way in which political elites place private interests above the public interest.²⁸

The other critical characteristic of these ecologies of malevolence is that they are globally connected. If the ecologies of malevolence were both isolated and insulated from the rest of the world, they would not be a problem. Unfortunately both transnational criminals and transnational terrorists exploit globalization as a great facilitator in the linkages they forge between areas of poor governance and areas of good governance. In effect, the ecologies of malevolence expand outwards in ways that render national borders irrelevant.

3. *Tipping Points and Epidemics*

Another extremely useful way of looking at transnational threats can be derived from Gladwell's analysis of tipping points and his notion that certain phenomena can be understood in terms of epidemics – whether of disease or of particular activities such as crime and terrorism.²⁹ Indeed, it is possible to distill from the tipping point analysis several key ideas that can be used to understand the rise of transnational organized crime and the rise of Islamic terrorism in the 1990s:

- The law of the few – people who, in one way or another, have high standing within certain communities, inspire certain forms of behavior, set examples that others seek to emulate and perhaps most important of all in Gladwell's terms, “are critical in spreading information.”³⁰
- The stickiness of ideas. As Gladwell has noted, “There is a simple way to package information that, under the right circumstances, can make it irresistible.”³¹ Certain kinds of ideas also prove attractive, either because they appear to solve problems or because they tap into alienation and despair and

²⁸ This fundamental point is made by William Reno, *Warlord Politics and African States* (Boulder Co.: Lynne Rienner, 1999).

²⁹ Gladwell, *op.cit.* .

³⁰ *Ibid.*, p. 139.

³¹ *Ibid.*, p.132.

offer an outlet for the attendant rage that often goes with this. Such ideas often prove contagious and we see considerable imitative behavior as individuals and groups succeed in what they are doing, thereby providing an example for others to follow.

- The power of context. As Gladwell notes, “epidemics are sensitive to the conditions and circumstances of the times and places in which they occur.”³² He also argues that behavior is often highly dependent on context and differs considerably according to context.

The result of all this is that little causes can have big effects, and change happens not slowly but at “one dramatic moment” that is the tipping point.³³ When that point is reached, there is a social equivalent of a phase transition in complexity science as problems expand from stable and manageable proportions to epidemic proportions in which they are essentially out of control.

This can very easily be translated into what can be understood as an epidemic of transnational organized crime in the 1990s. Nowhere was this more significant than in Russia. The rapid expansion of organized crime in Russia and its rapid development into a transnational phenomenon can be understood in terms of Gladwell’s model of the tipping point. In the first place there were people with authority and ideas who became natural organizers. In some cases, these were *vory v zakone*, thieves professing the code, who made up the traditional criminal class in the old Soviet Union; in others they were new criminal entrepreneurs who quickly realized that with the collapse of the Soviet Union and the introduction of capitalism, there were new opportunities to get rich quick. Figures such as Semën Mogilevich and Sergei Mikhailov who reportedly became the leaders of the Solntsevo criminal organization were originally based in southwest Moscow, but soon developed a portfolio of international criminal activities to accompany Solntsevo’s extortion and other criminal activities in Moscow. The collapse of the social control mechanisms of the Soviet state provided a very permissive context, and, within this, organized crime began to appear highly attractive to people who had few alternative opportunities for sustained employment let alone making considerable amounts of money. Many organized crime figures flaunted their wealth, driving luxury cars and wearing ostentatious watches and gold jewelry. For deprived youth the lifestyle seemed to carry lots of rewards and few risks.

In effect, the situation tipped from one where organized crime was a serious but contained problem to one in which organized crime became a major challenge not only to the new Russian state but also to the efforts to achieve a liberal democracy and a free market economy. Parallel developments occurred in oth-

³² Ibid., p. 139.

³³ Ibid., p. 9.

er states in transition creating a serious organized crime problem in countries where such a problem had hitherto been minor or nonexistent.

A similar framework also helps to understand the rise of Islamic terrorism. A charismatic leader, Usama bin Lādin, combined with a superb organizer, Zawahiri, had shown very graphically (at least in their minds and those of their followers) in Afghanistan that a superpower could be defeated. The idea of turning the *jihād* against the Soviet Union into a *jihād* against the United States elicited considerable enthusiasm in the Islamic world, where the United States presence in Saudi Arabia combined with its strong support for Israel in the struggle with the Palestinians to create a groundswell of resentment. Indeed, it is arguable that bin Lādin was acutely aware that he was a messenger; in addition his message was very simple, with the result that he has been able to win – certainly in the Muslim world – what Arquilla and Ronfeldt call the “battle of story.”³⁴ And because of key characteristics of the environment – the adverse effects of globalization in parts of the world including the Middle East, along with the continued festering of the Palestinian problem – both al-Qa’ida’s cause and its example resonated significantly throughout the Islamic world, inspiring both imitation and emulation – and attracting large numbers of recruits, some of whom were willing to be suicide bombers.

4. Networked and Distributed Threats

Another characteristic of transnational threats illuminated by components of complexity theory is the way in which these threats are networked. Indeed, networks provide the connectedness that is a fundamental part of complex systems. One of the key findings to come out of the study of large scale networks by Barabasi and others is that not all nodes are created equal. A clear distinction has been made between random networks in which all nodes have a similar (and usually a small) number of links to other nodes, and scale free networks in which a few nodes have an extremely large number of links. Networks with these super hubs degrade gracefully under random attack but are vulnerable to targeted attack designed to destroy the hubs.³⁵ This notion of network topology can be applied to criminal and terrorist networks and suggests that analysts should look for critical nodes in the network.³⁶ Critical nodes can be described as high in importance (they create a lot of linkages and make network distance much small-

³⁴ John Arquilla and David Ronfeldt (eds.), *Networks and Netwars* (Santa Monica: Rand Corporation, 2001).

³⁵ Barabasi, *op. cit.*

³⁶ The idea of super hubs is a graphic example of a critical node, but the notion itself has been around for a long time, although has not always been used with much precision. A useful discussion of critical nodes in networks can be found in Malcolm Sparrow “Network Vulnerabilities and Strategic Intelligence in Law Enforcement,” in *International Journal of Intelligence and Counter-intelligence*, Vol. 5, No. 3 (Fall, 1991), pp. 255-274.

er) and low in redundancy (there are few of them). Identifying both critical and sub-critical (high in importance but also high in redundancy) nodes is essential to understanding how the network operates as well as its strengths and vulnerabilities.

It is important to bear in mind, however, that critical nodes are not necessarily leadership nodes. Some critical nodes will have important substantive roles that are critical to the network's substantive mission (whether it be delivering drugs for profit or death and destruction for political reasons) while others will help to ensure that the network functions effectively as a network. A critical node in a terrorist network, for example, might be a bomb-maker with unique expertise in creating certain kinds of bombs; the counterpart in a drug trafficking network would be the chemist who provides the expertise for processing raw materials into psychotropic drugs. These are substantive roles. In terms of generic network roles a critical node might be a person who acts as communication hub, linking together members of the network who never talk to each other directly because of security concerns. In effect, this node acts as a critical facilitator in the network. While he would have to have earned a high level of trust from others in the network, he would not necessarily be part of the leadership.

This is not to deny the importance of the leaders who provide the core of the network, define its mission, and give it strategic direction. In this connection, it is obviously important to capture bin Lādin – if only to limit the growth of the bin Lādin myth and the aura of invincibility he has created. Yet his imprisonment or death will not have the impact many hope and expect: a network cannot be decapitated in the same way as a traditional hierarchy and the removal of bin Lādin, while a serious blow to morale, would not render al-Qa'ida and its affiliates incapable of operating. Indeed, one of the other crucial characteristics of networks is the ability to regenerate even after having suffered considerable damage or degradation.

While much of this is very obvious, for decision-makers and analysts who have traditionally focused on hierarchical bureaucratic adversaries it is hard to accept that the traditional model of top-down control is not applicable to many transnational threats. In some quarters, for example, there is still a tendency to see al-Qa'ida as the director of global *jihād* rather than as the inspiration for follow-on terrorist organizations dedicated to following the example it has set, but autonomous in determining how, when, and where this is best done. Thinking of adversaries in terms of monolithic decision-making and hierarchical command structures is a recipe for failure if not disaster. In a complex world it is better to think horizontal networks rather than hierarchies, and bottom up activities rather than top down commands.

The other point that initially seems self-evident, but is nevertheless worth emphasizing is that networks are distributed organizations. One of their great strengths is that they can cross boundaries and borders, and unlike traditional

centralized threats have no single center of gravity. They have a distributed territorial presence but, in the strict sense, are not territorially based. Consequently transnational networks can engage in terrorist or criminal activities in multiple places at once.

Unfortunately this simple observation gets obscured in the political debate over Iraq which all too easily inhibits clear thinking about networks. Supporters of the United States involvement in Iraq, for example, have contended that this has become the front-line of the war on terrorism and that it is better for the global *jihād* groups to be attacking United States forces in Iraq rather than initiating new attacks on the United States homeland. The problem with this, however, is that it fails to fully appreciate the notion of a dispersed threat, seeing terrorist attacks in terms of an either/or (either Iraq or the United States) rather than in terms of one and the other (Iraq and Madrid or Iraq and the United States). Dispersed networks can concentrate resources when necessary, but can simultaneously maintain some form of dispersal which provides insurance and gives them a capacity to attack elsewhere. Networks are capable of dispersed and discrete actions within an overall strategic objective.

A parallel can also be drawn between malevolent political and criminal networks and diseases that spread from one host or carrier to another. Indeed, when looking at epidemics it is clear that – as with nodes of a network – not all those who carry or spread the disease are created equal. In almost any epidemic such as SARS or AIDS what might be termed “super-spreaders” play an inordinate role. Perhaps the most famous super-spreader was an Irish cook in New York, Mary Mallon, more commonly known as “Typhoid Mary” who never suffered from typhoid herself but transmitted it to the families she cooked for. Mary was eventually kept in quarantine.

More recently during the SARS epidemic, several people were identified who had passed on the disease to a surprisingly large number of other individuals. There are several reasons why some people become “super-spreaders”: a lot of travel during a period in which the disease is particularly virulent and susceptible to transmission from person to person; symptoms such as coughs and sneezes which transmit the disease to people in close proximity (on a crowded sub-way train, for example); and, in the case of sexually transmitted diseases, a large number of sexual partners.

The transmission of ideas or pieces of information (sometimes called memes) in social networks operates in very similar way. It is central to the recruiting process, especially for terrorist networks. In this connection, two radical Islamic preachers in London, Abu Qatada and Abu Amzar have played a very important role in transmitting extremist ideas and encouraging Moslems to join al-Qa’ida and other terrorist organizations.

Criminal organizations also seek to extend their membership through recruitment, often seeking members from outside the dominant ethnic group as these

are less likely to be profiled by law enforcement. Nigerian drug trafficking organizations, for example, have sought to recruit middle-aged white women as couriers, sometimes attracting them with offers of money and sometimes using deception. Whatever the specifics of recruitment patterns, however, it is clear that criminal and terrorist organizations constantly adapt by seeking new ways of circumventing law enforcement and intelligence efforts. This is not very surprising and can, in fact, be understood as a characteristic feature of complex emergent organizations.

5. Complex Emergent and Adaptive Organizations

Another way of thinking about transnational threats in general and networks in particular is in terms of complex adaptive organizations. The implication is that when a network is attacked it will adapt to compensate for damage and still carry out its critical missions. A good example of high levels of adaptability can be seen in the behavior of Colombian drug trafficking networks in the early 1990s. These networks were, in effect, tall and thin, exhibiting a high level of vertical integration and concentrating power and authority in a relatively narrow association of drug traffickers in the cities of Medellin and Cali. After the key organizers in the network were either killed or imprisoned, the drug trafficking networks reconstituted themselves in a much flatter form.

No longer were the drug trafficking organizations vertically integrated and in control of the industry from leaf to nose; instead they morphed into a flatter or more horizontal network that focused largely on processing and transportation of the drugs out of Colombia where they were handed over either to Mexican organizations or to Dominican trafficking networks in the Caribbean. In effect, what was happening was coevolution between the drug trafficking organizations and their activities on the one side and United States law enforcement agencies and drug interdiction efforts on the other. The Medellin and Cali drug trafficking organizations were not only highly visible, but by managing the whole process of drug distribution to the United States they had elicited vigorous responses from United States law enforcement and intelligence agencies. The smaller horizontal organizations in contrast tried to avoid becoming a target of the United States government by contracting out the trafficking of drugs into the United States itself.

Something similar appears to be going on in the world of terrorism where al-Qa'ida has been seriously damaged by the United States "war on terrorism" but where other parts of what is now clearly a "network of networks" committed to global *jihad* have begun to take the lead in carrying out attacks against the United States and its allies. Not only is the next generation leadership emerging to replace those members of al-Qa'ida's core who have either been killed or captured, but other organizations such as the Salafists for Call and Combat which operates in Europe are becoming more active. Lashkar-e-Toiba, which operates

out of Pakistan, has members who have been active in countries as diverse as France and Australia, and is an organization that is moving from relative obscurity to the forefront of the global *jihād*.

Another – and closely related – characteristic of transnational threats is that they are constantly, adapting, evolving and mutating. This is true of bacterial infections that have become highly resistant to traditional antibiotics and of new viruses such as HIV-AIDS and, more recently, SARS. It is equally applicable to criminal and terrorist networks.

Illicit networks are adept at organizational learning and this enables them to continue to surprise governments as they can mutate into unfamiliar forms, adopt novel and unexpected methods of operation which differ significantly from anything they have done before, and generally confound those who seek to combat them. In fact, there is another component of complexity theory that is relevant to the capacity of emergent organizations to adapt and morph – the notion of fitness. Because of the coevolution of competing systems or organizations, the outcome of the competition will be determined largely by which one evolves most rapidly and effectively to the challenges posed by the other. Thinking in terms of the fitness landscape, the danger is that governments will compel terrorists to move to new fitness peaks in the landscape yet fail to move to higher peaks themselves.

A very good example of morphing behavior that complicates efforts to combat terrorism is the response of many Islamic charities to the actions of the United States and the international community designed to choke off the finances of terrorism. New regulations, the closing of some charities in the United States and in some Middle East countries, and the indictments of officials running some of these charities, have certainly made the diversion of funds to terrorism more difficult. The network of Islamic charities has also adapted in ways that make the tracking of their activities more problematic. Among the changes identified by Matthew Levitt, have been the following:

- Charities which have been closed down simply change their names and re-register under a new name.
- In some cases where the head office of a charity has been closed some of the branches of the charity still operate. Similarly, even though the offices of charities in some countries or even the head office might be regulated, other branches are not necessarily subject to the same kind of control and scrutiny. This should not be surprising: after all charities are network organizations
- Some charities have changed the nature of their support for terrorist organizations moving from logistical support to infrastructure support. In practice, this could mean that they provide fewer funds for terrorist operations but might provide employment for potential terrorists planning to carry out an attack.

- Because of the monitoring of institutional accounts by banks as well as governments, law enforcement and intelligence agencies, some charities are increasingly using personal accounts.
- Some charities are operating in new areas such as Cambodia and Iraq where they are less subject to oversight or investigation.
- Charities, like terrorist organizations themselves are also making greater use of non-sophisticated but trustworthy methods of transferring funds such as the use of couriers and movement of commodities such as gold and diamonds.³⁷

In effect what Levitt has identified in this analysis is a classic example of adaptive behavior or morphing. Similar shifts are likely in other areas of terrorist finances.

The clampdown on the transfer of terrorist-related funds through the banking system, for example, has led to greater use of hawala, greater use of trade-based methods of covert funds transfer such as over-invoicing and under-invoicing, and greater reliance on physical commodities such as diamonds and gold. In terms of the fitness landscape, the United States and international effort to combat terrorist finances has compelled the charities to move to a higher fitness peak, but it is not clear that the institutions in the forefront of the international effort to combat terrorist finances can do the same.

6. Implications

The implication of all this is that complexity theory is highly suggestive of some new ways of looking at the world. The notion of looking at systems as a whole rather than in terms of the parts suggests a global perspective, which translates quite nicely into the notion of a global borderless intelligence space. Ecologies of malevolence are also important as they not only help to give birth to and incubate transnational threats but subsequently provide support and safe havens. The notion of tipping points is one that highlights the need to take small changes and small problems very seriously; the small changes can have large consequences transforming small problems into major challenges. It is equally important to think in terms of networks, distributed rather than concentrated threats, and the capacity of networks to morph and achieve a better location in the fitness landscape as they coevolve with those combating them. Thinking in this way provides a powerful lens through which intelligence analysis can view transnational threats. The other issue, however, is the way in which they analyze these threats. And it is to this that attention must now be turned.

³⁷ For a more complete and very incisive analysis see Matthew Levitt, "Charitable Organizations and Terrorist Financing: A War on Terror Status-Check," Draft Paper Presented at the University of Pittsburgh Workshop on the Dimensions of Terrorist Financing, March 19-20, 2004.

Analyzing Transnational Threats

If complexity theory provides some illuminating ways to look at transnational threats, it is also relevant to the analysis of these threats. It suggests both a focus for analysis and methods of analysis that can – and should – be used by members of intelligence agencies tasked with working on transnational issues and threats.

Complexity theory not only underlines the need for an alternative competing hypotheses (ACH) methodology enunciated most explicitly by Richards Heuer, it suggests that we need to go even further in this direction.³⁸ Because of the unpredictability of outcomes in a complex environment, it is necessary to consider multiple possibilities or multiple alternative competing hypotheses (in effect, to go from ACH to MACH). While this can be a highly daunting task, it is appropriate to the realities of a complex world in which interdependencies can push forces and events in a variety of different and often unpredictable directions. Analyses which take into account the probability of unintended consequences, herd or imitative behavior, and cascading effects, and which incorporate these into their MACH are likely to develop a solid track record of anticipation. Those who ignore such phenomena or limit their ACH within narrow boundaries, however, are likely to be much more susceptible to surprise.

Another approach that has been identified for dealing with complexity is sense-making.³⁹

Enunciated by Fishbein and Treverton as a continuous, iterative, largely informal process through which organizations understand and interpret their environment, sense-making goes well beyond immediate analysis of possible outcomes. It is particularly appropriate for developing insights into “problems that must be grasped holistically,” understanding “situations that are intricate, shadowy or ill defined” and assessing threats that are distributed and constantly morphing.⁴⁰ Sense-making can also be understood as a long-term collaborative conversation in which analysts share insights and ideas in ways designed to highlight differences of perspective and approach. It is designed to encourage a culture of “mindfulness” in which analysts constantly re-examine and refine or reject the concepts, categorizations and implicit models they use to understand the world.⁴¹

³⁸ Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Washington DC.: GPO, 1999).

³⁹ Warren H. Fishbein and Gregory F. Treverton, *Making Sense of Transnational Threats*, Kent Center Occasional Paper, Vol. 3, No. 1, available on the CIA public website at www.cia.gov.

⁴⁰ Guy Claxton, *Hare Brain, Tortoise Mind: How Intelligence Increases When You Think Less*, (New York: Harper Collins, 2000), pp. 3-11, as quoted in *Ibid*.

⁴¹ This is emphasized in Karl Weick and Kathleen Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Uncertainty* (San Francisco: Jossey-Bass, 2001). For a fuller discussion see Fishbein and Treverton, *op. cit*.

Among the specific phenomena that transnational threat analysts need to be looking for and utilizing are tipping points and cascading effects. In attempting to forecast events and provide what Sherman Kent termed speculative evaluative intelligence⁴² it is important that analysts develop an understanding of the notion of tipping points and consider trends or developments with the assumption that small changes can have surprisingly large effects which happen very quickly. Approaching the future with an explicit model of tipping points in mind could well illuminate possible developments in ways that more traditional analysis would not.

Perturbations or instabilities in a system have a variety of knock on consequences. Sensitivity to cascades of change, for example, might have made intelligence analysts better able to predict the consequences of change in Eastern Europe for the Soviet Union itself. Such sensitivity would also have given analysts greater capacity to predict the Asian financial crisis and the contagion it caused. A model of contagion or cascading effects that is closely linked to notions of tipping points would also be of considerable help in not only explaining transnational threats but in attacking transnational entities. If terrorist cells are tightly coupled, for example, (and this seems to have been the case in Europe through 2001 to 2003 and up until the Madrid rail attacks) then taking down a cell in one country can provide information that leads to the destruction of cells elsewhere. One focus for analysis, therefore, might be interconnectedness which, in some cases and under some conditions, can be exploited as a major vulnerability of terrorist or criminal organizations.

In responding to network based threats, analysts also have to learn or develop several techniques. The most obvious is social network analysis – which is well known and well established. Concepts such as network distance, cliques, and network centrality can be identified mathematically within a network and help to explain the dynamics of the network as well as its strengths and vulnerabilities. Yet this needs to be extended into what might be termed strategic network analysis. After mapping the network as a whole (or as much of it as possible) and identifying the critical nodes it is important to try to remove one or more of these critical nodes and to assess how the network responds to such a loss.

One possible network response would be a simple substitution for the removed node, what might be termed a direct replacement strategy. An alternative would be a more distributed approach with the critical functions shared among several alternative nodes. In effect, this could be regarded as an indirect substitution strategy. A third approach would be for the network to function without the node or any replacements (direct or indirect) by developing compensatory mechanisms or work-around strategies. There might well be distinct forms of

⁴² Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1949).

compensation that are used by the network to respond to attack and minimize the extent of the resulting degradation.

The crucial point, however, is that network responses can only be discerned by placing the network under stress, closely observing its adaptive measures, and assessing these in strategic terms. Such an approach is fully consistent with Snowden's notion of probing the environment. It means that strategic network analysis has to be an iterative process closely related to efforts to probe the network and thereby obtain greater insights into the network's adaptive capacity and patterns of adaptation. It requires close coordination between analysts, operators and collectors. This again demands a somewhat novel approach given the conventional separation of these tasks and the personnel involved in them.

Probing and stressing transnational targets also allow analysts and operators to achieve a greater understanding of the target and its adaptation strategies. Understanding transnational adaptive dynamics is critical: as targets morph, the analysis needs to anticipate possible outcomes of the morphing process. Given the notion of coevolution discussed above, intelligence should also help to inform US initiatives about the possible results of US actions. It is not a case of a simple action-reaction effect; rather is it about the impact of our actions on the adversary's location, both short and long term, in the fitness landscape. Analysts need to work with a variant of an old adage: what does not destroy the adversary might simply make him stronger. Consequently, it is important to provide a more comprehensive analysis of possible impacts and consider which might be benign or positive and which might be negative. Such an approach might at least provide some insights about potential developments, outcomes, or even events which reflect unintended consequences.

In addition to these intelligence strategies, it is also desirable to identify opportunities and methods for transforming ecologies of malevolence into ecologies of benevolence. Of course, this is something that also needs to be done with great caution, precisely because of the unintended consequences, cascading effects and morphing possibilities discussed above. Notwithstanding the caution, however, efforts to modify the environment, even in small ways, could have large payoffs. Finding the forces or identifying the small changes that might tip an ecology of malevolence into an "ecology of benevolence" would be a major intelligence coup that could help to create a more stable security environment.⁴³

In sum, intelligence analysis for the world of transnational threats needs to be very different from the traditional approach. It has to (1) recognize complexity and variability of outcomes by using multiple alternative competing hypotheses; (2) make greater use of efforts to probe and manipulate transnational actors in order to achieve a greater understanding of their structure and behavior; (3) think in terms of emergent behavior rather than monolithic decision-making, hierar-

⁴³ I am grateful to Carol Dumaine for this observation.

chical command structures, and rational choice; (4) identify how network strengths can be undermined and network vulnerabilities exploited; (5) use tipping point analysis to increase understanding and to prepare for the unexpected; (6) focus on morphing and identify undesirable morphing possibilities that, if they cannot be avoided, at least need to be anticipated.

Essential to all of this is a willingness on the part of analysts constantly to develop and refine new concepts and categorizations, think in new ways and use new tools and techniques. With such a willingness and careful use of the perspectives and methods of analysis described above, it should be possible to develop more effective analysis for transnational threats. Nevertheless, there is another dimension that also needs to be added to the equation – organizational reform. This is particularly important because it is clear from the preceding analysis that intelligence for transnational threats can be understood in part as a competition in learning. And who wins this competition and comes out better located on the fitness landscape will do much to determine how successful or unsuccessful the United States proves to be in combating terrorism and other transnational threats.

New Intelligence Structures

Combating transnational threats requires not only new ways of thinking and new methods of analysis but also what Dee Hock, in a different context, termed “iconoclastic concepts and ideas” about organizations and institutions and their management.⁴⁴ There are several aspects of organizing for transnational threats that need to be emphasized. In terms of organizational structure it is necessary to mimic the threat: intelligence agencies need to move from center to edge organizations, place less emphasis on directors and more on connectors, develop transnational partnerships, emphasize sharing rather than secrecy, develop more effective red team analysis through rule free thinking and simulations, and become more adept at early warning based on environmental scanning and a deeper, more profound understanding of the threat. In addition, transnational intelligence organizations need to develop effective methods of organizational learning. After all, this is the key to location in the fitness landscape.

Facing threats operating in a global borderless intelligence space, it is essential to cultivate a transnational intelligence community (TIC) to provide more comprehensive coverage and better analysis. The TIC can best be understood as a dynamic pulsating ad hoc network that shifts from issue to issue and that includes trusted (but uncleared) actors including NGOs and academics. It also shifts the emphasis from secret intelligence to the development of adjacent communities engaged in transnational, non-secret but controlled intelligence collab-

⁴⁴ Dee Hock, *Birth of the Chaordic Age* (San Francisco: Berrett-Koehler, 1999), p.48.

oration aimed at sense-making, pattern and anomaly detection, and early warning through the assembly, collation, and analysis of disparate pieces of information from the public domain.⁴⁵

Such a community, however, cannot be composed of traditional centralized, hierarchical institutions. Developing institutions which can collaborate effectively and generate high-quality intelligence in a complex world cannot simply be done with more of the same. Not only do such institutions require innovative thinking, but they also require adoption of some of the enemy's methods of operating and ways of thinking. John Arquilla and David Ronfeldt summarized this idea very succinctly in the notion that it takes a network to defeat a network.

Yet the issue is not simply about networks; it is about understanding the enemy and where it is useful being willing to imitate the enemy's characteristics. There is an interesting parallel to this in what is called bio-mimicry which has been described as "a new science that studies nature's models and then imitates or takes inspiration from these designs and processes to solve human problems e.g., a solar cell inspired by a leaf."⁴⁶ The idea of the adversary as a model or even mentor is not an easy one to accept; yet if one is concerned about competition in the fitness landscape it no longer seems quite so outlandish.

With this in mind, it is necessary to create edge organizations that are responsive to dimensions of complexity and the nuances of the targets. This requires "moving power to the edge" i.e. "changing the way individuals, organizations, and systems relate to one another and work. Power to the edge involves the empowerment of individuals at the edge of an organization (where the organization interacts with its operating environment to have an impact or effect on that environment) or, in the case of systems, edge devices. Empowerment involves expanding access to information and the elimination of unnecessary constraints."⁴⁷

As Alberts and Hayes have noted, the topology of an edge organization is very different from that of the traditional centralized hierarchical model – a model that still dominates most of the military and intelligence agencies. Edge organizations have "greatly enhanced peer-to-peer interactions" and reduced the role of those "whose role is to manage constraints and control measures."⁴⁸ By removing stovepipes and other barriers to information sharing, edge organizations become highly inclusive collaborative organizations with "the attributes to be agile. This is because agility requires that available information is combined in new ways, that a variety of perspectives are brought to bear, and that assets can be employed differently to meet the needs of a variety of situations. ... edge

⁴⁵ The formulation here owes a great deal to Carol Dumaine.

⁴⁶ Janine M. Benyus, *Biomimicry: Innovation Inspired by Nature* (New York: Morrow, 1997), foreword.

⁴⁷ David S. Alberts and Richard E. Hayes, *Power to the Edge: Command... Control in the Information Age* (Washington DC.: CCRP, 2003), p.5.

⁴⁸ *Ibid.*, p.5.

organizations ... are particularly well suited to deal with uncertainty and unfamiliarity because they make more of their relevant knowledge, experience, and expertise available.”⁴⁹

Because edge organizations are robust at the periphery they can reach out to other very similar organizations, creating what could be understood as a “chaordic” structure that mixes chaos and order.⁵⁰ The order would be provided by a series of protocols across the community permitting sharing of analytic methods, threat assessments and warnings. The chaos would come with dynamic approaches to collaboration, loose and unstructured forms of leadership providing inspiration rather than control, generative models of organizational learning and change, and global variable geometry relationships – coalitions, communities, and partnerships – that could be mobilized and energized as necessary.

A chaordic structure of this kind provides the basis for what could be described as a surge analytic capability. In the event of the emergence of a new disease, for example, the capacity to share information and ideas rapidly and easily, to identify and quarantine super-spreaders, and to develop other containment methods, could significantly augment the response of the international community. Once again, the transnational intelligence community would be most effective when it evolves in the same way as the threat itself.

Although the United States has a long tradition of intelligence-sharing and intelligence cooperation with selected partners such as the United Kingdom, in the new threat environment, expanded cooperation which goes beyond traditional partners to include new collaborators is essential. Not only can foreign partners provide greater access to key areas of the world, but they can help to identify and monitor the multiple geographic watch points which are an essential component of the response to transnational threats in the global borderless intelligence space. Such cooperation can start off rather modestly with information or analytic exchanges and if successful these can provide a basis for incrementally extending cooperation.

In thinking about the evolution of a transnational intelligence community, however, it is not simply other governments which need to be included. With the revolution in the availability of information, and the kind of work that is being done in some parts of academia and by NGOs which monitor particular kinds of activities (some of which are directly or indirectly relevant to transnational organized crime, terrorism and disease) the idea of extending the intelligence community to incorporate these novel but highly relevant players is compelling. Not only can these new participants provide new perspectives and sources of information and help to fill gaps in “sense-making” but they can also facilitate the cross-fertilization of methods.

⁴⁹ Ibid., p.217.

⁵⁰ See Hock, for more on this theme.

Moreover, multinational and transnational analysis that goes beyond governments provides far greater opportunities for challenging ethnocentrism and cultural biases as well as for developing the multiple alternative competing hypotheses discussed above and for sense-making. By providing broader perspectives and alternative filters, this extended transnational intelligence community can facilitate the development of more analytic tipping points not only in pattern detection (known patterns) and pattern discovery (new patterns) but also in anomaly detection.

There are, of course, serious obstacles to the development of such a community. The desire to maintain high levels of secrecy, concerns over sources and methods, a lack of trust in relation to certain governments and to non-traditional intelligence actors, divergent interests, parochialism, skepticism that what others might know would provide value-added, along with simple resistance to change, all inhibit the kind of adaptive behavior necessary for the emergence of such a community.

If the issue of clandestine sources and information is put on one side, however, and if there is broad acknowledgement that transnational problems are as much about mysteries as secrets (although discovering secrets can be particularly critical in providing warning information) then it is clear that multiple inputs of information and analysis can be highly advantageous.

Moreover, the evolution of a transnational intelligence community cannot take place overnight, nor can it be forced. This is not an area in which it is possible to impose an artificial order. Exploratory contacts, if they provide mutually beneficial will be sustained and developed incrementally, resulting in what might be described as a mix of epistemic and virtual communities exploiting shared working spaces in cyber-space.

If such ideas seem far-fetched, there is a myriad of examples (albeit with similar bodies linked together) of transnational collaboration ranging from the World Health Organization and Interpol to the Financial Intelligence Units which make up the Egmont Group and share information in regular face to face meetings and through a secure intranet.

As well as building on these precedents and experiences – both good and bad – the transnational intelligence community also needs to be effective at learning. Fortunately, both the transnational nature of the community and the edge organizations which make up this community would facilitate this. The notion of community is itself central to learning and “communities of practice” have been described as both “the embodiment of learning and the context for the exercise of competence.”⁵¹ Consequently, a transnational intelligence community would stand a far better chance of competing with transnational threat networks in the fitness landscape of complexity.

⁵¹ See Ken Starkey, Sue Tempest and Alan McKinlay, *How Organizations Learn* (London: Thompson, 2004), p.135.

Conclusion

None of this is intended to suggest that complexity theory, network strategic analysis, or edge organizations provide silver bullets for the intelligence community. But the analysis does suggest that radical changes need to be made. The structure and thinking of the intelligence community in the United States still owe much to the Cold War, which provided both the rationale, the focus of attention, and the framework for analysis for over forty years. Many of the assumptions, practices, and methods that defined the intelligence task during the Cold War are still dominant. Consequently, change has to take place not only in the areas identified in this analysis but also in areas such as recruitment, training and human resource management.

The more fundamental changes, however, are intellectual and analytic, and for these to be successful parallel changes in organizational structures are also required. This is reflected in Table 1 which, in effect, provides a cryptic but, it is hoped, useful summary of the notion and components of complexity, the ways of thinking they generate, the methods of analysis they require, and the organizational changes that need to accompany the shifts in thinking and analysis.

Table 1

Complexity Component	Way of Thinking	Method of Analysis	Organizational Structure
Holistic Macroscopic level	Global Borderless Intelligence Space	System level analysis	Transnational Intelligence Community
Context as starting point	Ecologies of Malevolence	Multiple Alternative Competing Hypotheses Search for opportunities to create ecologies of benevolence	Edge organizations including NGOs and academics
Phase changes Tipping points	Small changes have big effects	Strategic Epidemiology and Contagion Models	Transnational multiple perspectives
Emergent behavior Adaptability Organizational learning	Bottom up not top down perspectives	Identify morphing behavior, dimensions and directions	Explicit learning organizations

Coevolution	Think interdependence with adversary	Look for unexpected consequences of own actions	Edge organizations closer to the coevolution process
Interconnectedness	Networks	Social Network Analysis and Strategic Network Analysis	Networked transnational intelligence personnel
Fitness Landscape	Competition in learning	Look for undesirable morphing	Flexible and adaptive “communities of practice”

Implementing the changes that are required at any of the levels identified will not be easy. Complexity theory is itself an emergent science in which new discoveries and course corrections are constantly being made. Moreover, complexity theory is not a complete answer to the problems of intelligence analysis for transnational threats. Yet, some of its components are very suggestive of the kinds of thinking, analysis and organization that might be more relevant than those currently prevailing. Merely thinking about the world in terms of complexity, the avoidance of chaos and the imposition of order where chaos is inescapable, offers new insights and ideas. Both the insights and ideas will need refinement while the repertoire of tools and methods for analysis will need to be expanded enormously.

Coping with complexity will not be an easy task for intelligence analysts; but unless they realize that this is the essence of the task they face, the prospects for improving either the analysis itself or the products that it yields remain low. Intelligence managers and politicians can facilitate the process by moving to create edge organizations, rewarding innovative thinking, and creating effective learning organizations.

To expect intelligence managers to do this all at once in an environment that is generally enormously timid and risk averse is wishful thinking. Nevertheless, the development of pockets of innovative thinking might be feasible along with the creation of edge sub-organizations that can engage in collaborative learning. Once these new units are created competitive tasking would allow management to compare the capacity of traditional analytic units, with the innovative edge-based network organizations in understanding and where possible anticipating transnational threats. Such a competition is highly likely to provide proof of concept and if it does, it could act as the basis for transforming the intelligence community in the United States into a complex adaptive learning organization capable of understanding the global borderless intelligence space and effectively analyzing and anticipating transnational threats to global and United States security.

Historical Attention Span Deficit Disorder: Why Intelligence Analysis Needs To Look Back Before Looking Forward

*Christopher Andrew**

Twenty-nine years ago, as the Khmer Rouge entered Phnom Penh, Pol Pot announced the beginning of Year Zero, insisting that Cambodia must disown its past and start again from scratch. There are nowadays some eminent voices in the United States who appear to tell us that Intelligence too must declare its Year Zero. To quote Brent Scowcroft:

This is a very new world, to which none of the structures or habits of thought established within the intelligence agencies are geared.

Mr. Scowcroft does not say simply that *some* changes are needed but that *all* existing intelligence structures and habits of thought are out of date. Though he has a remarkably distinguished record and is an improbable candidate for a US Pol Pot, his message for the future pays too little attention to the past.

Historically, many of those who prophesy the future have tended to fall into one of two categories, both of them mistaken:

- 1) Those who say we've seen it all before – that there's nothing new under the sun.
- 2) Those who say the world is entirely new and we have to start completely afresh.

Today's false prophets fall far more into the second category than the first. Most have been seduced by short-termism, the distinguishing intellectual vice of the late 20th and early 21st century. For the first time in recorded history, there is nowadays a widespread conviction that the experience of all previous generations save our own is irrelevant to present and future policy and intelligence analysis. Our political culture is dominated by an unprecedented malady: Historical Attention Span Deficit Disorder or HASDD (the only medical term and the only acronym I have ever invented).

* Prof. Christopher Andrew is Professor of Modern and Contemporary History at the University of Cambridge.

Disrespect for the long-term past produces two serious intellectual disorders.

First, the delusion that what is newest is necessarily most advanced – not a proposition which anyone with even an outline knowledge of the thousand years which followed the fall of the Roman Empire would take seriously. It took about fifteen hundred years before Western plumbing and bathrooms, for example, got back to the standards set by the Romans.

There are significant ways in which early 21st century intelligence agencies can still learn from the experience of the Second World War. Forgive me if I take the British example. British intelligence had a good war record—indeed the best war record any intelligence agency had ever had. As is now well known, its SIGINT successes enabled it to learn more of the enemy's secrets than any power had ever known in any previous war thanks to codebreakers who also invented the world's first electronic computer. British HUMINT successes led not merely to the rapid capture of every single German spy but also to the establishment of the Double Cross system, the largest scale and most successful deception in the history of warfare.

British Intelligence achieved these successes in large part because it employed innovative recruitment techniques which are still relevant in the twenty-first century.

Two techniques in particular:

The first was to recruit, along with more senior people, the youngest people ever recruited to executive positions by any government agency anywhere in the world, thus producing an extraordinary mix of youth and experience which has probably not been bettered since. On the eve of and during the Second World War, Bletchley Park, Britain's wartime SIGINT centre, sent recruiting teams to Cambridge and a handful of other British universities to recruit the brightest students they could find, irrespective of the subject they were reading, then gave them the chance to outshine the Faculty members they recruited at the same time. And some of them did. Among them was the twenty-year-old Harry Hinsley, who had just finished his second year reading history at Cambridge when he was recruited at the outbreak of war. Though Hinsley never finished his BA or any other degree, that did not prevent him after the war, as Sir Harry Hinsley, going on to become Vice-Chancellor of Cambridge University and a great deal more. At the age of only 24 it was Hinsley and not any of the more senior intelligence officers who was chosen to negotiate in 1943 the BRUSA SIGINT agreement between Britain and the United States, the most important international intelligence accord which had ever been concluded and which, in a modified form, is still at the heart of today's British-American intelligence alliance.

As a number of leading 21st century intelligence agencies become increasingly youthful, the Second World War precedent of combining youth with experience becomes increasingly relevant. The CIA Directorate of Intelligence is younger now than ever before in its history. Over 60 per cent of the British Se-

curity Service, MI5, are in their 20s and 30s, and the Service continues to become younger. Intelligence studies too are an unusually youthful field of research. Following the neglect of the intelligence dimension of international relations by many 20th century academics, graduate students are now producing as much innovative research as established academics on a range of intelligence-related topics from suicide bombers¹ to differences between American and British intelligence analysis.²

The second innovative recruitment technique employed by British intelligence during the Second World War was the welcome it gave to eccentrics. Though Alan Turing was probably the best code-breaker of the War, I wonder how many of the intelligence agencies represented at this conference would recruit him nowadays. He cycled to Bletchley Park wearing his gas-mask, which he thought might protect him against colds and flu, then chained his coffee mug to a radiator to prevent his colleagues stealing it. These were not the actions of the kind of team-players most intelligence agencies are anxious to recruit nowadays. Nor was Turing's decision during his first weekend at Bletchley to bury his life savings, which he'd converted into silver ingots, in the local woods. During weekends after the Second World War – and this is well attested – Turing was a tragic figure as he wandered round the Bletchley woods trying to remember where he'd buried the ingots.

Intelligence agencies nowadays need more Turings. The idea that we *all* need to be team-players is simply an ephemeral late-20th century fashion which it's time to return to what Trotsky called the dustbin of history. Though the majority of us should certainly operate as a team, we also need a minority of free spirits and original thinkers who are deeply unhappy with conventional wisdom and bureaucratic consensus. If I were in charge of intelligence recruitment, which is most unlikely, I would arrange presentations by some of the best intelligence analysts, then recruit those applicants who most successfully picked holes in their presentations.

Intelligence recruitment at its best was so innovative in the Second World War not because it *rejected* past experience but because it *learned* from it. Cambridge and Oxford recruits to Bletchley felt that the atmosphere there was quite similar to the one which had taken several centuries to emerge at Oxbridge – one in which Faculty members enjoyed the stimulation and challenge of bright students and respected the originality of eccentrics. Tradition and innovation are

¹ Kim Cragin, who is preparing a PhD thesis on Hamas at Cambridge University, is also co-author with Bruce Hoffman of the important forthcoming RAND study on suicide bombers.

² Among the postgraduate members of the Cambridge University Intelligence Seminar who have carried out important comparative studies on British and American intelligence analysis are Matt Perl and Keri Steffes. Though I am best acquainted with recent graduate research on intelligence at Cambridge University and have therefore chosen Cambridge examples, intelligence is also an increasingly thriving field of research at a number of other British universities.

not, as is often supposed, contradictory but complementary. When Cambridge is at its best, which is by no means all of the time, it combines one of the oldest traditions of academic independence anywhere in the world with one of Europe's largest concentrations of innovative high-tech businesses.

The second delusion produced by Historical Attention Span Deficit Disorder is the belief that interpreting the present and forecasting the future require an understanding only of the recent past. Little of real importance about future trends, however, can be deduced from the study of a mere generation of human experience. As my Cambridge colleague, Quentin Skinner, argues, only long-term historical perspective can “liberate us from the parochialism of our own forms of cultural analysis” – the kind of intellectual parochialism which has, for example, led to the common belief that globalisation is an off-shoot of late 20th century American capitalism rather than the product of a long and complex interaction between the West and other cultures. For intelligence analysts, the most effective antidote to Historical Attention Span Deficit Disorder is to follow Winston Churchill's celebrated (though nowadays neglected) advice: “The further backwards you look, the further forward you can see.”

Failure to heed the lessons of long-term past experience has done at least as much damage to intelligence analysis as the failure to realise how much the world has changed. Those who showed the most understanding of the threat of transnational terrorism before 9/11 were those who took Churchill's advice. Those who got it most wrong were those who ignored it. That is not simply being wise after the event but an argument which I put for some years before 9/11.

In my paper to the February 2001 Priverno conference, which paved the way for this year's conference in Rome, I argued that:

- The nature of the current terrorist threat has been widely misunderstood because it has been seen in too short-term a perspective. For the past generation the conventional wisdom has been that the terrorist's prime objective is publicity rather than victims, to terrify rather than to kill....This [late twentieth-century variety of terrorism, however,] is simply a short-term deviation from a much more dangerous longer-term terrorist tradition which is now reasserting itself.
- As Bruce Hoffman has argued, historically most terrorism has been far more concerned to kill than terrify. Until the nineteenth century terrorism was essentially Holy Terror...
- Over the last 20 years there has been a resurgence of traditional religious and cult-based terrorism, whose aims are epitomised by words of the former Hezbollah leader, Husayn Maṣāwī: “We are not fighting so the enemy will *offer* us something. We are fighting to *wipe out* the enemy.” That was the ideology of the religious wars in early modern Europe. That is also the ideology of, among others, Usama bin Lādin... If... bin Lādin... possessed WMD [weapons of mass destruction], [he] would probably already have used them. Indeed bin Lādin declared in 1998 that acquiring WMD is a “religious duty.”

In the quarter-century before 9/11 much academic research actually lessened our understanding of terrorism by extrapolating from short-term late-20th century trends, as embodied, for example, by the IRA, rather than the long-term threat posed by holy terror and other fanatical ideologically based terrorism which seeks to destroy its enemies rather than bomb them to the negotiating table. During that quarter-century, for example, only three issues of the generally excellent *Journal of Strategic Studies*, the premier British journal in the field, included articles on terrorism, presumably because it did not regard transnational terrorism as a problem of major strategic significance. Even more remarkably, during the decade before 9/11, *International Security* contained no article on terrorism at all.³

Much of the recent surprise caused at the extent of the problems of re-establishing peace and security in post-war Iraq similarly derive from lack of attention to the long-term historical perspective. The British general who occupied Baghdad in 1917 proclaimed, "Our armies do not come into your cities and lands as conquerors or enemies but as liberators." The Iraqis, however, were not easily persuaded. The announcement in 1920 that Iraq was to be a League of Nations 'mandate' under British trusteeship produced a widespread revolt which by the end of the year had caused 2,000 British casualties and angry complaints in parliament at the cost of the operation. "I am willing to bet," writes Niall Ferguson, "that not one senior commander in Iraq today knows the slightest thing about these events."⁴ Though a knowledge of the experience of 1920 does not, of course, provide easy answers to the problems of 2004, it would doubtless have helped to prevent premature claims of 'mission accomplished' after the rout of Saddam Hussein's forces in April 2003 and have given a better sense of the formidable problems which still remained.

Recovering a sense of long-term perspective, looking a long way back before attempting to look forward, is so contrary to the current spirit of the age that it is bound to be a difficult enterprise. But we already have both a starting point for the enterprise and several proven, though neglected, methodologies.

The starting point was indicated in the "State of Analysis" speech on 11 February 2004 in the CIA auditorium by the DDI, Jami Miscik, which is available on the CIA website. Ms. Miscik posed the question, "What are our analytic strengths and weaknesses?" That is a question, she says, which is "central to our mission" and requires "a serious and immediate dialogue." Unless we begin by identifying our strengths and weaknesses, we cannot possibly raise our game. But Ms. Miscik's question can only be satisfactorily answered by "a serious ex-

³ I owe these examples to Amelia Walker, who is currently preparing a Cambridge MPhil dissertation on academic analysis of terrorism in the generation before 9/11.

⁴ Niall Ferguson, "Forget Vietnam, Remember 1920," *National Post* [Canada], 12 April 2004. See also Ferguson's 2003 article in *Foreign Affairs*.

amination of experience which goes well beyond the immediate past.” “When we make mistakes,” she says, “we need to learn from them collectively as a Directorate.”

The 21st century, however, is simply too short a period within which to identify most of the intelligence mistakes and lessons which really matter.

Four proven methodologies already exist for learning from longer-term intelligence experience. All complement each other and all offer ways of answering the question posed by Ms. Miscik.

1. *The “Lessons Learned” Approach*

The first is what is known in the United States as the “lessons learned” approach – which derives from the after-action reports following military operations which seek to identify what went right, what went wrong and why. What Americans call “lessons learned” are known in Britain as “lessons identified” – in the, to my mind, correct belief that lessons identified are sometimes ignored rather than embodied in future practice. So far as I’m aware, the most sophisticated and promising “lessons learned” or “identified” programme is that recently developed by the CIA’s Center for the Study of Intelligence (CSI), which brings together the Center’s historians with analysts, operations and other intelligence officers to analyse past as well as recent operations.

One of the lessons that can, I think, be learned from the past history of the CIA is that, though the Agency has had some excellent historians over the past half-century, insufficient use has been made of their talents. One of those historians, Gerald Haines, concluded in 1997: “Most CIA officers and decision-makers, although they use historical analogies every day, are basically ahistorical. They believe they have no time or need for history.”

In the spring of 2004 the National Commission on Terrorist Attacks upon the United States identified as one of the weaknesses of the US intelligence community before 9/11 the lack of a “lessons learned” programme of the kind now run by the CSI:

... The Community had not institutionalized a process for learning from its successes and failures. We did not find any after-action reviews sponsored by the Intelligence Community after surprise terrorist attacks such as the Embassy bombings of August 1998 or the *U.S.S. Cole* attack of October 2000. The Community participated in Inspector General inquiries conducted by individual agencies, but these reviews were perceived as fault-finding, without enough constructive emphasis on learning lessons and discovering best practices. What we did not find was anything between the extremes of no investigation at all, and an adversarial inquiry triggered by a public outcry.⁵

⁵ National Commission on Terrorist Attacks upon the United States, “The Performance of the Intelligence Community,” Staff Statement No.11 [Spring 2004], p.12.

2. Official Histories of Intelligence

The limitation of the case-study approach is its tendency to miss long-term trends. For that reason it needs to be complemented by full-scale histories which analyse all stages of the intelligence cycle. Over the last quarter-century the development of intelligence history, in particular the increasing emphasis on the relationship between intelligence and policy, has transformed the once narrow agenda of in-house histories of intelligence agencies, most of which appear to have resembled regimental histories concerned with the minutiae of operations and organisation. At this point I need to declare an interest as the official historian of the British Security Service, MI5. Though unofficial historians will continue to have a major role to play, the nature of the intelligence archive will always make it impossible for any but official historians to have full access to sources and methods.

The ability to learn from historical experience, like the success of security services, is best measured by the things that don't happen – the mistakes that aren't repeated in the case of historical experience, the terrorist attacks and the security breaches that don't happen in the case of security services. Though calculation within this counterfactual world is obviously very difficult, the evidence of the way in which the official and unofficial histories of the First World War improved British performance in the Second World War is, I think, persuasive.

The least noticed thing about the British war effort in World War II are the dogs which don't bark – the First World War mistakes which weren't repeated. Very few of the bitter clashes between “frocks” and “brass hats,” civilian officials and service chiefs, which had bedevilled Lloyd George's government in the First World War reappeared in Churchill's during the Second. Inter-service rivalry, too, was significantly lower in Britain than in the United States or any other of the major combatants.

One consequence of the low level of civil-military and inter-service rivalry in World War II was that it was possible to establish and make effective the Joint Intelligence Committee which brought together the heads of all the service intelligence departments and the civilian intelligence agencies with their main consumers under a Foreign Office chairman – the most advanced intelligence assessment system in the world.

Churchill was both the best and the most prolific historian ever to become Prime Minister. And it was Churchill's sense of history and awareness of the failures of intelligence coordination in World War I which helped to ensure both that the British intelligence community in World War II was better coordinated than any intelligence community had ever been before and that intelligence was better used than in any previous war.

Official histories of intelligence should, in my personal view, fulfil three criteria:

(i) *They should be based on full access to the files.* Though the need to protect sources and methods necessarily limits what can be published, the conclusions of official histories must be based on access to all relevant evidence.

(ii) *Official historians must have complete freedom to reach whatever conclusions they believe are consistent with the evidence.* That principle goes back to the very origins of British official histories and I'm fortunate to benefit from it. My own contract contains a guarantee that none of the judgements I arrive at can be changed in the published history.

As Jami Miscik said at the beginning of her "State of Analysis" speech, it is even more important for intelligence analysts to exercise independent judgement than to be right. The same applies to official historians. Ms. Miscik said this:

First and foremost, you need to know that our integrity has held firm. There has been a lot of talk about whether we were pressured to shade our analysis...If there is pressure, do we cave? No, we do not; and those who know us, know we did not...There is nothing more fundamental or important than our mandate to "call it as we see it"... It may surprise some of you to hear me say that. Many of you might have thought I would have said, "being right" is the most important thing.

The best definition I ever heard a British intelligence chief give of his role is very similar. "My job," he said, "was to tell the Prime Minister what the Prime Minister did not want to know." Just as intelligence chiefs have to be able to tell policymakers what they do not want to know, so "lessons learned" programmes and official histories have to be free, on occasion, to tell intelligence agencies uncomfortable truths.

(iii) *The third principle is that official histories of intelligence should not be simply internal histories but deal with the whole of the intelligence cycle, including the interaction with policymakers.*

For 21st century intelligence to improve on that of the 20th century, intelligence consumers as well as intelligence agencies will have to raise their game. On present evidence, for example, it seems likely that the weakest link in the 20th century American intelligence process was not collection or analysis but the use made of intelligence by policymakers. The first of the measures proposed in 1996 by the Aspin-Brown Commission to improve "the performance of U.S intelligence" was directed at policymakers rather than the intelligence agencies:

Intelligence needs better direction from the policy level, regarding both the roles they perform and what they collect and analyze. Policymakers need to appreciate to a greater extent what intelligence can offer them and be more involved in how intelligence capabilities are used.

⁶ Christopher Andrew, *For The President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (London/New York: HarperCollins, 1995).

As I've tried to show in *For The President's Eyes Only*, most presidents have not been very good either at managing the intelligence community or at understanding what it can – and cannot – do for them.⁶

The CIA Center for the Study of Intelligence has made an innovative beginning in this important area of research. In 1996 the former DDI, John Helgerson, produced a pioneering study of the CIA's early briefings of incoming Presidents from Truman to Clinton, based both on unrestricted access to CIA files and on interviews with surviving Presidents and their briefers. I wrote in a foreword to the unclassified version of Helgerson's study:

Until similar volumes are available on the briefing of, among others, British prime ministers, German chancellors, French and Russian presidents, and leading Asian statesmen, the use made of intelligence by world leaders will continue to be a major gap in our understanding of both modern government and international relations.

That major gap still remains. Basic questions about the attitude of most twentieth-century world leaders to intelligence have yet to be asked, let alone answered. It is high time they were. We cannot learn the lessons of experience until we know what that experience consists of.

3. *Retrospective Analysis of Our Assessment of the Opposition*

The third methodology necessary to identify our long-term strengths and weaknesses is the retrospective analysis of our assessment of the opposition. We cannot possibly assess our performance against the KGB during the Cold War, for example, without comparing what we know now about the KGB with what we said at the time. The same, more recently, applies to Saddam Hussein's Iraq. So, very briefly, I want to give some indication of what I think we can learn from those two examples.

(i) *The KGB*. Thanks to Vasili Mitrokhin and Oleg Gordievsky, I've been fortunate to have privileged access to some of the still classified contents of the KGB archives, as well to material which has been officially released.⁷ A comparison of that material with US and British intelligence assessments of the Soviet Union seems to me to reveal a recurrent failure to grasp the frequently huge gulf between Soviet intelligence collection and Soviet intelligence assessment.

⁷ Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev* (London: Hodder & Stoughton; New York: Harper & Row, 1990). Christopher Andrew and Oleg Gordievsky, *Instructions from The Centre: Top Secret Files on KGB Foreign Operations, 1975-1985* (London: Hodder & Stoughton, 1991); published in USA as *Comrade Kryuchkov's Instructions* (Stanford U.P., 1993). Christopher Andrew and Oleg Gordievsky, *More Instructions from The Centre: Top Secret Files on KGB Global Operations 1975-1985* (London/USA: Frank Cass, 1992). Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive, Vol.1: The KGB in Europe and the West* (London/New York: Penguin/Basic Books, 1999).

That failure was due first and foremost to a failure to situate Soviet intelligence assessment within its long-term context. The previous history of all authoritarian regimes should have been sufficient to demonstrate that Soviet political intelligence assessment was bound to be bad. Intelligence agencies in authoritarian regimes, especially those in one-party states, invariably tell their rulers what they want to hear. In the Soviet Union, as in Saddam Hussein's Iraq, they thus act as a mechanism for reinforcing the regime's misconceptions of the outside world.

Though the Soviet leadership never really understood the West until the closing years of the Cold War, it would have been outraged to have its misunderstandings challenged by intelligence reports. As one Line PR (political intelligence officer) later admitted, "In order to please our superiors we sent in biased information, acting on the principle 'Blame everything on the Americans, and everything will be OK.'" Even on the eve of the Gorbachev era, KGB assessments of the world situation continued to emphasise the supposedly insoluble international contradictions which beset Western capitalism, but tactfully refrained from mentioning the far more serious problems of the Soviet economy. In 1984 the KGB foreign intelligence chief, Vladimir Kryuchkov (later KGB Chairman), reported that "deepening economic and social crisis" was leading Western imperialists to consider war against the Soviet Union as a possible way out of their insoluble problems.

The best evidence I know of that Mikhail Gorbachev really was engaged in "new thinking" about foreign policy from the moment he became Soviet leader in March 1985 was his early denunciation of the political correctness of KGB reporting. In December 1985 the KGB Chairman, Viktor Chebrikov, was forced to summon a meeting of the KGB leadership to discuss an unprecedented memorandum from Gorbachev "on the impermissibility of distortions of the factual state of affairs in messages and informational reports to the Central Committee of the CPSU and other ruling bodies." The meeting sycophantically agreed on the need to avoid sycophantic reporting and declared the duty of all KGB officers both at home and abroad to "fulfil the Leninist requirement that we need only the whole truth."

The damaging effects of political correctness were made worse by the KGB's recurrent tendency to conspiracy theory, which in times of crisis escalated into a paranoid tendency. Looking back on the Cold War, Sir Percy Cradock, former Chairman of the British Joint Intelligence Committee and Margaret Thatcher's Foreign Policy Advisor, is surely right to identify "the main source of weakness" in the Soviet intelligence system as "the attempt to force an excellent supply of information from the multifaceted West into an oversimplified framework of hostility and conspiracy theory."⁸

⁸ Sir Percy Cradock, *Know Your Enemy: How the Joint Intelligence Committee Saw the World* (London: John Murray, 2002), ch.17.

We now know from documents in the KGB archives that on at least two occasions, in the early 1960s and the early 1980s, the KGB reported to the Politburo – with horrendous inaccuracy – that the United States was planning a nuclear first strike against the Soviet Union. On 29 June 1960 the KGB Chairman, Aleksandr Shelepin, hand-delivered to Khrushchev an alarmist and wholly unfounded report that “the Pentagon is convinced of the need to initiate [nuclear] war with the Soviet Union ‘as soon as possible’.” In March 1962 the GRU claimed that in September 1961 the United States had actually taken the decision to launch a nuclear first-strike but had been deterred at the last moment by Soviet nuclear tests which indicated a greater capacity to retaliate than had been expected.

Had CIA analysts in the early 1980s been aware of the terrifyingly mistaken KGB and GRU assessments of twenty years earlier, they would doubtless have been quicker to credit the intelligence which convinced their British colleagues that both the KGB and GRU were engaged in a vast intelligence operation designed to detect the non-existent plans of the Reagan administration for a nuclear first strike against the Soviet Union. But the analysts’ fundamental difficulty was, I think, in grasping that intelligence analysts and policymakers in Moscow were capable of crediting such an improbable conspiracy theory. A longer-term understanding of the mind-sets of authoritarian regimes would have made that possibility seem far less surprising.

(ii) *Saddam Hussein’s Iraq*. The remarkable amount of material from Iraqi intelligence files which has become publicly available since the Gulf War at the beginning of the 1990s has attracted surprisingly little attention. The several million Iraqi intelligence documents captured in 1991, chiefly by the Kurds, despite their limited operational usefulness once the war was over, were – or should have been – of central importance in understanding the mindset of the Saddam Hussein regime. Like the documents captured after the 2003 Iraq War, they provide – as in the case of the KGB archives – an opportunity to identify the strengths and weaknesses of Western intelligence assessment. Both sets of documents provide vivid evidence of the way in which, once again, the intelligence services of a one-party state acted as a mechanism for reinforcing the regime’s misconceptions of the outside world. Ibrahim al-Marashi, who has made a detailed study of many thousands of the Iraqi intelligence documents captured in 1991, has found a level of sycophancy towards the political leadership reminiscent of the Soviet era. The documents also go into extraordinary detail about Iraq weaponry. One file, for example, on an Iraqi soldier who deserted to Saudi Arabia even records the number of bullets which remained in his Kalashnikov.⁹

⁹ Ibrahim al-Marashi has given a series of very perceptive presentations based on these documents to the Cambridge Intelligence Seminar; see his “An Insight into the Mindset of Iraq’s Security Apparatus,” *Intelligence and National Security*, vol.18 (2003), no. 3.

Had the importance of the intelligence documents captured after the Gulf War been fully grasped, the capture of similar documents would presumably have had a higher priority for the allies during the 2003 war in Iraq – particularly given their likely relevance to the search for evidence of Iraqi weapons of mass destruction. And yet for thirteen days after the fall of Baghdad, Iraqi intelligence headquarters and the Foreign Ministry were not secured. During that period looters went in and out of the unsecured buildings. So did the Western media, sometimes bringing out remarkably interesting documents. The captured documents so far released show how Saddam’s distorted understanding of his opponents was reinforced by woefully skewed intelligence reports, leading him first to believe that the United States and its allies would not go ahead with an invasion, then even after hostilities had begun to delude himself into believing that he held the upper hand and could clinch a negotiated settlement through French and Russian mediation.¹⁰

4. *Seeing Ourselves as Others See Us*

The fourth methodology available to answer Jami Miscik’s question is, as Robert Burns recommended, to try to see ourselves as others see us. Intelligence communities have generally been slow to follow Burns’s advice. The Brown-Aspin commission on the role and capability of the US intelligence community, for example, had a wonderful opportunity to ask former opponents, such as the KGB defectors and exiles in the US, what they thought the strengths and weaknesses of US intelligence were. It did not, however, occur to the Commission to do so.

To resume the four stages of my argument thus far:

- Only long-term historical perspective can liberate us from the parochialism of our own forms of cultural analysis.
- The essential condition for the future improvement of intelligence analysis is to identify our existing strengths and weaknesses.
- These can only be satisfactorily identified by examining our longer-term record and not simply the experience of the last few years.
- A variety of complementary methodologies are already available to undertake this examination.

Back now to the question posed by Jami Miscik in her “State of Analysis” address: “What are our analytic strengths and weaknesses?” Long-term study of those strengths and weaknesses, based on methodologies that already exist, has

¹⁰ Richard Beeston, “Secret files show Saddam deluded to the very end,” *The Times*, 18 March 2004.

already begun to provide answers which go well beyond anything that analysis of only the recent past can possibly provide.

To follow the conventional distinction between “secrets” and “mysteries,” during the twentieth century we were frequently very good at discovering our opponents’ secrets when it mattered most but more confused than we should have been by the mysteries of what they intended to do. The American and British success in discovering the capability and deployment of enemy armed forces shortened the Second World War, stabilised a Cold War which might otherwise have turned into hot war, and has since helped to make possible a series of breathtakingly rapid military victories.

The importance of intelligence reports on military strengths and capabilities went far beyond what the data they provided. Studies of the Cold War frequently forget the truth of Eisenhower’s dictum that intelligence on “what the Soviets *did not have*” was often as important as information on what they did. Shortage of reliable intelligence in the early 1950s generated the destabilising American myths of the “bomber gap” and the “missile gap” – the delusion that the Soviet Union was increasingly out-producing the United States in both long-range bombers and ICBMs. In 1955 US Air Force intelligence estimates calculated that by the end of the decade the Soviet Long-Range Air Force would be more powerful than U.S. Strategic Air Command, whose head, General Curtis Le May, became dangerously attracted by the idea of a pre-emptive strike to prevent the Soviet Union achieving nuclear superiority. The introduction of the U-2 spy-plane in 1956, followed four years later by the first imagery intelligence (IMINT) from spy satellites, provided proof that the Soviet nuclear strike force was not overtaking that of the United States. The U-2 missions, wrote Eisenhower, “provided proof that the horrors of the alleged ‘bomber gap’ and ‘missile gap’ were nothing more than the imaginative creations of irresponsibility.”¹¹ Without the IMINT revolution, US policy to the Soviet Union would doubtless have continued to be confused by other destabilising myths about the extent of the Soviet nuclear strike force. It is difficult to exaggerate the importance of the National Technical Means (NTMs) and the analytical tools devised to interpret them, chiefly by US intelligence, to Western policy during the Cold War. According to Robert Gates, DCI from 1991 to 1993:

The great continuing strength and success of the analysts of CIA and the intelligence community was in describing with amazing accuracy from the late 1960s until the Soviet collapse the actual military strength and capabilities of the Soviet Union... And these numbers and capabilities would be relied upon, with confidence, by the Executive Branch (including the Defense Department), the Congress, and our allies both in arms control negotiations and in military planning.¹²

¹¹ Andrew, *For The President’s Eyes Only*, ch.6.

¹² Robert Gates, *From The Shadows*, paperback edition (New York: Touchstone, 1997), p.562.

The undoubted weaknesses of Western intelligence during the Cold War should not lead us to underestimate its unprecedented strengths.

Of the “mysteries” which confused us during the Second World War and the Cold War, the one we were worst at unravelling was the mindset of our opponents – in particular, the understanding of fanaticism. That remains a serious problem because of one fundamental, largely unnoticed continuity between the threats that faced us in the 20th century and those that face us in the 21st.

One of the very few to draw attention to that continuity has been Elie Wiesel, Nobel laureate, holocaust survivor and human rights activist. Several years before 9/11 Wiesel said this: “The principal challenge of the 21st century is going to be exactly the same as the principal challenge of the 20th century: How do we deal with fanaticism armed with power?” Wiesel is surely right. Locating and analysing the threat from “fanaticism armed with power” is, for the foreseeable future, the greatest challenge facing strategic intelligence. All those who did most damage to the 20th century were fanatics armed with power: Adolf Hitler, Joseph Stalin, Mao Zedong and Pol Pot chief among them. Those who are likely to do most damage to the 21st century – Usama bin Lādin, for example – will also be fanatics armed with power, though we may have to deal with a different kind of fanatic. Fanaticism, like other disorders, evolves over time.

What makes the 21st century so far a less dangerous place than the 20th century is that fanaticism is not in control of any of the world’s major powers. The more democracy and prosperity increase, the fewer the opportunities for fanatics to achieve the positions of immense power which they occupied in the last century. Today’s most dangerous fanatics are on the margins of the international system rather than at its centre – rogue regimes and terrorist groups.

But if the political power of fanaticism has declined, its *destructive* power over the next generation will be enormously increased by the proliferation of weapons of mass destruction.

Fanaticism, like the terrorism which it generates, needs to be interpreted in a long-term perspective.

Short-term analysis of fanaticism commonly arrives at one of two misinterpretations:

(a) The fanatic is a rational actor. His (rarely her) aims are rational even if we do not always recognise their underlying logic.

(b) The fanatic is a madman. The British Foreign Secretary, Jack Straw, calls bin Lādin “obviously psychotic and paranoid as well.”

Seen in long-term perspective, fanaticism looks rather different. The most dangerous fanatics have always had, and will doubtless continue to have, two distinguishing characteristics:

(i) First, all fanatics are necessarily conspiracy theorists. Their extreme hatred of the enemies they have sought to destroy over the last millennium (among them heretics, witches, Jews, Trotskyists and the United States) can only be justified by substituting demonic, conspiratorial myth-images for reality. As Voltaire warned us two and a half centuries ago, “Those who believe absurdities will commit atrocities.” Conspiracy theory is the only ideology which – as in the case of earlier fanatics – all the otherwise disparate most dangerous terrorists of the last decade (the first World Trade Center bombers, Aum Shinrikyo, Timothy McVeigh and al-Qa’ida) have in common.

(ii) Second, however, at an operational level, the most dangerous fanatics, despite their conspiracy theories, are calculating and often dangerously effective – as on 11 September 2001.

The fanaticism which is at the heart of today’s transnational terrorism can only be understood if both (i) and (ii) are taken into account. The historical record shows, however, that analysts have found it very difficult to grasp that those who threaten us have been both at the same time. That has been true of our response to Adolf Hitler, Joseph Stalin and – at least initially – Usama bin Lādin.

Because Hitler could, when he chose, play the role of a skilful international statesman, pre-Second World War Western assessments of his intentions simply could not credit the fanaticism with which he pursued his ultimate aims of a huge slave empire in Eastern Europe and the “final solution” of the Jewish question. Though Hitler was obsessed by the preposterous conspiracy theory of a Jewish plot for world mastery, he was none the less shrewd and calculating enough to out-negotiate Western statesmen before World War II and to drive his generals to achieve during the first two years of the war the most spectacular sequence of rapid military victories since Alexander the Great.

While British intelligence knew an unprecedented amount about Hitler’s military operations, caught every one of his spies in Britain and used them as the basis of the stunningly successful Double Cross deception, the Joint Intelligence Committee (JIC) understood very little indeed about how his mind worked – so little that it recruited two astrologers and a water-diviner. Until 1942 the JIC paid more attention to the astrologers than to the conspiracy theories of *Mein Kampf*. One of the reasons why the JIC predicted that Hitler was likely to choose a date soon after 19 October 1940 for Operation SEALION, the invasion of Britain, was that “Hitler’s horoscope, a sign to which he was reported to pay considerable attention, was favourable for this period.”¹³

¹³ See, on this subject, the pathbreaking 2003 Cambridge MPhil dissertation (to be followed by a PhD) by Paul Winter on the attempts by British Intelligence in the Second World War to understand the mindset of Adolf Hitler, and Mr Winter’s forthcoming article on this subject.

Understanding Stalin proved equally difficult. Stalin was, as Khrushchev described him, “sickly suspicious”: “Everywhere and in everything he saw ‘enemies’, ‘double-dealers’ and ‘spies’.” At different stages of his career he was obsessed by huge and mostly non-existent conspiracies by Trotskyists, Titoists, Zionists and homicidal Jewish doctors. The vast majority of the millions of “enemies of the people” who were shot or perished in the gulag were, in reality, enemies neither of Stalin nor of the Soviet system. Yet, because Stalin was also a skilful negotiator who got the better of both Roosevelt and Churchill, Western analysts found it impossible to grasp the centrality of conspiracy theory in his world-view.¹⁴ Some still do. I’ve been struck by the fact that some of those most resistant to the idea of bin Lādin as an obsessional conspiracy theorist misunderstand Stalin in much the same way.

Bin Lādin and his fellow-travellers are so dangerous precisely because, like Hitler and Stalin, they combine obsessional conspiracy theories about their opponents with great tactical and operational skill. Among other conspiracy theories, they believe in the Jewish world conspiracy supposedly revealed in the *Protocols of the Elders of Zion* and in what bin Lādin calls the United States’ “subordination to the Jews.” We cannot understand what al-Qa’ida think they are fighting against and what they mean by “Jews and Crusaders” unless we explore their conspiracy theories. The description of Stalin by the British diplomat, R A Sykes, as “a curious mixture of shrewdness and nonsense” also applies to bin Lādin and his chief lieutenants. A valuable addition to the 21st century US National Intelligence Council (NIC) would be a National Intelligence Officer for Fanaticism and Conspiracy Theory.

Let me return briefly to the Scowcroft mission statement with which I began:

This is a very new world, to which none of the structures or habits of thought established within the intelligence agencies are geared

To respond to the challenges of that “very new world,” here finally is a visionary statement of what a 21st century intelligence service should be like:

All the members of the staff...being intelligent people are treated as such; they are invited to make any suggestions which occur to them for the improvement of the machinery of the office and they are made to feel that they have an important and personal share in the work. So much is this the case that many of the important improvements that have been from time to time adopted, have been suggested by members of the staff.

...Every effort is made to allot to [staff] the work they like best and can do best. The rule is that, while the interests of the work must come first, those of the worker must by no means be overlooked.

¹⁴ Christopher Andrew and Julie Elkner, “Stalin and Foreign Intelligence,” in Harry Shukman (ed.), *Redefining Stalinism* (London: Frank Cass, 2003).

That visionary statement of the new work culture of a 21st century intelligence agency is actually almost ninety years old. It was a description produced in 1916 of the work culture of MI5, which did indeed produce some “successful results” – among them the capture of every German agent who landed in Britain during the First World War.

We should be foolish at the beginning of the 21st century not to attempt to learn from our past successes as well as our past failures.

New and Emerging Challenges for Intelligence Analysis

Markus Ederer*

After the fall of the Iron Curtain, we have not seen the end of history as some had predicted but a phase of rapidly changing parameters of International Security Policy. As unexpected as they were in nature and scope, the attacks of 9/11 are nevertheless paradigmatic of this New Age of Security Policy. But they are not the only symbol of a changed security landscape. The US have become the world's only superpower. We have witnessed that increasing globalisation and bloc building (EU, NATO, NAFTA, etc.) do not exclude concurrent regional fragmentation and ethnic strife as in the Balkans and in some parts of Africa. The borderlines between war and peace have become blurred. The same holds true for the distinction between internal and external security. Nowadays the debate about security is dominated by transnational and asymmetric threats which our free and highly developed societies are extraordinarily vulnerable to.

Intelligence analysts must attempt to rise above the shifting sands of daily crises and try to structure the threat environment as well as our responses. As a practitioner, I very much advocate defining intelligence requirements from the customer's angle, that is what governments expect from us. As I was asked to add a European view to this panel, let me remind you that in December 2003 the Member States of the European Union collectively defined the main threats in their EU Security Strategy:

- International terrorism
- Weapons of mass destruction
- Failing states
- Regional conflicts
- Organized crime

* Hr. Dr. Markus Ederer is Deputy Director of Analysis, Bundesnachrichtendienst (BND), Germany.

This threat analysis, which is primarily characterized by transnational challenges and asymmetric threats, requires intelligence services, too, to update and change their *modi operandi* fundamentally. The situation may be described by how a US colleague put it a couple of years ago: “A plane hit the Pentagon, and we have not changed our processes.” We Europeans would probably come to similarly sobering conclusions, even after the bombings of Istanbul and Madrid.

In this vein, let me refer to just three current issues in our wider intelligence culture which we can turn into opportunities, if we get things right:

- Culture of prevention: warning and response;
- Fighting the elephantiasis of reason;
- Fighting networks with networks.

Culture of Prevention: Warning and Response

First, we have to improve our culture of prevention. Crisis prevention is cost prevention. This is particularly pertinent when it comes to state failure and regional conflicts, but applies as well to fending off other threats such as the proliferation of WMD, international terrorism or organized crime. A culture of prevention which deserves its name is about warning *and* response. We, the International Community, are often not very good at timely and adequate responses; the Balkans and recent African crises are eloquent proof of that. Let me illustrate this with a recent experience. Some time ago, I accompanied a briefing team to an EU institution in Brussels. The case in hand was a failing state in the EU periphery about to corrode into a failed state. After listening to us, these people said: “Thank you, we fully agree and we, too, have it on our radar screen. Our problem is that with all the ongoing mega crises we cannot bring this one to the attention of politicians.” And then they jokingly added: “Can’t you organize a real conflict there?” This says everything about our culture of prevention and the missing link between warning and response.

Fighting the Elephantiasis of Reason

A second point I would like to make is particularly pertinent in countering the number one global threat: *jihād* terrorism. It is about overcoming the elephantiasis of reason. As most of us are educated in the Western world, we are taught to base analysis primarily on hard facts, to think in a linear way and to come up with rational conclusions. I suggest that while this is necessary, it is not enough.

In order to illustrate this, I want to ask you two questions: Would anyone in his right mind fly a plane into the World Trade Towers? Most of us would say No. Did it happen? Yes.

The conclusion to be drawn is that we need to improve our ability to think the unexpected or even – as in this case – the unthinkable. Furthermore, as a matter of methodology and when the situation at hand requires doing so, we have to be able to question our usual rational, linear thinking. We ought to understand that merely extrapolating on the basis of past data may be as fallacious as using your car’s rear mirror as a prognostic instrument for the road ahead. Moreover, skilled analysts know that assessing the perceptions of the other side is often more important than analysing facts.

But do our services have the type of analysts who live up to the above criteria? Without any doubt, there is a dire need for improvement, which can be achieved by more intelligent recruitment and training of future analysts. In this process, however, we are hitting several roadblocks, and I want to mention three of them:

- Most of our current analysts as well as the newcomers lack the historical and cultural knowledge as well as the religious and sociological backgrounds of Islamic societies which are required to penetrate the minds of jihadi terrorists.
- Our intelligence-gathering systems rely heavily on traditional data collection and on measuring quantifiable facts. Correctly assessing perceptions as well as cultural and religious aspirations is a still underdeveloped and yet to be conceptualised discipline.
- Intelligence is generated in bureaucracies. This reminds me of the old joke that “intelligence service” is a contradiction in terms. Indeed, intelligence is produced in bureaucracies, and bureaucracies are inherently averse to thinking in terms of discontinuity. They do not reward tangential thinkers and people who think “out of the box.” Therefore, we are losing much potential there, and it is a management question of how to tap this potential.

Fighting Networks with Networks

There is another field where we need to get better. The expansion of international communications structures and globalization have facilitated the emergence of networks which reflect the new dangers (such as international terrorism, proliferation of weapons of mass destruction, organised crime). Therefore, one of our central tasks must be to improve the formation of our own networks so as to be able to counter the adversaries’ networks.

Why is there no viable alternative for intelligence services? I see two main reasons:

- When it comes to information management, we have a famous saying referring to Germany’s biggest IT company: “If Siemens knew what Siemens knows.” This refers to the fact that in big organisms the piece of information you are looking for is often hidden somewhere in the system but is not available to

the person or the unit that needs it most. Networking and communications can prevent that.

- Networks unlike hierarchies have built-in redundancies. If part of a network is hit or becomes dysfunctional, other parts of the network can take over. This makes well-managed networks the most efficient organisational structure in times of crises.

A System of Network-Centric Intelligence

Such a network on our side of the intelligence community should look like a system of concentric circles, with each circle describing one network and all these circles communicating with each other on the pattern of a network.

The innermost circle represents the intelligence service. The network potential is chronically underexploited already in our organisations. Enhancing lines of intra-service communication, questioning those firewalls which hedge bureaucratic competences rather than secrets, as well as task force building are the needs of the moment. Regular meetings of regional experts from the various areas, collective tasks for multi-experts resulting in interdisciplinary and supra-regional analyses, tighter networking of analysts with their colleagues from HUMINT and SIGINT without giving up the intelligence-specific protective functions are additional tools to get better results.

The intelligence service (inner circle) needs to network with the entities in the next circle, which describes the national arena. We are talking about inter-service relations, we are talking about service-government relations, we are talking about service relations with lower layers of administration. There is a lot to be done in terms of better networking within governments, which brings me back to the issue of governance which was already mentioned today. We all know about the rivalries between services domestically as well as about communication gaps between government and services. The answer is to move away from this type of inter-blocking institutions and create interlocking institutions instead. As intelligence services, we also need to reach out to national competence hubs which have the expertise we don't have: think-tanks, NGOs, and even the private sector. To this end, we have to do a critical review of our self-created firewalls and of the needs of our civil society partners, whose professional purpose and integrity must not be compromised.

The outer concentric circle in this system of network-centric intelligence describes the network at the international level. When it comes to outreach to other entities such as NGOs, private sector and so forth, the rules of the national arena should apply *mutatis mutandis* and new approaches should be sought. When it comes to networking of intelligence analysts amongst themselves, this seems to be nothing new to them, as we convene at this conference. Also standard prac-

tice are bilateral exchanges, even multilateral exchanges, but all of these are really only exchanges of finished intelligence.

My understanding is that this will not suffice in the future. We have to take the network idea further. Decisions on countering transnational or external threats to our societies are usually taken at a multilateral level – be it the United Nations, NATO or the European Union. However, the intelligence assessments which serve as basis for governments to take their decisions are produced autonomously at national level. While there is some justification for that due to the very nature of the product, we are liable to generate more fissures in the International Community, such as over Iraq, unless we advance to selective joint assessments internationally. As long as national threat perceptions are potentially divergent, how can policies at the international level be convergent?

In this vein I would like to refer to what was said today about the “War against Terror.” Interestingly enough, the United States is in a war against terror, whereas the Europeans, while fighting terror, have prominently rejected the notion of war in this context. This is the result of different threat assessments. There are a few more cases in the transatlantic relationship where joint threat assessments such as on Iran or North Korea would greatly help joint decision-making.

I am not sure whether our American friends, who some believe are from Mars, are aware that we on Venus (Europe) have already engaged in the futuristic activity of joint intelligence assessments. With the Joint Situation Center (SITCEN) in its Secretariat General, the European Union has made the hitherto widest-ranging attempt at international level to lay the groundwork for its Common Foreign and Security Policy by generating integrated situation and threat analyses. Made up of analysts from a total of presently seven EU member states, the SITCEN essentially operates on the basis of the so-called watch list of about 25-30 crisis regions. Their joint assessments are to facilitate decision-making in the EU Council. The merits of this unique networking approach, as I see them, are clear:

- the knowledge base is broadened;
- pooling of different information from different services with different strengths;
- harmonization of warning cultures;
- joint conclusions which necessarily help for unified decisions.

Not only with its enlargement will Europe widen and deepen this approach. I would also like to refer to the appointment of a EU counterterrorism czar, Mr. de Vries from the Netherlands, in the aftermath of the Madrid bombings as well as to the decision to hold regular meetings of all EU security services.

There is a clear message emanating from the above: if we want to live up to our responsibility to protect our citizens from the new threats, we don't really have a choice. There is no more powerful alternative to fighting networks than with this level of networking amongst ourselves.

Evolving Approaches to Analyzing Transnational Threats: Key Challenges and Potential Partnerships

*David Gordon**

Let me start by drawing a distinction between transnational forces and transnational threats. We've tended to talk about them like they are the same. When we at CIA look at the world and organize ourselves to look at these issues, we draw an important distinction between them.

We identify the key transnational forces as:

1) Economic integration, including financial liberalization, trade liberalization, the expansion of trade, the growing interdependence of national economies.

2) The information revolution, i.e. the growing speed and volume of information flows around the world and across national borders.

3) The rise of transnational organizations of which there are four main types: international organizations (public organizations, governments); multinational corporations and transnational commercial ventures; non-governmental organizations (be they essentially beneficial such as relief organizations or threatening such as international terrorist networks); and media organizations, which are increasingly transnational influences in shaping the way people view the world.

These are the main sets of transnational forces that are shaping the world; transnational threats largely derive from the impact of those forces.

Earlier speakers have cited Joe Nye's important distinction between mysteries and secrets, and have claimed that mysteries will increasingly dominate in the new intelligence world of transnational threats. I don't think this is exactly right. While it is true that in the assessment of transnational forces we are mainly dealing in the world of mysteries, of challenges to analysis and to understanding, I believe that for the most serious transnational threats we are still engaged substantially in the world of secrets. The unstripping of secrets rather than the unwinding of mysteries still remains the primary function of intelligence analysis, particularly on issues of terrorism and the proliferation of WMD.

* Dr. David Gordon is Director of the Office of Transnational Issues, Directorate of Intelligence, Washington, D.C.

So for us in the US and at the CIA, we haven't organized ourselves around transnational threats as a general category. There are two different types of transnational challenges as we see them. There are those that are driven by individual actions – whether those be actions by overt adversaries such as Wahhabist terrorists or by international criminals or narcotraffickers that are motivated by greed rather than creed but threaten us and global security nonetheless. This first set of transnational threats is very much driven by individual action and motivation.

For the most serious of those issues, our approach in the US has been to take the analysts working on those issues and move them as close as possible to the operations needed to undermine and prevent those adversaries from having their way. We've set up integrated centers that combine intelligence analysts with our operational forces; our two main centers are the Counter-Terrorism Center and the Counter-Narcotics Center. Our goal is to maximize our ability to identify the individuals and the nodes, the groups, the networks, and be able to disrupt them. Our effort to move the analysts and the analysis as close as possible to operations facilitates the exchange of information and the creation of actionable intelligence as rapidly as possible as well as the feedback to analysts from operations. That's been our main mode.

On weapons proliferation, we've organized ourselves a little bit differently. There we've moved to a different form of integration; analytic integration of what had been disparate analytic enterprises earlier – weapons analysis, proliferation analysis particularly of WMD, and treaty monitoring and monitoring of international organizations and agencies in proliferation issues. On WMD issues, we've tried to integrate across what had been historically a disparate set of analytic occupations to get the best picture possible of weapons development and weapons proliferation issues.

After Sept 11, of course, there was a lot of concern in the US about obstacles to sharing between foreign intelligence agencies and domestic security agencies. Under American law, historically we've erected a fairly sharp fence between the two. In the aftermath of 9/11, one of the major challenges we faced was how to better integrate threat analysis from both the foreign and domestic perspectives. Last year, we set up the Terrorist Threat Integration Center – comprised of personnel from CIA, FBI, Department of Homeland Security, Department of Defense, and Department of State – as our main instrument to aggregate and integrate threat information from both foreign intelligence and domestic and other sources.

So those are the main organizational issues I wanted to talk about as far as the set of transnational challenges that are focused on individual actors and networks, etc.

There is a second set of transnational phenomena which, while driven by collective behavior, don't have the same individual or action group drivers but that

nonetheless shape national regional and global political evolution and national security. In this category, I include issues such as the globalization of finance and the increasing frequency of financial crises, and the impact of financial crisis on global economic consideration and national security in affected countries and regions. We also assess demographic issues such as youth bulge, aging, urbanization, migration and other demographic forces that are literally reshaping the way the world looks and will play very powerful roles in determining which countries are well positioned for the future and which countries are less well positioned for the future. Failed states, political instability, religious extremism, ethnic and regional violence are another set of challenges that are less driven by particular individual actions but the analysis of which is important for understanding the nature of transnational challenges and the outcome of which has national security implications for policy makers. Global infectious diseases that Peter Schwartz spoke about in this conference are another increasingly important issue. The AIDS pandemic is a phenomenon that is already shaping national security considerations in sub-Saharan Africa. And in the future in China, Russia, other countries on the Eurasian land mass, and areas of the Caribbean and Latin America the potential for large scale disruption from AIDS cannot be ruled out. So these are some of the issues that we include in our assessment of transnational challenges label, and that that I manage in the DI's (Directorate of Intelligence) Office of Transnational Issues.

Let me speak about some of the key analytic challenges that we face in examining these issues. A very important one is how to balance the priority of operational and tactical support for policy makers, for war fighters, and for intelligence operators, with the need to step back and assess strategic and longer-term trends. What we have done in our directorate increasingly is to create small strategic units of analysts that are explicitly focused on stepping back but work in an overall environment that retains a connection with more operationally and tactically focused analysts.

Second, we've had to learn to work with new partners, be they in our Department of Health and Human Services, our Centers for Disease Control, our Justice Department, our Customs office, and components of our international economics bureaucracies that previously had been largely independent of the intelligence community. Also within our government there are new efforts to make linkages to levels of government much lower down in our federal system, as individual state and urban security agencies set up intelligence-based organizations. These are coordinated in the US system by the Department of Homeland Security.

All of this provides a fluid context, and really a new world for us as intelligence analysts. This is especially the case for my analysts in OTI (Office of Transnational Issues), whose sources are predominantly drawn from open source information. It involves learning how to utilize the open sources, distinguishing

what is useful information from what is less useful information in a world where overload is the norm, figuring out who has useful information and engaging with them whether they be in business organizations, in think tanks or in non-governmental agencies. One of our most important best practices has been understanding the need to “strip the bias” from open source information, recognizing that banks and financial houses take positions and these positions shape their analytic writing, that non-government organizations and think tanks promote certain policy stances and that in engaging with them you have to learn how to separate the analytic germ from the chaff of policy preference.

We have found that there is a creative tension between analysts working on transnational issues and those analysts in our regional offices whose focus is more on national and regional analysis. But our overall product can be considerably enhanced by sharing with regional analysts our perspective on the drivers coming from the transnational arena, understanding that the perspective coming from the regional arenas will often be somewhat different.

Finally, I feel we have a real challenge in creating a diverse work force that can help us meet these analytic issues, diverse in terms of their training, diverse in terms of their culture and background, and in terms of their experience. Diversity is very important partially because of the danger of groupthink, of closed mindsets and the potential for diversity to be a built in barrier to help ward off those important analytic challenges.

Let me speak finally and very briefly on potential for partnerships. As we do our work, we are finding an increasing role for various kinds of partnerships. We have partnerships with other agencies in government that have analytic value to the issues we cover but haven't engaged much in the past with intelligence agencies and intelligence analysts. Second, we are generating partnerships and joint analytic ventures with institutions outside of government based on mutual respect and benefit. Finally we are increasingly looking to engage with other intelligence services to share not only information and intelligence nuggets but how to look at the world, how to have insight on key issues of concern, how to take advantage of differing analytic strengths. I have been continually impressed by the growing analytic competencies in numerous services, including those with which we in the US have not had broad relationships. Building partnerships among different services takes a long-term commitment, understanding the sensitivities of each of the partners, the importance of reciprocity and respect, and the need to protect sources and methods and highly sensitive information. Moreover, both sides will need to be sensitive to the fact that different legal environments particularly between countries with different legal traditions can make partnerships operationally challenging to create and sustain, even when there are shared policies and shared interests. But, given the potential benefits, perseverance will be the key.

The Future of Intelligence Analysis

*Greg Fyffe**

My comments are from the perspective of the head of a small assessment organization, trying as we all are, to anticipate where intelligence analysis is going and must go.

What could change to further complicate our profession? The answer is just about everything. The attributes of states, the nature of the enemy, technology, and even the physical nature of the planet, are changing in ways that will alter what has to be assessed and why.

The point of intelligence collection and analysis is to give information and judgments to decision-makers that will help them advance their national interests. During the Cold War this could be translated into specific objectives:

- Ensure adequate warning of a possible attack.
- Gain sufficient knowledge of Soviet Bloc weapons systems, order of battle, and strategic and tactical plans so that if war did come, it could be won.
- Prevent the other side from gaining a parallel or greater intelligence advantage.
- Gain wherever possible, directly or through proxies, victory in the struggle for the allegiance of non-aligned states.
- Prove the superiority of the liberal democracies.

Today the challenges are similar in a very general sense, but their essence has been transformed by the reality of imminent danger. Now governments have to:

- Protect citizens at home and abroad from terrorist attack, often without any certainty that an attack is or is not likely, or if likely, may be imminent.
- Understand in detail which groups and individuals are implicated in terrorism. Intelligence has to remove suspicion from the innocent as well as tighten the net of evidence around the guilty. “Joining the dots” really means pursuing all suspicions, which can lead to controversy about the involvement of individuals and the consequences of suspicions about them.

* Mr. Greg Fyffe is Executive Director, Intelligence Assessment Secretariat, Privy Council Office, Ottawa, Canada.

- Track shifts in terrorist targeting and preferred weapons and tactics. What are the real vulnerabilities so analysis can lead to concrete measures to protect what is at risk?

- Anticipate the weapons systems and force structures that will be needed in future conflict scenarios, including and beyond terrorism.

- Understand the emerging global economic system, and identify the realities that will have an impact on the economic stability of populations of interest, and their vulnerability to terrorist or criminal recruitment.

- Support effective governance in states at risk from terrorism, insurgency, crime, and corruption, or a reversal of the trend to democracy.

- Understand the security impact of environmental change, and combat criminal activities which raid scarce resources or evade environmental safeguards.

- Understand the security and intelligence implications of new technologies, for terrorists and criminals, and states. Every change in communications technology has implications for terrorist networks.

- Understand the future that will be shaped as waves of change interact.

And as before:

- Defend the ideal of free and open democracy, not this time against communist totalitarianism, but from maniacal religion, the corruption of governance, and global criminality.

We are, happily, entering an era when our preoccupation is not primarily the possibility of state against state conflict. As globalization has advanced, and alliances have expanded, the prosperity of nation-states has become increasingly dependent on the adherence to minimal international norms.

Countries which promote totalitarian ideologies, finance terrorism, are identified as WMD proliferators, or systematically violate human rights, find they have a relentlessly diminishing circle of friends. In the global village, however disputatious, there are norms, and they are increasingly pursued by pressure on problem states.

As it becomes more difficult for states to reject the value of the international community, that community has become progressively more pre-occupied with non-state actors – small groups led by semi-anonymous and often autonomous leaders, who rise through shadowy hierarchies.

The ideological divide which ran between countries now runs through them.

The ideological war is de-centralized, ubiquitous, and partly invisible. The Islamic extremism which drives the current terrorist phase is not in its essence a state ideology, although some states have embraced it. It is the integrated religious vision of a portion of the Muslim populations across the globe. Within the worldwide population of 1.6 billion, an indeterminate number are of extremist views, exposed to extremist views, or may be recruited to extremist views.

Some important boundaries are not between countries but in people's heads.

Communism was defeated in part because people who lived under it experienced its failures. The factors which validate or ultimately challenge a religious vision are complex, long-term, and difficult to challenge through debate, or earthly experience.

Terrorist structures are different in every significant trait from the large and skeptical bureaucracies that supported, or in some cases turned spectacularly against, communism. The potential for recruitment from within of agents motivated by disillusionment is slight. Similarly, elusive terrorist groupings are changing even as the analyst gets a fix on them.

Terrorist leadership groups are based on family, clan, religious faction or fighting pedigree. The supremely important question of whether captured or killed leadership elements can be replaced does not admit an easy answer where the recruitment pool is huge, and the ideological drivers likely persistent over decades. So far, it looks like the extremist vision will be taken up by new leaders, and projected by a steadily replenished supply of planners and attackers.

Another change in the environment of intelligence analysis is the further expansion of the coverage of open sources. Academics and journalists have studied terrorism extensively. Both have good access to the ideologues and perpetrators themselves because the struggle is in part a propaganda struggle. Some books and articles have information and insights of great value that would only be available to intelligence collectors at great risk, if they were accessible at all.

What are the consequences of these changes for the craft of analysis?

1. Much more of our focus will now be on the dynamics of mass movements, and the means by which a multi-state religious movement can maintain itself across borders. Will recruitment to terrorism produce all the needed skills? What would weaken such a movement? Will moderate Islam enhance its appeal? Can there be a counterpart to the successful ideas struggle of the Cold War? Can the drivers of anti-western emotion be blunted? Will the struggle be local or globally controlled? These are important questions with a high mystery content.

2. The need for rapid reaction means a compacted intelligence cycle. Collection, analysis and dissemination must be done on an urgent basis, leading to decentralized cell structures formed from elements of less agile, large, permanent bureaucracies. There is no time for information to move through multiple layers, so specialized cells have been created to shorten the time from collection to analysis to action. Strategic intelligence has to be joined to the kind of shorter-term intelligence and action capacity developed by internal security services and police forces.

We have to join a global analysis of the terrorist threat with the capacity to supply on-the-ground security and police forces with integrated and actionable information. This is a formidable challenge, particularly for those countries

which have not experienced lethal internal security threats in their recent history. We can know a great deal about terrorist intentions and capacities without knowing when and where they will strike. Canada's recent budget provided funding for an integrated threat analysis capacity, but as we all know finding analysts with the right skills is not always easy.

3. A feature of the post-Cold War period, consistent with the long term trend to international cooperation and coordination, has been frequent and often rapid deployment of forces to unstable regions. This makes it necessary to maintain a basic intelligence capacity in many areas of marginal strategic interest so that the terms of deployment can be developed, and the deployment itself supported.

Analytical assets developed for today's challenges may not be on target for those we have to meet tomorrow. Annual or longer-term priorities, reflecting national interests, will certainly be dislocated by international emergencies.

We are likely to continue to need to arbitrarily re-assign analysts to new fields, as many were re-assigned to terrorism. This will produce frustrations, since many of the unstable areas that suddenly become international priorities are complex, distant in their culture from the countries deploying military or civilian aid, and will speak languages that are difficult to learn – and these difficult-to-acquire skills could in turn become quickly outdated.

4. The challenge to understand trends and global drivers is at a premium when the number of unpredictable and unstable areas of the globe seems to have expanded. Understanding and parrying the individual deadly threats generated at the micro level lies at one end of a continuum. At the other end are vast historical, governance, economic and social changes resulting from the impact of globalization, technological change, and the reality of global environmental change and its likely impact on human relationships within states and between states.

Organizations need to equip individual analysts to speculate about the future, and absorb into their analytical perspectives work now being developed by specialized strategic groups. This is a major issue for smaller analytical organizations.

5. On the positive side, we will find much more of what we analyze is analyzed in parallel, at the strategic level, by open sources. Terrorist groups have an agenda to sell to donors, potential adherents, and possible recruits. They are, like the rest of us, entranced by the communications potential of the internet. And, they believe there is value in talking to journalists and academics. In Western societies much of the terrorist discourse is in semi-public forums. Some of this information is gathered by journalists at great personal risk.

Part of our contribution as analysts will be not just our access to covert material but an expertise that allows us to sort out what is relevant in the vast amounts of open source material to the agenda of government.

There is less reason to believe, unfortunately, that open sources will be useful at the tactical level, although the media plays a role in broadcasting warnings, telling people what to look for, and perhaps searching for clues after an attack.

6. Because of the immediacy and breadth of the terrorist threat, intelligence has become more important to more people, but expectations of intelligence are high. There is an understandable belief that the expensive investment in intelligence should have parallel payoffs.

When very small and secretive units can cause enormous casualties, this is a difficult expectation to meet, and success and failure alike are quickly visible.

7. Increasingly, our natural surroundings will be an analytical concern for intelligence. Changes forecast for the environment may have a more profound effect on global security than those intentionally pursued by nations and leaders and terrorists. Whatever the causes of climate change, something critical is occurring.

One important consequence of global climate change is already clear. Drought, flooding, wind and ice storms, and forest fires are expensive. They dislocate national budgets and take money from other urgent priorities.

We can probably expect the trend to weird weather to continue. The resulting spending pressures will have an impact on domestic priorities, and on foreign aid and defence spending. They will increase the need of poorer countries for emergency aid, and diminish our capacity to give it.

If climate change progresses further, some of the most predictable consequences include:

- temporary damage to productive agricultural and industrial areas;
- possible permanent loss of growing areas if temperate zones shift;
- significant shifts in patterns of precipitation;
- flooding of low-lying lands, which is already happening to some degree.

If we see changes in patterns of food production, water availability and the physical availability of land, then we can also foresee population shifts and changes in the relative prosperity of nations and parts of nations. This will interact with the challenges we already face – global population growth, pollution, religious fanaticism, large-scale migration, technological change, and more favourable conditions for the rapid spread of epidemic disease. Increased global prosperity may increase political stability, but further damage the environment. We see a microcosm of this trade-off as oil production remains critical to the prosperity and stability of key countries, while the increased accessibility to cars in developing countries speeds the impact of greenhouse gasses.

In the end our challenge is simply that we expect we will be living in a world with more immediate dangers, but whose shape will form and re-form in unpredictable ways, possibly veering at times to the chaotic.

The present is characterized by immediate dangers that force us to make analysis immediately relevant, but we cannot diminish our efforts to understand the longer-term future, which may or may not be preoccupied by terrorism, but which is likely to see the re-emergence of state-to-state conflict, crises driven by global economic interdependence, and an increased impact the natural environment on the shape of the security environment.

Our clients expect us to get the judgments right on both the long and short term, on the immediate dangers and the future context.

Our greatest challenge in this interconnected, intermestic world may be that we cannot easily separate the strands and set priorities. If it is all connected then we must, until the shape of things to come is clearer, be prepared to do it all.

Analyzing Transnational Intelligence

*Michael Wesley**

Transnational issues have been affecting international relations since the 1970s, acknowledged intellectually but not practically by the national security structures of states until late in the 1990s. Since the 1970s, of course, the globalisation of consumer culture in affluent societies, shifting concepts of sovereignty and the removal of impediments and barriers to the flow of goods, finance, and to some extent people has intensified transnational threats (to some extent states are now trying to re-impose barriers against the dark sides of globalisation, but whether the good and the bad of globalisation can be separated is doubtful). The terrorist attacks on 11 September 2001 and the ensuing War on Terror – which has had to confront along with terrorism the problems of proliferation, illicit financial flows, irregular people movements, the drug trade, networks of criminal facilitators and corruption – have brought transnational issues to the forefront of national security. Transnational threats are here to stay as issues of practical national security importance, not the least for having changed permanently the logic of strategic competition and alignment among states.

I define transnational issues as those that arise from within one or more societies (rather than from within the decision structure and resources of the state) and are transmitted or replicated across national borders to threaten the security or values of society – and ultimately the security or viability of the state. They include terrorism, proliferation of WMD and missile technology, organised crime, drug production and distribution, serious disease epidemics, irregular people movements, illegal resource exploitation, and disruptive doctrinal movements. Many of these issues were elevated to the top “hard targets” priority for intelligence collection by the Clinton administration in PDD-35 in 1995, but none of them fall easily into the long-understood logics of international relations. By definition, they are unable to be stopped by any state acting alone.

* Dr. Michael Wesley is Assistant Director-General, Transnational Issues, Office of Transnational Assessments, Australia.

Many are also immune to standard multilateral responses. And as the *National Security Strategy of the United States* of 2002 observed, “traditional concepts of deterrence will not work against a terrorist enemy... whose most potent protection is statelessness.” We could add that traditional state-to-state deterrence will not work against any of the stateless, transnational threats listed above.

As if this wasn't enough, transnational issues have become a major political issue since September 11. Before these attacks, Mark Lowenthal observed that “in some respects intelligence is expected to operate perfectly when dealing with terrorism.”¹ Yet the public's tolerance for intelligence failure on terrorism and other transnational issues has only decreased since. Added pressure is placed on intelligence agencies to get it right as society demands that those responsible for the outrage – be it a terrorist attack, a major people-smuggling operation, or a drug importation racket – be brought to justice. And as states put increasingly onerous measures in place to protect society from transnational threats, governments have begun to use intelligence publicly to build support for their security measures. Once again, intelligence agencies are put in a difficult position – not only does increased publicity threaten the secrecy of sources and methods, it increases the public's expectations of the omniscience of their intelligence services. Placed squarely in the front line of protecting society from transnational threats, intelligence agencies have become worried they will miss the significance of a piece of intelligence warning of an impending attack. Facing the choice of not reporting a piece of intelligence and risking it might be genuine, however spurious it may look, the natural reaction is to report it. So the onus of evaluating and reacting to threat intelligence is pushed to higher and higher levels of government, challenging the very reason for being of intelligence analysis agencies.

Intelligence on Transnational Issues

Writing in the early 1990s, Walter Laqueur despaired of the scale of the task of mounting an adequate intelligence effort against terrorism, not to mention other transnational threats:

[Terrorism] is not only dangerous, but exceptionally complex ... the terrain is ... largely unexplored. Western intelligence services subjected to economising do not have the funds or manpower to deal with the enormous infrastructure, encompassing hundreds of channels, through which money, people, and weapons are transferred.²

¹ Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2000), p. 175.

² Walter Laqueur, *The Uses and Limits of Intelligence* (New Brunswick: Transaction Publishers, 1993), pp. 103-104.

September 11 has put paid to economising on intelligence services, but the complexity of transnational targets has not diminished – indeed there is much evidence that it’s increasing. Most transnational issues are the work of networks of non-state actors distributed across several societies, interacting amidst the vast quantity of transactions occurring daily in a globalised world. The most effective and difficult-to-target networks are those that have discovered the benefits of decentralised transactional networks. Linkages are increasingly made on the basis of either shared general goals or common interests in a particular transaction, rather than being based on ethnic- or family-based loyalties or formal command structures. As a result, the most dangerous transnational threats we face are beginning to exhibit what biologists term “emergent behaviour,” where the dynamic interactions of agents reacting to local situations give rise to collective behaviours that are more flexible and complex than a centralised, hierarchic organisation would be capable of.³ Globalised communications enable far-flung groups to observe and adapt the most effective techniques they see used elsewhere. Often the most dangerous transnational flows are not people or goods but information – be it the doctrine of world *jihād*, gas centrifuge designs, synthetic amphetamine recipes, or how to make shape-charges.

Compare the task of collecting adequate intelligence on such networks to that confronting Western intelligence agencies at their outset: to collect and interpret intelligence on a few secretive but rigidly hierarchic and centralised states, usually on policies, dispositions and capabilities that were developing in a single, coherent direction over decades. Penetration of transnational networks may or may not be easier than penetrating the Kremlin, but in the absence of a clear hierarchy of command and control, the real challenge for collection and analysis is assessing the value of the intelligence gained. Reporting on the intentions of one or several actors in a transnational network gives intelligence agencies a highly uncertain picture of the intentions and capabilities of the network as a whole. And as decentralised actors constantly adapt their behaviour to deal with local requirements, it is difficult to build a dependable picture of the network incrementally. Collectors of intelligence on transnational threats increasingly have to do their own, on-the-spot analysis in order to validate information and prioritise collection targets against a rapidly-evolving organisation.

Transnational issues are also challenging other traditional intelligence structures. They are blurring the distinction between domestic and international intelligence collection as well as that between the public/state sphere and the private/societal sphere of security.⁴ As transnational issues widen the range of se-

³ See John H. Holland, *Emergence: From Chaos to Order* (Oxford: Oxford University Press, 1998).

⁴ Gregory F. Treverton, “Reshaping Intelligence to Share with ‘Ourselves,’” *CSIS Commentary*, No. 82, Summer 2003, p. 5.

curity threats to states, more departments of government are being drawn into the business of national security and are becoming consumers and collectors of intelligence. The vulnerability of societies and their infrastructure to terrorist attack has brought immigration, health and transport departments into security structures and made the information available through their bureaucratic networks vital to intelligence early warning systems. Transnational issues have also forced intelligence agencies to internationalise. Many Western intelligence agencies, as part of the campaign against transnational threats, have increased their co-operation with counterpart agencies of states outside of traditional alliance structures. The resulting sharing of intelligence and tradecraft gives rise to fears about the protection of sources and methods and the effect that co-operation will have on these states' future counter-intelligence capabilities. Expanded intelligence liaison has also delivered a greater amount of intelligence material of uncertain reliability for intelligence analysis organisations to cope with.

As intelligence collection and analysis on transnational threats increasingly resembles forensic police work, so what were once thought of as criminal acts have become redefined as transnational threats. With law-enforcement being asked to take on roles outside of the traditional parameters of police work and intelligence being directed at transnational issues, law enforcement and intelligence agencies have begun to work more closely together. Here lies another set of practical and conceptual boundaries. Intelligence work is essentially forward-looking, seeking to predict and forestall emerging threats to 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 prosecuting the perpetrator. Information-sharing difficulties abound: intelligence agencies are unwilling to let covert intelligence material be used in making criminal cases against the perpetrators of transnational crimes; while police won't allow evidence crucial to an ongoing investigation be passed outside the bounds of the investigation. Police often want to arrest and charge criminals while intelligence agencies want to leave them in place and see how far their networks lead. Law-enforcement organisations whose remits are legislatively constrained are often reluctant to see themselves as part of the state's national security structures – and all the more so if their co-operation with overseas agencies would be endangered if the police were seen to be co-ordinating with foreign "spies." But however difficult and painful, further convergence needs to occur. Law-enforcement agencies have been developing their own concept of strategic criminal intelligence since the 1960s; there is much they can learn from the intelligence community. And the intelligence community, increasingly drawn into the world of transnational threats, can learn much from police organisations also.

Analysing Transnational Intelligence

In an ideal world, traditional intelligence analysis is a process that is supposed to look something like this:

Analysts simultaneously – and for the most part instinctively – use inductive reasoning to find patterns amidst the flood of data, and use deductive reasoning to provide meaning and context for the patterns they find. Incoming bits of intelligence data are filtered through this framework, and those that fit are imbued with meaning and context, while those that do not fit are set aside as potential modifiers of the concepts.⁵

Currently, the analysis of transnational intelligence is hampered by several problems. Unlike traditional country-based, scientific, economic or strategic analysis, transnational analysis is still an emerging thematic specialisation – it is yet to develop its own core concepts and doctrines to help it navigate through the intelligence material. In such a situation transnational intelligence analysis confronts what Robert Jervis terms “a grave danger”, which “lies in not having sufficient expertise about [a geographic] area ... to detect and interpret important trends and developments ... [to] make up for such deficiency, analysts tend to impose on the information the concepts, models and beliefs they have derived elsewhere.”⁶ On the other hand, as transnational issues upset previous truths about a country or issue, analysis also faces what Jervis calls “the parochialism of the expert”, where a Western analyst with long experience of working on a country or issue dismisses evidence of significant changes or trends that are at variance with their long-held judgements.⁷ Transnational analysts need also to beware of the dangers of “mirror imaging” – whereby an analyst in an hierarchic, integrated bureaucracy that relies on functional specialisation, oversight and bureaucratic process to achieve corporate results starts to expect a relatively autonomous, multi-skilled, entrepreneurial protagonist in a decentralised network to think in the same way as he or she does.

Transnational analysis also finds itself at the forefront of political pressures and confronted by an avalanche of intelligence information of highly variable quality. It faces the requirement placed on all intelligence analysis: that its customers are presented with hard baseline judgements and forecasts of likely out-

⁵ Stephen Marrin, “CIA’s Kent School: Improving Training for New Analysts,” *International Journal of Intelligence and Counter-Intelligence*, Vol. 16, 2002, p. 623.

⁶ Robert Jervis, “What’s Wrong with the Intelligence Process?,” *International Journal of Intelligence and Counter-Intelligence*, Vol. 1, 1986, pp. 31-2.

⁷ In Australia there is currently such a debate occurring over the spread of Islam in the South Pacific; many Pacific experts in government and academia dismiss the possibility as being incompatible with traditional Melanesian tribal culture, despite evidence of the successful conversion of significant numbers of locals to Islam.

comes in a timely manner, while the intelligence is still “fresh.” This leads inevitably to analysts having to make judgements on the basis of the information at hand without being able to await confirmation or a fuller picture. It also means that analysts are rarely in a position in which they can spend time trying to verify the information they have received. The need for real-time analysis has only been increased by the flow of raw intelligence to Ministerial offices and policy departments – a development that is likely to be permanent given Ministerial appetites for intelligence and the collection agencies’ interest in expanding their bureaucratic profile and customer base – as Ministerial offices and policy departments become panicked by incoming intelligence and demand immediate analysis of its credibility.

The sheer volume of intelligence on transnational issues poses its own challenges. As analysts become increasingly tied to watching and digesting the intelligence “take”, there is a real danger that they will begin to think that the patterns emerging in the covert intelligence constitute the whole picture, when in reality covert intelligence can only provide a partial picture provided by the sources collection agencies are able to access, recruit and exploit. There is an attendant danger in “fetishising” secret intelligence – thinking that covert information is more valuable than other information, and that if there’s no secret intelligence on a subject, the subject has ceased activities or no longer exists. Yet another danger is that the flood of intelligence begins to crowd out analysis at the expense of mere description of what’s coming in.

Because analysing transnational intelligence is more labour-intensive than analysing most other types of intelligence, it raises a whole set of challenges for the management and leadership of intelligence agencies. If a moderately-sized team of generalists is chosen to cover the transnational patch, an easy ability to provide overview assessments of the problem comes at the price of being able to follow the flood of intelligence in adequate detail. If large numbers of people and resources are thrown at the issues, detailed coverage comes at the price of trying to co-ordinate an overall view from the conclusions of hundreds of experts.

In analysing transnational intelligence, we find ourselves in an asymmetric contest. For terrorists and criminals in decentralised networks, every problem is local and dealt with locally, whereas the intelligence effort is required to try to grasp the entire problem. Transnational intelligence analysis is required not only to report on strategic trends in various transnational threats, but is also being drawn into tactical analysis geared towards enforcement operations. This is a task that traditional analytical agencies are not set up to do, and nor are they adequately linked into enforcement agencies to be able to play this role effectively. Tactical analysis is also required by intelligence collecting agencies for further tasking: transnational targets move so fast that collection agencies need real-time and precise tasking that is often beyond the capacities and resources of

analytical agencies. There are two apparent responses to these pressures: either the fusing of collection, analysis and enforcement in specialist centres each devoted to a transnational issue; or the development of tactical-operational analysis cells that sit between strategic analysis bodies and the collectors.

Ways Forward

The analysis of transnational threat intelligence will be a service that our governments require from intelligence agencies for the foreseeable future. It is a task that requires at least part of each intelligence agency periodically to detach itself from the day-to-day press of evaluating the flow of current intelligence and reporting on it, so that it can begin to build up a series of thematic concepts that can serve as analytical guideposts to the analysis of transnational issues. It has struck me how many commonalities there are among the various transnational issues with which we are currently concerned. We need to focus on certain themes – the logic of different network structures, how networks respond to pressure, modes of transmission of tactics and methods, the usefulness of different forms of governance for various transnational actors – and work to deepen our conceptual knowledge on them and use this to strengthen our analytical techniques and develop better-targeted collection management regimes. There is much to be gained from co-operation between intelligence agencies and with academics and other specialists. Also, as I mentioned above, from increasing our interactions with police and criminal intelligence organisations. This will provide, over time, the conceptual ballast that is already used by long-established country and thematic specialists in intelligence agencies, and help us better come to grips with the fast-evolving world of transnational issues.

Adapting to the Analysis of Transnational Threats. Challenges for a Small Intelligence Service

*Christian Jenny**

Introduction – A Changing World

In the 15 years since the fall of the Berlin Wall, the world has considerably changed: Transnational forces *are* shaping today's globalized world more than ever. Today transnational threats are truly global as "9/11" and the actors behind al-Qa'ida demonstrate – as if that was necessary. According to the definition of my service, "transnational threats" comprise the proliferation of weapons of mass destruction, terrorism and organized crime – often considered to be "new" threats, although these are not really new phenomena. But today, their transnational dimensions are much more important than they were previously. Climate change, environmental degradation or the population growth and migration do not, however, figure on our radar as transnational threats – rather as transnational challenges.

We all live in the same world although we might perceive it and the opportunities, risks and threats "out there" differently. Obviously, where you stand depends on where you sit or who you are: Switzerland is a small country with "soft" national interests and a reserved foreign and security policy. What is true for the country also applies to its foreign intelligence service – the Swiss Strategic Intelligence Service: Swiss SIS is a small service. Its personnel numbers and finances thus are comparatively limited. Obviously, no organization disposes of too much of both and every organization faces the constant challenge of making ends meet, but compared to larger intelligence services the difference in size is a matter of scales: The US military supposedly has more musicians than the CIA has analysts – the same is true in the case of Switzerland, although, to start with, the number of musicians in the Swiss Armed Forces is much smaller than that of the US military.

* Mr. Christian Jenny is Head of the Proliferation/Terrorism Analysis Branch, Swiss Strategic Intelligence Service (SIS).

Adapting to the Analytical Challenges Posed by Transnational Threats

In adapting to the analytical challenges posed by transnational threats, Swiss SIS has faced the challenges of:

- finding and defining a “new enemy”;
- making ends meet, i.e. simultaneously describing “mysteries” and solving “puzzles”;
- managing the ever-rising volume of available information;
- organizing ourselves properly;
- increasing cooperation;
- finding and retaining the right people to do the job.

Finding and Defining a “New Enemy”

Whereas my – and for that matter our – predecessors during the Cold War faced a single, albeit large and daunting target: the Soviet Union – today, my colleagues and I face a multitude of smaller, but more imminent targets. My predecessors had to convince their bosses that proliferation and terrorism were relevant and thus “worth” looking at. Starting out with a “strategic” outlook, our approach to these threats has over the past ten years become increasingly “operational.” One thing, though, has remained the same: establishing the intentions of the actors behind the threats.

The actors behind the transnational threats specified above – proliferation and terrorism – vary in their characteristics:

- they can range from single actors (lone crazy) to groups (terrorists or procurement networks);
- a group actor will be organized in a loose and constantly changing network (such as al-Qa’ida) or in a more hierarchical manner (“classical” terrorist groups, for example ETA);
- it can be a non-state (terrorist group) or a state actor (a procurement agent);
- the actor may act covertly (terrorist group) or (semi-)openly (a procurement agent), or both at different times, depending on the situation;
- an actor at the radical fringes will probably pursue radical aims (furthering “Armageddon”) and might be inclined to use radical means in order to cause a commensurate impact (terrorist use of CBRN).

Mysteries vs. Puzzles – Making Ends Meet

Intelligence services have two main analytical tasks: *illuminating mysteries* and *solving puzzles* – to paraphrase Joseph Nye and Gregory Treverton. In other words: describing an increasingly complex world to decision-makers and providing the competent authorities with operational support in the framework of export controls and counter terrorism – to speak of my own responsibilities. De-

scribing mysteries and solving puzzles, however, are two separate tasks, requiring the analysts to use different information and answer different questions. Some services clearly distinguish between the two tasks in assigning them to different analysts and/or units. It has been suggested to break-up existing large intelligence organizations into smaller, leaner and meaner organizations that can “cater” more specifically to the needs of their respective clients.

As my team is fairly small, we cannot fully concentrate on either strategic or operational analysis. While “smallness” has its advantages, this leaves us constantly juggling between the varying demands posed by informing the decision-maker on the one hand and by supporting law-enforcement on the other hand – a dilemma obviously reinforced by the nature of the transnational threats. Namely in times of crises – as only too recently with “3/11” – this regularly forces us to toe the very thin line between doing the desirable vs. doing the possible and nevertheless remaining pertinent also for the decision-makers, as it is them who frame the framework within which we then can support the relevant authorities with operational intelligence. The decision-makers’ generally limited attention span forces us to generate “sound-bite intelligence” – as we called it in my breakout group – while nevertheless basing this on solid analysis.

Managing the Ever-Rising Volume of Available Information

On the one hand, the information revolution of the last decade has led to an inflation of the amount of information available, both from open and classified sources. On the other hand, combining OSINT and classified information can prove very valuable. The plethora of information requires a careful selection of the information made available to analysts. Knowledge management is thus rapidly gaining importance for analysts and analytic units of intelligence services.

In the case of Swiss SIS, the ever-rising volume of available information remains to be matched by an increase in the number of analysts. Nevertheless, facing today’s severe financial constraints, we consider it an important achievement that we have not been forced to downsize. Knowledge management has thus become critical and we are in the process of finding and implementing solutions that should help the analysts with their work within the next three to four years – a fairly long period of time in terms of transnational threats.

Organizational Challenges

In analysing and fighting transnational threats, intelligence services – classical bureaucratic organizations – are increasingly facing loose and ever adapting networks. This fluidity can probably hardly ever be matched by governments on an organizational level. One way to address this gap, though, is by limiting the compartmentalization of information to an absolute minimum and to encourage

the sharing of information both intra-service and beyond, inter alia including tapping outside expertise.

In Swiss SIS we have and we are encouraging the exchange between CP (counterproliferation) and CT (counterterrorism) analysts and their regional and technical counterparts. As this is not enough, we are increasing contacts between analysts and source managers (case officers and source managers); we have, however, not yet gone as far as other services in bringing the respective analysts and case officers together in thematic or regional units – rather, we have chosen to create “virtual” units by integrating the respective processes to a certain degree.

Increasing Cooperation

In facing transnational threats, sharing information goes beyond one’s own organization: Information and analysis ought to be exchanged both within the intra-governmental and the inter-governmental frameworks (including international organizations). Intra-governmentally, this applies to foreign intelligence and domestic intelligence services, law-enforcement authorities as well as policy-supporting bodies on the more operational level. Inter-governmentally, the same bodies should be found involved in this exchange of information and analysis. Ultimately, this will have to happen in a reflected and efficient manner and in keeping the justified needs of source protection in mind. Nevertheless, intelligence could certainly be inspired to a certain degree by the level of exchange among law enforcement circles – especially when we have in mind that in fighting terrorists, law enforcement is a crucial partner.

Within the Swiss government, Swiss SIS is the “new kid on the block” in dealing with transnational threats – previously only the domestic intelligence service dealt with terrorism or the proliferation of WMD. The Swiss system has improved over the last years, but there remains room for even further improvement, mainly because the institutional anchorage and roles of the respective services have not yet found their way into everybody’s head or daily actions. As Switzerland finds itself largely outside of multilateral intelligence frameworks, Swiss SIS must rely on bilateral relations with partner services. This has its disadvantages but also its advantages. Cooperation with far larger partner services can sometimes be a major challenge as the example of the Global War on Terrorism demonstrates: receiving significant amounts of information, integrating them into our databases, analyzing this information and responding in due time to requests for information is often challenging – especially when keeping the nature of the threat in mind!

Finding and Retaining the Right People to do the Job

The analysis of transnational threats requires a “new” generation of analysts: scientists, financial experts and regional or language experts with expertise in ar-

was previously not required. Moreover, in an increasingly integrated world and work environment, today's analysts need both deeper and wider thematic skills than was previously the case. This is also reflected in the increasingly diverse experiences and skills needed by their managers.

For Swiss SIS this has proven to be a challenge, as we can only recruit in limited numbers and the process of adapting to these different needs has proven to be time-consuming. Compared to other services, the individual analyst who covers a wide field of analysis gains in relative importance. Only time will show, whether we have been able to recruit the right people, retain them and develop their carriers, allowing them to do their job.

Conclusions

I would like to conclude by drawing the following general observations:

- Analysis alone is not enough to face transnational threats, combating is the key to dealing with them. This entails that our analysis must be “actionable” both on the strategic and on the operational level.

- Fighting transnational threats leads to a blurring of the distinction between foreign and domestic and between intelligence and law-enforcement – governments will have to find ways to further increase the cooperation between foreign and domestic intelligence services, as well as between these and law-enforcement authorities (both nationally and internationally).

- As the actors behind transnational threats are constantly adapting, so will intelligence and law-enforcement services face the challenge of continuously adjusting themselves to their opponents' *modus operandi* – i.e. finding ways to efficiently fight loose and ever-changing networks both nationally, within the classical bureaucratic framework, and internationally.

The Buddha as an Intelligence Analyst

*David Chuter**

In this paper, I look at some of the ways in which the ways in which we understand the world cause us problems when we try to analyse it. Most problems of analysis, and most “intelligence failures” – certainly today – take place at the conceptual level rather than the factual one. We may not have enough facts of course (and more might be helpful), but too often facts come to resemble pieces of Lego when we do not know what model it is we are trying to make. There is a good principle philosophers use, which is that you cannot arrive at a true conclusion from false premises, and it is these premises with which I am largely concerned here. I begin by looking at some concepts about the use and purposes of intelligence; I go on to look at what it should illuminate, and I conclude by looking at obstacles to doing all this productively.

We can define intelligence as the acquisition of information from another individual or group that they do not want you to have, and without them realising that you have it. It is therefore the *mechanism* by which intelligence is collected which sets it apart, and this helpfully recalls that intelligence (in the English sense) is just a special case of information. Governments run on information, as cars run on petrol, and they need it to make present decisions and to attempt to prepare against future problems. Much information has always been openly available, and today this is truer than ever. But of course there are major problems with the reliability of much open source material, and it is unwise to rely on its accuracy. It is of most value when it provides a mechanism (generally through the Internet) for quickly discovering material of known types such as government statements or newspaper reports. Indeed, the Internet is increasingly coming to resemble the Library of Babel, in Borges’s story of that name – an infinite space where any conceivable book can be found, confirming or disproving any hypothesis.

Better understood are the usual processes by which governments exchange

* Dr. David Chuter is Senior Research Associate, Center for Defense Studies, London.

information with each other, about themselves or other governments, as well as the more sensitive relations which governments have with each other where their interests overlap. Much information is also available by and through international organisations of various types. Individuals in governments may also pass to friends from other countries information on a privileged basis, sometimes to ease bilateral relations along, at other times because they are worried about the policies which their government is pursuing.

Nonetheless, there are obviously circumstances where what governments need to know exceeds all that is available from these sources, and that is where intelligence comes in. It is likely to be most used in two sorts of cases. The first is where the *nature* of the target makes it difficult to penetrate by normal means. Any closed society, from North Korea to the Catholic Church to a multinational corporation to the Tamil Mafia, comes under this heading. Groups or societies with closed and secretive structures, speaking minority languages, and with ambiguous feelings about the outside world, are difficult to engage with through conventional diplomatic means even if (as in the case of organised crime) that is what you actually want to do. Secondly, there are *subjects* which, even in the most faultlessly open society, do not find their way into the open media unassisted. Governments do not usually give press conferences to announce that a major change in trade policy is being contemplated, or that a Minister is under investigation as a security risk, or that the Chief of Defence is losing his credibility with the President and may well be replaced.

The modern origins of intelligence can be found in a pre-democratic age, where for the first time the security of states depended on keeping secret their military co-operation and mobilisation plans and their procurement programmes. It was originally the task of the intelligence services to discover these military plans.¹ Broadly, this mode of thinking continued for a century or more until the end of the Cold War. But although it is not without application in some areas of the world even today (the Korean peninsula, for example), it is out of date today inasmuch as it assumes that all of the really important things we might need to know are hidden. Often, this is not the case.

Whilst the *details* of, say, Russian intentions towards their Near Abroad will no doubt still be hidden, even governments have adopted a more open and somewhat calmer means of dealing with crises than their Cold War habit of chasing each other around a firework factory with lighted matches. So it would have been pointless, for example, for a Middle Eastern intelligence organisation to have wasted a lot of time and money covertly collecting on US intentions to-

¹ Hence the use (even today) of *Renseignement militaire* in Francophone countries to render “intelligence.” The latter, incidentally, generally only meant “information” until at least the 18th Century. English is relatively unusual in having separate words to distinguish information from the stuff spies look for.

wards Iraq in 2002/3, since all the information needed to make a sound prediction had been in the public domain for some years. Similarly, for many non-state actors, concealment of their objectives would be counter-productive. Such groups have, in modern times, sought to use violence to achieve political objectives of various sorts, and have usually loudly announced what these objectives are. Sometimes these objectives have been minimalist and largely political, such as the resistance organisations in occupied Europe in the Second World War which could do little beyond the symbolic level. Sometimes there have been attempts to raise the military and political costs of an occupation to unsustainable levels, as with the Afghan *mujāhidīn*, or various Palestinian groups today. And increasingly non-state actors now try to apply force directly to Western states in an attempt to affect their foreign policies. Since al-Qa'ida (to take an example which is becoming tedious) wishes to influence the US towards a different policy in the Middle East, there is little point in concealing what that policy (withdrawal from the Gulf and a changed attitude towards the Jewish-Palestinian conflict) actually is: it would be perverse to do so.

However, we should not assume that transparency of objective is necessarily the end of the story. Not only will agencies, understandably, still think they should devote efforts to things like personnel and methods, which are likely to be less transparent, but there are likely to be powerful political obstacles to recognising the objectives of non-state actors, no matter how easy it may be. I shall have more to say about this later: here, it is enough to remark that recognition that the objectives of non-state actors are as they are described can prove awkward, because it can imply that there is a rational case to be made against the policies of one's own state. Far better to write off such groups as fanatics without a plan of any kind, or servants of a vast conspiracy. The epitome of such an approach is probably that adopted by the South African state in the 1980s. Unable to accept as true the professed objectives of the ANC (broadly, the end of apartheid and a multi-racial democracy), they constructed for themselves a lurid fantasy in which the ANC were precursors of a huge Soviet-Cuban armoured force which would sweep down the west coast of Africa and massacre most of the whites, driving the remnants into the sea.

A related and consequent question is what it is that we should be looking to intelligence actually to tell us. Broadly, we can distinguish three potential outputs from intelligence into the policy-making process. First, there is *information*, by which is meant just undifferentiated data – stuff out there. Second, there is *knowledge*, which is essentially information combined with judgement and collateral material, but perhaps lacking a context. Finally, there is *understanding*, which supplies a context and tries to make sense of the whole. In the Cold War, the West, at least, tended to concentrate on the first and second of these. It was thought (erroneously as we now know) that we understood the Soviet Union and its objectives, and so information (such as codes and ciphers or exercise schedules) and

knowledge (such as war plans) tended to get priority. Western failure to understand the Soviet Union was not because of a lack of knowledge or information (perhaps there was too much), but rather the inability to seek a true understanding of context, without which information and knowledge made little sense.

There is even less reason now to believe that our problems can be solved by information and knowledge on their own. Of course at one level, say in the quotidian struggle against proliferation, more detailed information will be necessary and useful. For some time to come, there will be those who are professionally excited by the news that X has sold a consignment of Uranium Hexafluoride to Y for onward shipment to country Z. But the really big questions of the present and the future are not going to be illuminated this way, and there is no reason to suppose that *any* quantitative increases in information and knowledge of which we can conceive will automatically bring about a qualitative change in our understanding. Thus, the humming sound of people speed-reading the Koran has abated in recent months, not only because of a recognition that Islam, as such, had relatively little to do with the events of 11 September 2001, but more because of a further recognition that attempting to find convincing explanations of behaviour in a body of doctrine is a fool's errand. In the end, any large text can be made to yield any reading you want, with enough determination.

If this seems controversial, consider an example closer to the homes of many of us – the Old Testament of the Christian Bible. A Martian political analyst would have, as information, the bloodthirsty injunctions to destruction and genocide in the Book of Deuteronomy. It is a matter of knowledge that the history of ancient Israel, as of much of Christendom, is extremely bloody, and also that a number of Western leaders have claimed, and some claim even now, to be divinely guided in what they do. But our Martian, if it was sensible, would surely conclude that attempting to draw simple conclusions about the behaviour of contemporary governments was a hazardous enterprise, given the thousands of years of polemic on such issues as whether, for example, Christianity or Judaism are pacifist or militarist religions.

The really intractable and difficult issues of today's world demand understanding, rather than just information or knowledge. There is nothing new in this, but it is rather more obvious today, with the comfort blanket of Cold War analysis ripped cruelly from us, that the world has always been a more complex place than we had realised. This need for understanding is a far more ambitious target for an analytical organisation than any amount of increased knowledge or information. It requires a cadre of people, per subject, who are familiar with languages and cultures, have lived in one or more relevant countries and understand how they think. Such people can be found in large analytical organisations, but there are probably never enough of them, and in principle governments need to look outside their own ranks as well, where many of the genuine experts will be found. Yet, the use of such experts is not as easy as might be thought.

Some of the reasons are obvious: there are few subjects on which a genuine academic consensus can be said to exist. Whilst there will usually be a fairly solid foundation of agreed interpretation (albeit often with variations of emphasis), academia invites – almost requires – disputation and debate on more topical issues. So it is quite possible that canvassing a group of experts will do no more than reproduce differences of analysis which exist internally already. Moreover, there will be an obvious temptation for governments to invite inside the tent academics who they know have supportive views, and for academics to unconsciously adapt their views to what they think government wants to hear. So outside involvement is not a panacea: but it remains true that governments are henceforth going to have to pay relatively much more attention to understanding than was the case in the past, and that analytical organisations, even large ones, are going increasingly to have to look outside for help and assistance.

If it is accepted, based on the argument thus far, that governments require primarily understanding of complex problems to fill gaps in their knowledge, then we need to look at why, in practice, this understanding is often difficult to achieve. The essential difficulty is that no analytical problem ever feels as though it is encountered for the first time. Rather, in considering a problem, we ask not *What is Going on Here?* but rather, *What Pre-existing Model does this Situation Most Resemble?* Models drawn from the past (or more usually from fanciful interpretations of the past) tell us how we must respond to new and potentially confusing situations.² These explanatory paradigms, of course, do not arise by accident or through careful analysis. They are usually highly political constructs, and, as we shall see, the ability to enforce a paradigm on the rest of the world, by violence and intimidation, has historically been a very important advantage for the West, and one which may now be about to attenuate. These models, powerful and useful as they are, have to be recognised and jettisoned before any useful analysis can be done, but they remain very attractive, because of their simplifying and clarifying function. Debates about how to analyse a situation can very quickly descend into cliché, from which they may never be recovered. Some of these are *idées reçues*: the Dark Continent, Ethnic Hatreds, Ethnic Extremism, Religious Fanatics, Foreign Incitement. Some are thematic: We must learn the lessons of; we must not repeat the mistakes of; we thought this would happen; we warned about the effects of such a policy. Clearly, in any large bureaucracy, interest groups will compete to define an analytical problem both

² I have said quite a lot about the abuse of the Munich myth in David Chuter, “Munich, or the Blood of Others,” in Cyril Buffet and Beatrice Heuser (eds.) *Haunted by History: Myths in International Relations* (Providence: Berghahn Books, 1998). An interesting in depth study of one recent episode is Roland Paris, “Kosovo and the Metaphor War,” *Political Science Quarterly*, Volume 117, Number 3 (2002).

in terms of their previous analytical positions, and also in terms of their suitability to control the new issue.

Some of these obstacles to understanding are general and important enough to warrant more extended treatment. The first example is the Really Big Conspiracy, or analysis as applied paranoia. Because paranoia provides a complete explanation of any situation, it is a popular mode of analysis. In addition, it is also very flattering, since your state, or ethnic or religious group, is obviously important enough to be the target of this monstrous conspiracy. And finally it is obscurely comforting: if it is disturbing to learn that everything is connected, it is far more disturbing to learn that nothing is.

So paranoid analysis is widespread, and intelligence organisations – for whom paranoia is a professional hazard – are especially likely to practice it. But there are degrees. Paranoid analysis often arises at times of crisis, especially in societies (the US is a convenient example), which are caught between the demands of modernisation and those of tradition, and where organised religion is a powerful force. Religion – or at least monotheism – seems to be a major factor in promoting paranoid analysis (God, we recall, is the original conspiracy theory), because of its tendency towards a simplistic, dualistic, world view. He that is not with me is against me, as Jesus of Nazareth said, and others have since repeated, and by extension all those that are not with me are part of a huge conspiracy against me. So in the United States, tens of millions of books are sold positing huge conspiracies organised by Satan with the assistance of the United Nations, only thwarted at the last moment by the literal Second Coming of Christ. It would be naïve to suppose that such beliefs leave no trace at all in the more sober business of intelligence analysis.³ Indeed, during the Cold War US Intelligence was greatly hindered by the activities of James Jesus (now there's a middle name) Angleton of the CIA, who took seriously the reports of defectors like Lyalin, that there was a huge conspiracy to deceive the West about the Sino-Soviet split, which, according to Lyalin, never happened. Another area where paranoid explanations of the world are influential is the Middle East, although here, the conspiracy is naturally a Christian-Zionist one, aimed at attacking and occupying Arab countries and wiping out Islam.

A good test for identifying paranoid analytical schemes is the presence of the word “International” followed by an abstract noun. So today International Terrorism is popular in some quarters as an analytical device. Its origins, conceptually, obviously lie with the now defunct International Communism of the twentieth century, which was known before that as International Socialism and international agitation for Democracy – all dastardly enemies to be fought. In turn, these were secularised versions of the International Jewish-Masonic con-

³ The classic analysis is Richard Hofstadter, *The Paranoid Style in American Politics*, (Harvard: Harvard University Press, 1964).

spiracy (bent on our destruction, etc.) and had their ultimate source in the International Satanic Conspiracy, whose origins were in medieval times but which acquired another lease of life with the religious schisms of the Reformation. To complicate things, the ideas above do not always follow each other sequentially: rather (as in the US today) many of these ideas coexist or are reinvented over time.

The problem, of course, is that some conspiracies do actually exist, and in a complex world there are very often linkages between non-state actors, just as there are states. Just as with states, such linkages often do not mean a great deal. Yet an analyst commissioned to produce a survey of non-state groups (no doubt referred to as “terrorists”) and the linkages between them, may well, simply through a list and indications of occasional linkages and occasional cooperation, produce something which supports and reinforces a paranoid analysis.

An analytical error which reinforces these problems is the tendency to examine opposition to one’s policies, whether peaceful or violent, in terms of what opponents are apparently for, rather than what they are obviously against. This is a constant temptation, since it is very hard for us to accept that the policies of our state or our group are wrong, still less that they have provoked, and perhaps merit, violent opposition. Much easier to assume that groups, especially violent ones, are actually trying to impose an agenda on us. Yet these assumptions – a form of paranoid analysis again – are contradicted by history, as well as our everyday experience, both of which suggest that human beings are far more likely to mobilise against a perceived wrong than they are in favour of a cause, no matter how attractive.

So in occupied France, during the Second World War, much of the early armed opposition to the Germans came from the *Franc-tireurs et partisans*, (the FTP), closely linked to the Communist Party. This was partly because the FTP members had a special ideological loathing for the Nazis, and partly also because their existence, even in peacetime, had been a semi-clandestine one. But in practice, the main reason for their activities was simple patriotism, and disgust with the collaborationist Vichy authorities. Other groups of wildly different political persuasions joined the resistance forces also, but what linked them was a shared desire to evict the Germans, or at least maintain national respect by showing that not all French people were collaborators. This did not stop the Germans and their Vichy allies dismissing the resistance groups as “communist terrorists” attempting to impose a reign of terror on France. Nor did it stop the British and Americans panicking about a possible Communist coup after liberation, and a bloody civil war. Nothing of the kind happened of course.

As a rule, opposition to an authority, a regime or an invader tends to be expressed in ideas which are fashionable or with which the opponent is at least familiar. Until the latter part of the twentieth century, a Marxist vocabulary was in vogue, and groups often used this to express dissent. The urban guerrillas of the

1970s, like the Red Brigades in Italy and the Red Army Faction in Germany, were in practice protesting against the lies and equivocation of their parents' generation, as well as the inadequate cleansing of their societies because of the pressures of the war against communism. The African National Congress, at the same time, was essentially a collection of decent-minded individuals horrified by the realities of apartheid. (In retrospect, it is surprising, not that so many educated whites opposed apartheid, but that so few did). But the regime, and its supporters in the West, chose instead to take the slightly Marxist and anti-colonialist rhetoric of the ANC and confuse it with substance. This enabled them, of course, to avoid asking why even some educated whites opposed a system which gave them such advantages.

A related obstacle to understanding is the idea of the Implacable Enemy. This is the enemy bent on our Destruction, with whom No Compromise is Possible, and to whom the least weakness or sign of accommodation is a kind of treason. The origins of this kind of thinking lie, pretty clearly, in fear. This is not necessarily fear of a stronger opponent: rather, it can be fear of one's own weakness and vulnerability, or simply fear of a society or ideology that one does not understand and cannot control (Islam in the obvious example). This habit of thinking is convenient and attractive in several ways. If an enemy is bent on our destruction, then there is obviously no point in attempting to understand, let alone reason with, them. Extermination is the only possible option, and faint-hearts who believe that non-military solutions are possible can be conveniently stigmatised as traitors. An undue attachment to morality, the laws of war or simple human decency itself becomes a kind of treason, since it objectively benefits those whose only objective is our destruction. It is not surprising that such ideas lead to atrocity and even genocide. It was in this spirit that the apartheid regime in South Africa defended itself, and in this spirit also that the *Wehrmacht* invaded Russia in 1941, specifically instructing its troops that the Geneva Convention did not apply to enemy forces it would encounter.⁴

A third analytical danger is the temptation to misunderstand the nature of risk. Analytical organisations have really got to stop talking in terms of Threats – of which there are few if any against the West today – but rather of Risks. The question is not “What are the threats to our interests from that group or that area?” but rather, “What risks do we run if we continue our policy in that area or change it to the one we are now considering?” Analytical organisations, in

⁴ See for example Hans-Adolf Jacobsen, “The *Kommissarbefehl* and Mass Executions of Soviet Russian Prisoners of War” in Jacobsen, Hans Buchheim and Martin Broszat, *Anatomy of the SS State* (London: Collins, 1966), and Omer Bartov, *Hitler's Army* (Oxford: Oxford University Press, 1992), pp. 83-89. The *Kommissarbefehl* was the notorious order for the German Army to kill all the Red Army political commissars it captured. In practice, this soon came to mean the murder of anyone who held a post of responsibility in the Communist Party at all.

other words, have an obligation to look into the future and attempt to set out clearly what dangers may flow from the adoption of a particular policy. This is complicated by the general human inability to gauge risk very well. As individuals, we tell questioners that we are much more worried about dying in air crashes than in car accidents; that we are more afraid of being killed in a bomb attack than being struck by lightning. A sensationalist media and a sensationalist political culture naturally confuse the issue further.⁵ In these circumstances, and especially in a democracy, it is probably inescapable that analytical organisations will be obliged to divert resources to studying the latest fashionable threat, as opposed to longer-term and more serious risks. And bureaucratic pressures to secure funding tend to add to these pressures. But any reputable analytical organisation has to resist these pressures as far as it can, if it is actually to do its job.

The biggest single obstacle to a correct analysis of risks, however, is the set of assumptions which surround the legitimacy of the use of violence. All groups – states, non-state actors, ethnic, racial and religious entities – in practice believe that their interests take priority, and that any violence to defend their interests is automatically acceptable, whereas any violence against them is automatically wrong. In theory, of course, this should not be so. There is a corpus of law going back more than a century which attempts to regulate behaviour in armed conflict, and it is asserted that there is something called the “conscience of humanity” which is collectively shocked in an objective fashion by certain events. In practice, this seldom happens: we make excuses for evils committed by groups we support, as we dismiss such excuses by groups we dislike. The distinction between good and evil acts tends to be a political rather than a legal one. I was giving a lecture on these issues at our Air Force College a few years ago, explaining why certain attractive military options were not acceptable, when a worried officer raised his hand. Surely, went the question, these limitations don’t apply when your country is in danger of annihilation? One imagines that such questions are probably asked in every military college around the world, reflecting what happens when ethnic or other group solidarity encounters the international legal norm that it is better to suffer casualties, or even lose a war, than to fight unfairly.

A constant theme of such thinking is the right to disproportionate revenge. The Nuremberg prosecutor Telford Taylor relates that, when he was in Washington in the Christmas of 1944-5, even New Deal Democrats (relatively liberal, therefore, by American standards) were demanding that all members of the SS (several million at the narrowest definition) be shot out of hand in revenge for the murder of about 60 US soldiers who had been shot after surrendering to the

⁵ See for example Barry Glassner, *The Culture of Fear: Why Americans are Afraid of the Wrong Things* (New York: Basic Books, 1999).

SS.⁶ Similarly, the massacres at Srebrenica in Bosnia in 1995 apparently resulted from the determination of Mladic, commander of the Bosnian Serb Army, to punish everyone who *might* have been involved in the mass killings of Serb villagers in the surrounding area in recent years.⁷

We feel justified in this disproportionate revenge because we do not see the rights of other groups as equally important as the rights we have. We regard our own violence as legitimate, and the violence of others as illegitimate. Now of course it is practically impossible for every group to have more rights than every other group. As a result, it is groups which have political or military dominance, in an area or globally, which are able to impose their own relativist concepts of rights upon others. Sometimes (as in the United States) there are metaphorical battles between groups to establish the pre-eminence of their rights over others. Sometimes, as in the Balkans, there are real battles for such purposes. But for much of the last 500 years, it is the West, primarily white colonial powers (including the US), which has been able to impose its view of the legitimacy of violence upon others.

According to this view, violence against Westerners, or Western interests, or those supported by the West, is always wrong. Conversely, violence *by* the West is in principle always right. Now of course there is nothing unusual about these precepts: what is unusual is the degree of success the West has had (until recently, anyway) in enforcing them on the rest of the world. So non-westerners are required to accept, in effect, that the West has rights that they do not, and is justified in using violence against them, where they are not justified in using violence against the West. Whilst political elites in non-western countries are often prepared at least to pay lip-service to such ideas (and will generally be honoured with the title of “moderate”), ordinary people are seldom so indulgent, and their spokesmen will therefore be dismissed as “extremists”. One consequence of this, as we shall see, is that analysts very often hopelessly overestimate the degree of actual support for Western policies and precepts in other countries, and so give bad advice.

An example is the so-called Mau-Mau campaign for independence in Kenya. Only trivial numbers of whites actually died at the hands of the insurgents (probably fewer than died in traffic accidents), whereas thousands of blacks of all types were killed. But the issue is not just numbers: the handful of actual Mau-

⁶ See Telford Taylor, *The Anatomy of the Nuremberg Trials: A Personal Memoir* (London: Bloomsbury, 1993), p. 42.

⁷ It is not disputed that the Bosnian Serbs entered the town with the names of nearly 400 Muslims they believed were responsible for the massacres, but by that stage almost all the men of military age had fled. When they were eventually captured, little attempt seems to have been made to sort the innocent from those presumed guilty. I discuss the background to this incident, on the basis mainly of captured Bosnian Serb documents, in David Chuter, *War Crimes: Confronting Atrocity in the Modern World* (Boulder: Lynne Rienner, 2003), pp. 233-39.

Mau killings were resented, and portrayed as outbreaks of primitive sadistic black cruelty, because of the inherent illegitimacy of blacks using violence against whites. Reprisals (including the public execution of about 1000 blacks) by contrast were part of the natural order of things.

Sometimes the Western pre-emption of legitimate violence was expressed in terms of crude power-politics, but sometimes also in moral terms. Military punishment of lesser races (often including the slaughter of women and children) was defended as a requirement of the *mission civilatrice*, or the White Man's Burden. It was frequently compared to the firm chastisement of the loved child (at least in the days when chastisement of loved children was fashionable). But habits of thought persist, and today the West still expects those against whom it uses violence to concede that they deserved to be punished. Conversations with visitors to Belgrade after the 1999 NATO bombing revealed genuine puzzlement (shared by many media commentators) that the Serbs should *mind* being bombed. Why, it was asked, did they not understand that they were justly punished for the behaviour of their police in Kosovo?

This kind of thinking has led historically to disastrous misunderstandings where Western interests are involved. Throughout the colonial era, for example, it was an article of faith in Western capitals that colonial subjects understood and appreciated the benefits of their status. Because opposition (especially violent) to Western imperialism was seen as illegitimate in the West, the kind of normative thinking then prevalent assumed that it must be similarly marginal in the colonies themselves. Those violently resisting colonial rule, therefore, must be a small and unrepresentative minority within their own society. It was therefore possible to dismiss them as terrorists, thugs, murderers, psychopaths, and, of course, tools of international communism. The West was therefore serially surprised that, on examination, colonial subjects seemed to actually support the men of violence. The British government was certainly taken aback in the early 1970s, when an independent commission visiting the (then) Rhodesia reported that blacks, on the whole, did not favour a continuation of white minority rule, and indeed supported the liberation movements.⁸ But unreality persisted to the point that the West's assumption, before the first free elections in the new Zimbabwe, in 1980, was that Bishop Muzorewa, who had advocated accommodation with the white settlers, would triumph, and that the men of violence, principally Joshua Nkhomo and Robert Mugabe, would be sidelined. In practice, of course, the men of violence won by a landslide. Similarly, in South Africa in the 1980s, the apartheid regime, much of the white opposition and many Western states put their money on Chief Buthelezi as the moderate voice of black opinion, whose toleration for the white regime was believed to be widely shared. Few

⁸ Rhodesia: Report of the Commission on Rhodesian Opinion under the chairmanship of the right honourable Lord Pearce, London, HMSO, 1972.

thought that Mandela, the man of violence and the Usama bin Lādin of the 1980s, could expect to do well in a free election.⁹

Examples could be multiplied, and there are, of course, many similar situations today. The essential point is that other states, and other groups, in practice, seek to universalise the merits of the use of violence in their interests just as the West does, and can sometimes achieve this in small and local ways. Thus, the West has failed to understand the Balkans (as one reason among many) because it cannot realise that groups there take a similarly absolutist view of what violence is acceptable as we do. Western commentators have been surprised that people from various ethnic groups in the former Yugoslavia have been unwilling to hand over alleged major criminals for trial. “He was only protecting his people” is a cry without much apparent resonance in the West, but in fact it is exactly how we would behave. So the Bosnian Serb leader Radovan Karadzic, for all that he has been associated with some major crimes, is seen by his co-ethnics as a kind of Winston Churchill figure, an inspiring national leader at a time of crisis and danger. The killings at Srebrenica (which to be fair Karadzic probably knew nothing about) no more attenuate this view than Churchill’s (much greater) personal role in the bombing of Dresden. Our problem with such societies is not that they are different from us, but that they are the same.

It is equally possible, of course, for non-state actors to believe that their use of violence is appropriate and serves higher moral aims. So the resistance forces of occupied Europe, the anti-colonialist rebels, the ANC in South Africa, and the *mujāhidīn* in Afghanistan, all believed that what they were doing was justified and necessary, in spite of being dismissed as terrorists by the states with which they were in conflict. In those cases where violence was directed against the West, or Western interests, there was a corresponding Western inability to perceive that this violence was widely viewed as legitimate in the region, and so the West was permanently surprised when history went off in directions which it had no right to follow.

In the past, this did not matter so much. Non-state actors, in particular, could safely be marginalised and dealt with at arms length, secure in the knowledge that they could do nothing to harm the West. If necessary, they could simply be wiped out. An invasion or attack on a third world country, might, it is true, lead to a few shots being fired at an embassy somewhere, but that was regarded as acceptable. Western leaders enjoyed, in effect, total impunity from the consequences of their actions. The world was a giant video-game in which nothing had any consequences. Manifestly, this is not now the case. Indeed, there are signs that the sprites are fighting back: non-state actors are learning how to use

⁹ The ANC was officially listed as a terrorist group by the US government until at least the late 1980s. According to the South African *Sunday Independent* (10 August 2003) the US began to reconsider the status of Mandela and others as early as 2003.

violence on as large a scale as we do, and for purposes as wide-ranging as those we ourselves choose. In the future, moreover, they may enjoy the kind of impunity we ourselves do now. It is this component of self-confidence and organisation which is different. In the past, Algerian independence fighters could not then devastate Paris; now who knows? Indeed, one of the reasons for the glut of conspiracy theories which have surrounded the events of 11 September 2001 is the disbelief that Arabs were capable of anything as complex and difficult as what was actually achieved.

This recovery of confidence by the rest of the world, together with a willingness to use violence against the West and wide acceptance of its legitimacy may be new, but it is not occurring in isolation. For example, the Cancun WTO summit of 2003 – a kind of economic 11 September – demonstrated for the first time that non-western states could stand up to the West economically if they wanted to. They could have done so before, of course: what was missing was simply organisation and self-confidence. There are wider analogies as well. Thus, the Open Source software movement is now challenging the might of the (largely American) software corporations which have dominated computing for the last generation. But it does so, interestingly, on an essentially ideological basis. It pits long-term objectives, decentralised co-operation, and work for fun rather than money, against short-term greed for profits. It is winning, of course; not simply in terms of quality, but because it is slowly destroying the top-down, command-economy, profit-driven model to which software has historically been made.¹⁰ Another analogy is internet file-sharing. Until recently, a group of very rich and powerful media companies controlled how and when you could entertain yourself. That model – once again, top-down, command economy and profit-driven – is now dying, to be replaced by an altruistic and communitarian model. It is this paradigm conflict, rather than any fancied loss of profits, which drives the immoderate response of the media companies.

So we can see the changes in recent years as a move towards an Open Source model of violence, coordinated by peer-to-peer networks. Governments have responded as Microsoft has to Linux, and can expect to be approximately as successful. Governments will naturally behave in this way: they are, after all, members of the most exclusive closed shop in the world, and are desperate to defend their Weberian monopoly of legitimate organised violence. “Terrorism” is the one thing all governments can agree to combat (as all media companies can cooperate against file sharing), since it strikes at their very sense of legitimacy and threatens to shatter the rules of the exclusive club to which they belong.

But are there any reasons to think that the model of Western-dominated, state-legitimated violence is itself going to change? There are some reasons at least to

¹⁰ See for example, Glynn Moody, *Rebel Code: Linux and the Open Source Revolution*, revised edition (London: Penguin Books, 2002).

think that the current model is losing its power. Ultimately, ownership of the world's operating system is dependent on political, and therefore financial influence. Changes in political and security situations take longer to have an effect than purely economic changes, because they are less concrete, and also because there is an inbuilt drag while political patterns reconfigure themselves. Thus, in the aftermath of the Second World War, much of the world was in debt to the United States. This produced various patterns of political subordination which are still seen in some form today, albeit that the United States is now in debt to the rest of the world. Nonetheless, changes are afoot (the Cancun summit already referred to is one indication) and will continue and accelerate. The general consensus is that, compared to the present, in a generation the US will be relatively much weaker economically, Europe about the same, and Asia considerably stronger. It is not too much to suppose that in a generation the world's operating system will be largely Asian owned, and judgements about what use of violence is and is not legitimate will increasingly be made in Beijing. In any event, there will certainly be a stage – perhaps transitional – when different concepts of the legitimacy of violence co-exist, and Western ones may not have much support outside our own region. Coping with such a world will be an immense challenge for the West, and analysts should really start thinking about it now.

In addition, non-state actors will increasingly find it easier to pursue their objectives by force. This does not mean that the apocalyptic predictions of the media and others should be given more credibility than they deserve, but it does mean that a sensible and thoughtful non-state actor can easily inflict damage which is *proportional* to the political effect they wish to achieve. The greatest asymmetry the West is likely to face is asymmetry of objective: a group fighting to recover its national territory is, to put it simply, going to be ready to accept higher casualties and more damage than a Western invader, because they care more. Equally, a group seeking a Western change in Middle East policy would presumably care quite a lot about its objectives, whereas a Western government would only be prepared to tolerate a limited amount of violence before changing its mind. Indeed, a truly microscopic level of violence might be adequate. Consider assassination, for example: how many Western leaders are so attached to a foreign policy initiative that they are prepared to die for it?

We are not going to be able to understand this confusing new world unless we divest ourselves of our traditional assumptions and patterns of thought. Here, we might invoke the example of the Buddha. That name, for all that it is usually translated in flowery terms, really means only “the man who woke up.” The Buddha never claimed to be wiser or more knowledgeable than anyone else, only to have been given the power to see things as they really were. And intelligence agencies have the duty to try to see things as they really are as well, and to divest themselves of the received ideas about the world which, in Buddhist thinking, obstruct our view of reality. What Buddhists call *Samsara*, some times

translated as “Hell”, is the situation of living not for yourself but for others, and being trapped in patterns of thought and behaviour which you mistake for your own thoughts and desires. Analysis should be a process, at least in part, of divesting oneself of received ideas and telling decision-makers how it really is.

This is difficult, of course. Analysts are, thankfully, not a cadre of people entirely separate from the rest of government. Not only do they interact with officials from defence and foreign and interior ministries all the time, but they often have the same background and education as well. This is good, but it does mean that analysts are always tempted to identify with the policies and expectations of their governments, and may be slow to point out where assumptions are misguided or policies are failing. It would take a brave – perhaps a suicidal – Chief of Intelligence to approach a national leader and say “Mr President” (or “Mr Prime Minister”) “intelligence suggests that our policies stink and everybody hates us.” But ultimately heads of analytical organisations do have that responsibility.

If it is not discharged, two very practical dangers arise. Firstly, the acceptability of Western ideas abroad will often be over-estimated. Western culture is very solipsistic, and it is also widely distributed at a superficial level. A fortnight’s tour of Asia, staying in English-speaking hotels, deriving local news from the *Wall Street Journal Asia* and CNN, meeting English-speaking politicians and businessmen, could actually delude the unwary into believing that they have been somewhere and learned something. Because our governments overwhelmingly speak to those who tell us what we want to hear, there is an obligation on analytical organisations to make the voices telling us what we don’t want to hear equally audible. Otherwise the West will, as it has so many times in the past, delude itself about the popularity of its ideas and go into a sulk when they are eventually not accepted.

Secondly, and as a consequence, there is the need for accurate prediction of the results of Western activities, including political and military reactions. Whatever we may feel about the justice of our own cause, there is no reason of principle to assume that people from other cultures will feel the same, any more than we would automatically approve of what we do. It really is about time that we stopped being so surprised all the time when our interventions are greeted with anger and fury and even violence, and when this violence is ultimately turned against us.

The decay of the Western monopoly of sanctified violence will be an uncomfortable process. It may lead in time to another monopoly, which we will not control and will certainly not enjoy, or simply to a set of contending aspirational monopolists, operating probably at regional level. In any event, the West will probably have to get used to living in the kind of fear and insecurity which the rest of the world has always had to put up with. We had better start thinking about these things now.

Tools, Techniques and Teams for Analysis

*Gilman Louie**

I come from a gaming background, so I'm a journeyman in intelligence. Although I have been here for about five years, I'm not an expert. Sometimes I think the Agency actually invited me in because I don't know any better.

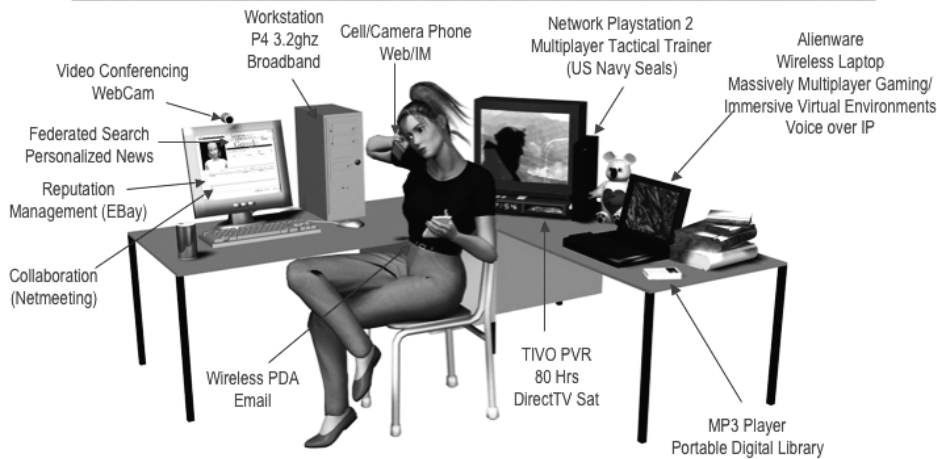
My experience in gaming can help shed some light on the challenges facing the Intelligence Community. Too often we resort to technology to solve problems without a basic understanding of our own abilities or the complexities of the problems we're up against. Any skilled computer game writer will tell you that it's impossible to write a quality game without understanding social dynamics of the system. Consider the teams who wrote the Big Blue chess computer program that took on Kasparov, and the challenges they confronted in order to defeat him. Some of the common rationalizations I hear are: "We don't have the right work force" or, "there's too much information out there" or, "We can't handle this, we're in information overload."

When we go home, take a look at our kids and say "what the heck's going on with my teenager?" She is on fifteen different devices at the same time – cell phone, IM, email – all while watching television. How could anyone possibly learn anything in that kind of environment? Teachers may complain about attention deficit disorders in the classroom, but this is the archetypal teenager, the information warrior of today. The figure below shows the typical tools of today's teenagers: laptop computer, broadband access, Tivo recorder, Playstation, and a can of coke for a little stimulus along the way.

There's an assumption that this is a prototypical teenager in the United States. In actuality, this is more typical of Korean, German, or Israeli teenagers, where broadband and wireless use rates actually exceed those of the United States. There are two sides to this coin: on the one hand it presents an opportunity to catch up; on the other hand there is the threat that we will be marginalized unless we get on board.

* Mr. Gilman Louie is CEO of In-Q-Tel, Washington, DC.

Enders Game
Preparing The Future Analyst – Today’s Cyber Teenager



© 2004 In-Q-Tel, Inc.

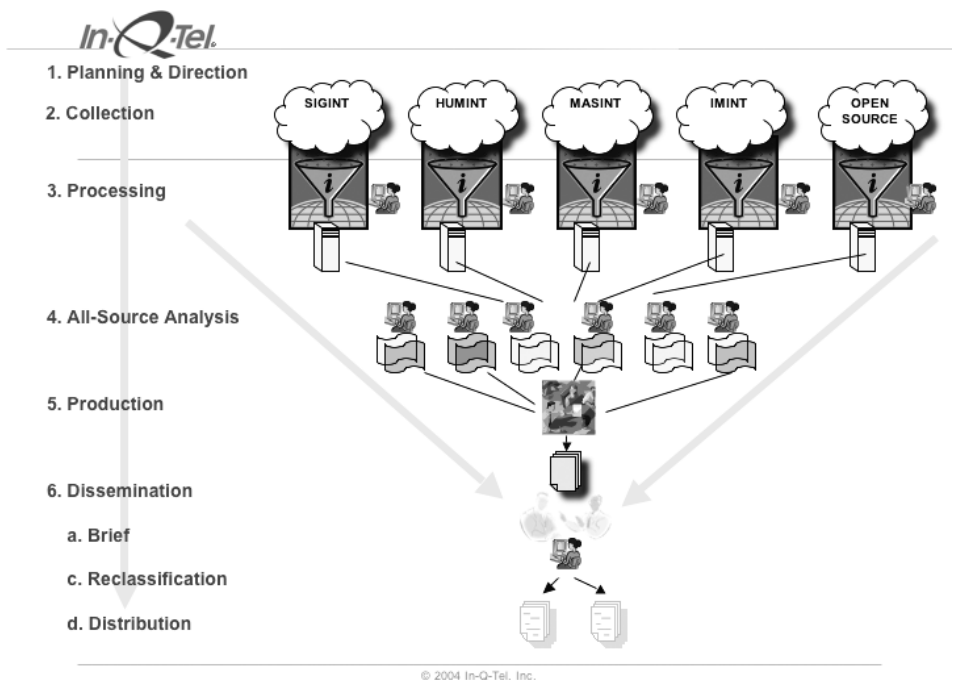
So for all of the analysts out there who complain that they have to perform too many searches to retrieve relevant information, who have to go through too many data repositories, compare that to what the typical teenager processes each year:

- 1200 hours on the cell phone;
- 10,000 hours instant messaging;
- 7500 email messages from 500 different sources;
- 500 hours on video chat;
- 200 transactions on E-Bay (Why is E-Bay important? Because of the focus on the reputation of both the seller and the buyer. If a seller is unreliable he or she gains a bad reputation in the online marketplace, consequently no one wants to buy from him/her.);
 - 1000 Blog entries – teenagers and younger children recognize the value of information sharing provided by this media;
 - 300 user group entries a year;
 - 15,000 queries using a search engine such as Google. You may think you are using a similar query system to these teenagers. Although U-boat/UVO is a super indexing system, it is the knowledge-aware tool. We do not have the equivalent of Google in the Intelligence Community – there is no search engine that can search across everything that is in the Intelligence Community.

- 4500 news sources from the Internet a year. There is no need for our children to read newspapers, as long as there is the Google news search engine just a click away;
- 5000 digital images taken a year;
- Hundreds of geospatial images and maps, all at their fingertips.

So this is how kids today are engaging information and utilizing information technology. But this is not some far off future scenario: these kids are showing up now in the work force. The problem is that tomorrow's work force is developing workflow habits at home, school, and in college; what we give them in the Intelligence Community doesn't even remotely compare. It's no wonder why they don't remain in job positions for long periods of time; some may not even make it through training.

Below is a classic depiction of the Intelligence Cycle. How do you take large amounts of data and reduce it down to a manageable set of information that you can digest?



The model was built in the 40s and in the 50s because we didn't have the capability of looking across all the dots at one time. So we had to have intermediaries who preprocessed the information. Today's cable traffic is not raw intelligence; the person on the other side who is typing the cable makes edits to create more concise text. It's all about reduction, a kind of batch publishing model designed to serve customers at the very top. Intelligence is produced to push up –

not to share across the community. Only after it has been seen by the appropriate authorities is it appropriately redacted and disseminated.

Here are all the favorite terms that are used:

- Volume is a problem.
- Sequential production system.
- Batch operations.
- 24-hour cycle times.
- Focus on publication and products.
- Here is one that I really worry about : “Actionable” intelligence (this is going to be our Achilles heel).
- Hierarchical structures.
- Information flows up, decisions flow down.
- Customers of greatest need are senior policy makers, therefore we do tasking for senior policy makers.
- Tasking is driven by senior planning and coordination.
- Data is owned and controlled by the collectors.
- We have a search-based IT system (the way we approach our analytics is very similar to the way a kid approaches a geometry proof).
- Analysis is framed by classical hypothesis and proof theory.
- Decision-making is based on highest probable outcomes.

You may or may not agree with the following:



Alternative Intelligence Model

- **Volume is an Asset**
- **Multi-path Discovery**
- **Supply Chain Management, Just-in-Time Delivery**
- **Real-Time Operation**
- **Focus on Service**
- **Focus on “Understanding” and Strategic Decision Making**
- **Network Structure**
- **Information flows based on demand & need**
- **Customers of Greatest Need are those Closest to the Solution**
- **Tasking is driven by Impact**
- **Information is designed to be shared, not owned**
- **Agent based IT systems**
- **Analysis is framed by non-linear, multi-path, scenario planning**
- **Decision Making is based on influencing probabilities**

© 2004 In-Q-Tel, Inc.

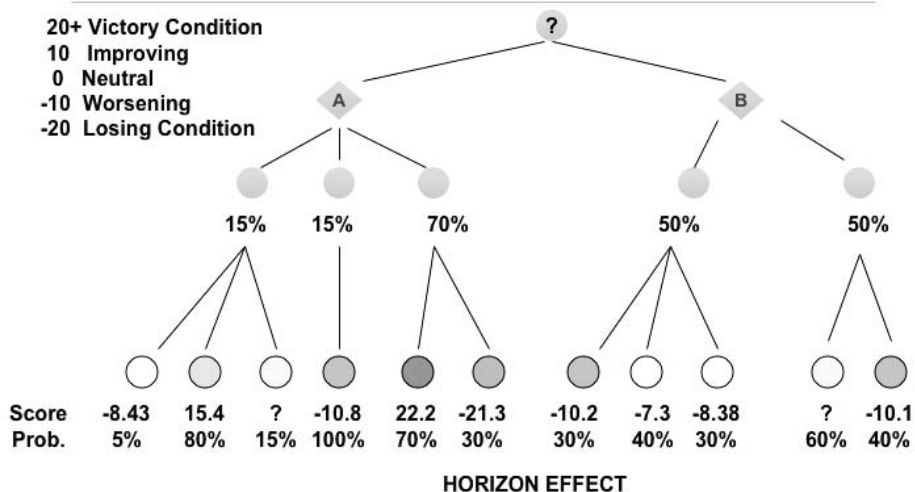
First, I believe volume is an asset. Anyone familiar with large, noisy systems knows the best way to get to a level of resolution is to be able to move a step backward from the problem. Once you look at the data as a whole, you see that patterns start to emerge. But you cannot see patterns emerge when if you don't have enough data to see the clumping of information.

Multi-path discovery means that stumbling across the answer may lead you to a particular conclusion, even if you were asking the wrong question. What we should be doing is examining all the possibilities before settling for a solution. We all search for the "right" answers because that is what we are trained to do, but there is a flaw in that unilateral focus. By putting such strong emphasis on the correctness of one direction, it negates the possibility for multi-path discovery and risk taking.

This is how we write a computer game program. This is what goes on in your chess engine, how we train a computer system to play like a person. So I am going to reveal the secrets behind the technology. We ask the computer to make a decision: move A or move B? Underneath this decision, the computer uses a set of complex algorithms to compute the probable list of outcomes. These algorithms are based on your opponent's set of possible counter moves, and the computer's best responding counter moves. In the first generation of these computer games, they did what we call weighted probability average. They looked at the score – a negative score meant that you lost the game and a positive score meant that you won the game.



Lessons from Gaming



© 2004 In-Q-Tel, Inc.

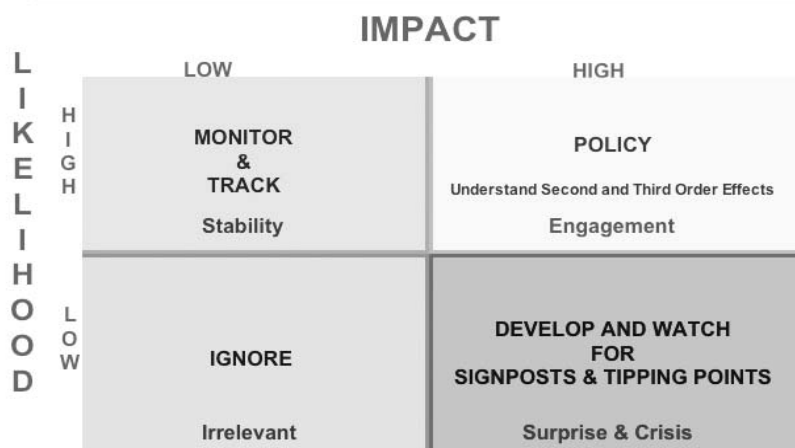
Now the problem is that in some of these models it is analogous with having one foot on the ice and one foot in the flame. You know that your average probabilistic outcome is neutral. If you make that decision to pull that lever you could get yourself in a lot of trouble. Likewise, you may get obsessed with moving a particular chess piece because you have a risk score of 22.2, which would mean that you win. A 70 percent chance of winning looks very tempting. But if something unusual happens, or you called it wrong, that negative 21.3 points of that same move means you lose.

So risk-takers are easily duped and trapped by that particular move. Depending on what kind of individual you are, you may decide to make a move worse than your current position in order to avoid the ultimate disaster. On the other hand, you may be a risk-taker and decide that you have nothing to lose and thus take a chance for the ultimate win.

That is the essence of the strategy used in a chess game. I propose to you that if you go for the world with a range of possibilities rather than the single best move, you may be able to understand those bottom dots. And one of the things policymakers do not understand based on what they read from the dots we give them, is that we don't let them see the full range of dots underneath – the full breadth of underlying information is invisible to them. As a result, we don't help them understand the consequences of certain decisions. In addition, they may get a target fixation, either constantly going for the big win or constantly preventing loss by avoiding all risk. They may also look back at data, because today's particular move may not show up well the next day.



Strategic Analysis – Understanding Possibilities



© 2004 In-Q-Tel, Inc.

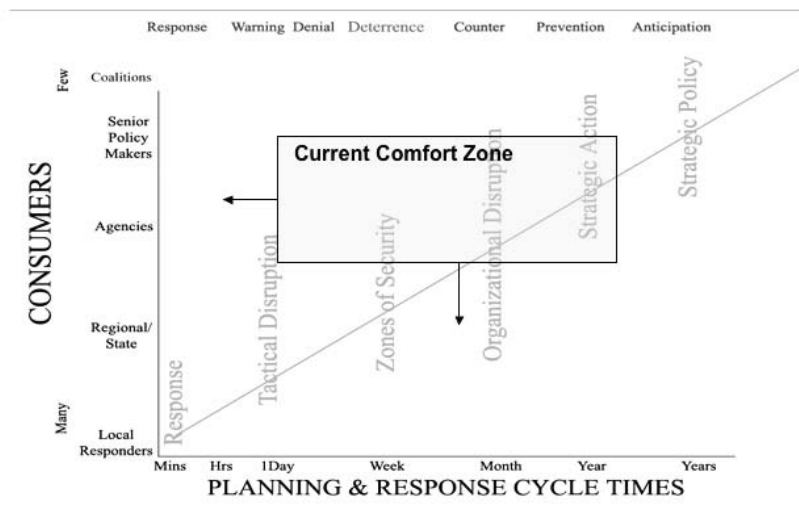
The preceding grid is directed at the expert. The expert likes to play in the yellow square (Policy – understand second and third order effects, engagement). The expert sets up policies, and engages. Actionable intelligence describes that yellow square.

The problem with the yellow square is that you start with a piece of information, a piece of intelligence, and you are in a response mode where you have to make a move. It is more effective to be in a proactive mode. It is in this mode where you look for second and third order effects from a decision that may not appear to relate to your particular problem – particularly in a networked global economy.

The red square is deadly. These are the low-probability, high-impact squares that are not given enough time to fully convey their impact. Consequently it creates surprise and crisis. The solution is to develop an understanding of tipping points and potential crisis scenarios early on to navigate effectively through surprise situations. The lower left hand square can be ignored, and the upper blue one should be monitored if you can afford to do so.

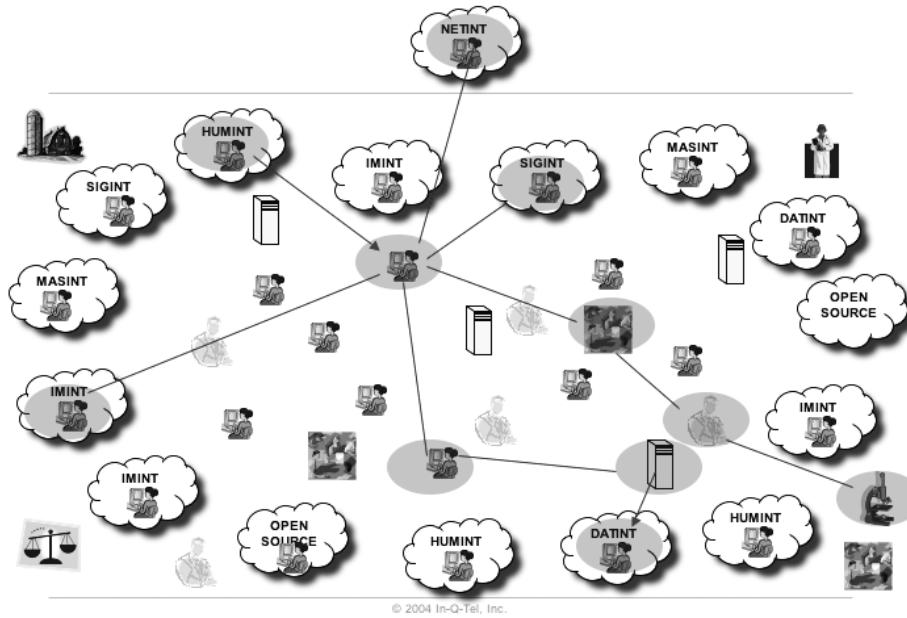
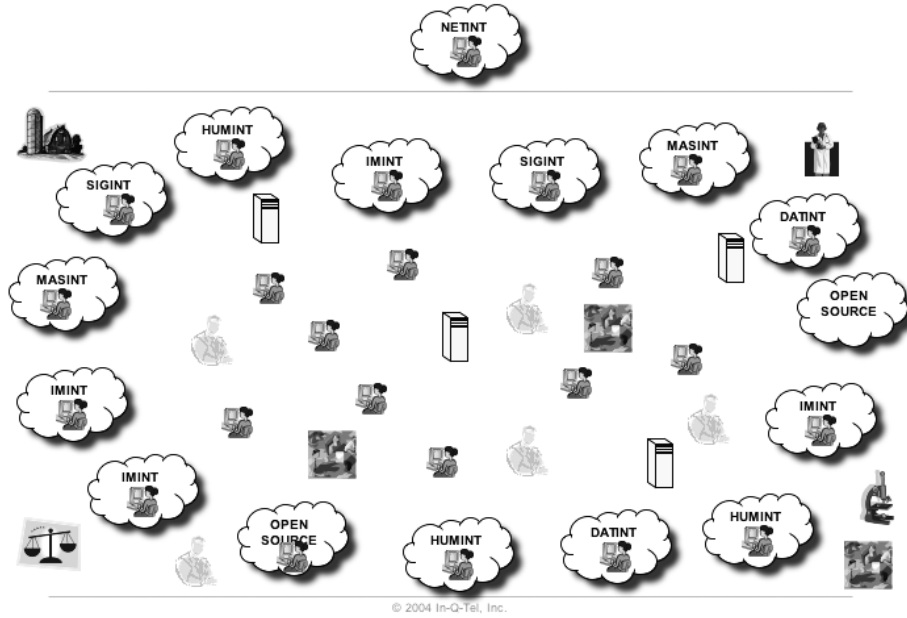


Time Based Targeted Intelligence



© 2004 In-Q-Tel, Inc.

Shown above is your average time-based competition model. The X axis lists the minutes, hours, days, weeks, months, and years. You know the processes we use – in other words you must have an instant response. Somebody who needs information right away is the guy closest to the problem, right? It doesn't need



to go through the process, it needs to go out to the field as quickly as possible, because there are huge consequences for missing that response time. On the other hand, any senior policy makers who like to play in the month column may be in the wrong place and unable to respond quickly, but they also have a bigger effect on the strategic goals. This may help explain some of the things we have discussed recently, such as a lack of funding and resources when you are working on this type of strategic analysis.

The network model is shown on the previous page. The fallacy is that the network diagram exists and is wired all over the place. But an exceptional network is one that allows for ad hoc networking, enabling you to contact people at your convenience. That means that by using the network, information held by another person can be easily located. This allows you to find somebody else who *has* the information, not necessarily the information itself. Collaboration is common; it is a model that requires the capability to set up virtual teams. The problem with virtual teams is that you don't know who is on your team. Information systems need improvement in order to help you find the experts.

Technology is about real time profiling. This means that our networks must have the ability to be network-aware. This is a critical set of tools for the user – much more so for the better search engines. The other problem with the network model is the level of sharing between people. The problem with intelligence services is that we write not to share, but to classify. This model assumes that the first time you put your fingers on the keyboard it is at an unclassified level allowing information to flow freely through the system before adding levels of classifications. It also means that the information needs to be readily available as well as relevant to the user.

There is also a need to understand what is going on in the network. They can tell you at any time the top 10 things people are searching for by country and by region. If they can say that East Paris has been hot in the last 10 minutes, maybe something's happening there.

IT is supposed to make your lives easier, not harder. The problem is with the tools that have been provided to you; IT has turned you into what I call data monkeys. You spend a majority of your time searching for information across multiple repositories, typing in search terms, doing queries, rather than having the system do it for you. In today's architectures, information can be delivered to you when you need it, before you even ask the question.

Architecture – before you get to the tools, the wiring needs to be correct underneath. The data of record needs to be a digital record otherwise I can't find it. If it's on a piece of paper, sitting in a safe, my search engines cannot locate the data. That's a huge problem. I mean that you need to have a common data layer. So all those programs that your CIOs are kind of whining about that always seems to get cut out of the budget because it's all that infrastructure stuff, is really about the wiring diagram, enabling the network to efficiently move information around.

Once the wiring is correct, then you can discuss these fantastic tools. The good news is that we don't have to create it from scratch. The commercial and consumer worlds have existed in the network environment for the last five years. They wired up for supply chain management, just-in-time inventory, expertise finding, to conduct market intelligence, and to exploit the Internet. This is a great opportunity for us. If we can get our wiring right, we can adopt their tools. If we adopt the right architecture we can slot the tools within a week of seeing it on the net and bring it up in your systems immediately.

So one of the things we all need to do is to take that 14-year-old, give her a haircut, dress her up a little bit better. Change the roles to allow yourself to put the right tools on the table so she can be productive. Now I'm going to leave you with a tool that was written by a group of computer gamers, not by geo-spatial analysts. This particular tool appeared on CNN, Fox, and ABC, at the outbreak of the war. It was used by CNN to do battle damage assessments, the same tool that was put into the Pentagon a week earlier

These gamers didn't know any better, because nobody told them that this couldn't be done on a laptop. I am going to give you a series of fly-throughs using commercial imagery. During the Gulf war certain areas of the global map were updated multiple times a day. This is all available across the Internet, a silicon graphics machine is not necessary. Since this runs over a modem, you don't need special equipment in your building.

I think we have been asking the wrong set of questions. As an analytical core, we need to look at the world of possibilities. Especially the possibilities based on bad policies, while low probabilities, that could have a massive destructive impact. Not looking for the right answer is the right answer. The right answer ultimately will get you in the position where one foot is on a block of ice and the other is in an open flame.



Tools on the Horizon

- **Expertise Finding**
- **Collaboration**
- **Federated Search**
- **Robust Link and Relationship Analysis**
- **Integrated Geospatial Tools**
- **Entity Resolution**
- **Visualization**
- **Pattern, Cluster, and Anomaly Identification**
- **Unstructured Data Analysis Tools**
- **Rich Media Exploitation Tools**
- **Large Scale Distributed Data Exploitation tools**
- **Machine Translation for Data Exploitation**
- **Document Exploitation**
- **Modeling and Simulation**
- **Risk Analysis Tools**
- **Intelligence Diagnostic Tools**

© 2004 In-Q-Tel, Inc.

Integrating Methodologists into Teams of Substantive Experts

*Rob Johnston**

Intelligence analysis, like other complex tasks, demands considerable expertise. It requires individuals who can recognize patterns in large data sets, solve complex problems, and make predictions about future behavior or events. To perform these tasks successfully, analysts must dedicate a considerable number of years to researching specific topics, processes, and geographic regions.

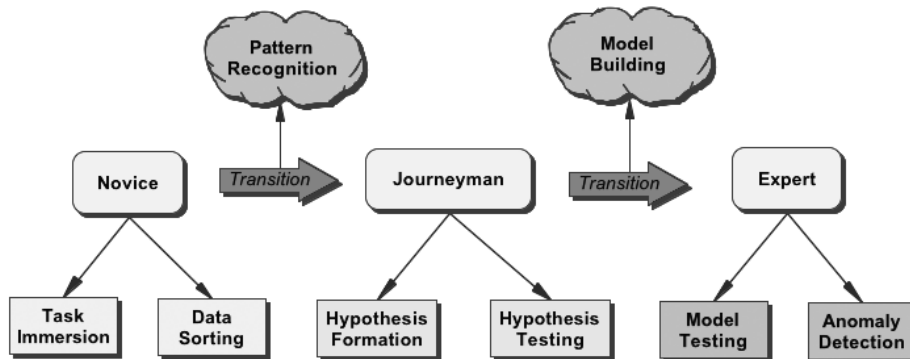
Paradoxically, it is the specificity of expertise that makes expert forecasts unreliable. While experts outperform novices and machines in pattern recognition and problem solving, expert predictions of future behavior or events are seldom as accurate as simple actuarial tables. In part, this is due to cognitive biases and processing-time constraints. In part, it is due to the nature of expertise itself and the process by which one becomes an expert.¹

Becoming an Expert

Expertise is commitment coupled with creativity. Specifically, it is the commitment of time, energy, and resources to a relatively narrow field of study and the creative energy necessary to generate new knowledge in that field. It takes a considerable amount of time and regular exposure to a large number of cases to become an expert.

* Dr. Rob Johnston is Postdoctoral research fellow at the CIA Center for the Study of Intelligence and member of the research staff at the Institute for Defense Analyses.

¹ More than 200 individuals contributed to this study. The author is indebted to the researchers, fellows, and staff at the Center for the Study of Intelligence, the Institute for Defense Analyses, the National Military Intelligence Association, Evidence Based Research, Inc., and ANSER Inc. Staff and students at the CIA University, the Joint Military Intelligence College, the Naval Postgraduate School, Columbia University, Georgetown University, and Yale University also contributed to the project.



An individual enters a field of study as a novice. The novice needs to learn the guiding principles and rules – the *heuristics* and *constraints* – of a given task in order to perform that task. Concurrently, the novice needs to be exposed to specific cases, or instances, that test the boundaries of such heuristics. Generally, a novice will find a mentor to guide her through the process of acquiring new knowledge. A fairly simple example would be someone learning to play chess. The novice chess player seeks a mentor to teach her the object of the game, the number of spaces, the names of the pieces, the function of each piece, how each piece is moved, and the necessary conditions for winning or losing the game.

In time, and with much practice, the novice begins to recognize patterns of behavior within cases and, thus, becomes a journeyman. With more practice and exposure to increasingly complex cases, the journeyman finds patterns not only within cases but also between cases. More importantly, the journeyman learns that these patterns often repeat themselves over time. The journeyman still maintains regular contact with a mentor to solve specific problems and learn more complex strategies. Returning to the example of the chess player, the individual begins to learn patterns of opening moves, offensive and defensive game-playing strategies, and patterns of victory and defeat.

When a journeyman starts to make and test hypotheses about future behavior based on past experiences, she begins the next transition. Once she creatively generates knowledge, rather than simply matching superficial patterns, she becomes an expert. At this point, she is confident in her knowledge and no longer needs a mentor as a guide – she becomes responsible for her own knowledge. In the chess example, once a journeyman begins competing against experts, makes

predictions based on patterns, and tests those predictions against actual behavior, she is generating new knowledge and a deeper understanding of the game. She is creating her own cases rather than relying on the cases of others.

The chess example is a rather short description of an apprenticeship model. Apprenticeship may seem like a restrictive 18th century mode of education, but it is still a standard method of training for many complex tasks. Academic doctoral programs are based on an apprenticeship model, as are fields like law, music, engineering, and medicine. Graduate students enter fields of study, find mentors, and begin the long process of becoming independent experts and generating new knowledge in their respective domains.

To some, playing chess may appear rather trivial when compared, for example, with making medical diagnoses, but both are highly complex tasks. Chess has a well-defined set of heuristics, whereas medical diagnoses seem more open ended and variable. In both instances, however, there are tens, if not hundreds, of thousands of potential patterns. A research study discovered that chess masters had spent between 10,000 and 20,000 hours, or more than ten years, studying and playing chess. On average, a chess master stores 50,000 different chess patterns in long-term memory.²

Similarly, a diagnostic radiologist spends eight years in full time medical training – four years of medical school and four years of residency – before she is qualified to take a national board exam and begin independent practice.³ According to a 1988 study, the average diagnostic radiology resident sees forty cases per day, or around 12,000 cases per year.⁴ At the end of a residency, a diagnostic radiologist has stored, on average, 48,000 cases in long-term memory.

Psychologists and cognitive scientists agree that the time it takes to become an expert depends on the complexity of the task and the number of cases, or patterns, to which an individual is exposed. The more complex the task, the longer it takes to build expertise, or, more accurately, the longer it takes to experience and store a large number of cases or patterns.

The Power of Expertise

Experts are individuals with specialized knowledge suited to perform the specific tasks for which they are trained, but that expertise does not necessarily

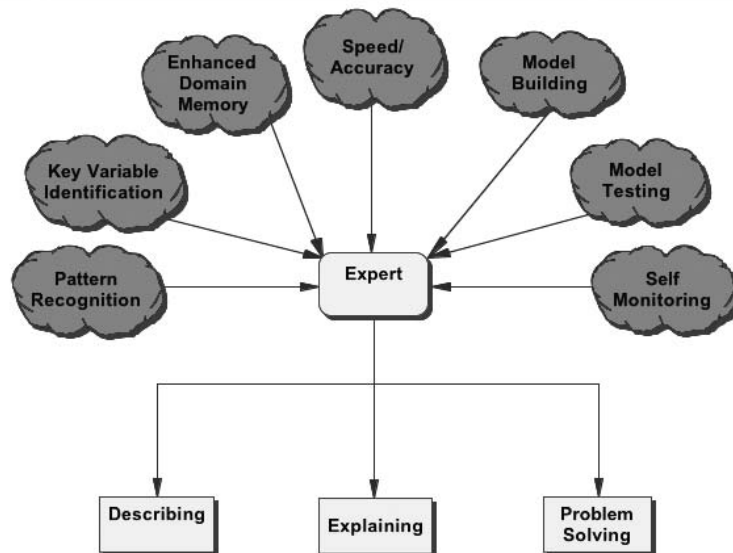
² W. Chase and H. Simon, "Perception in Chess," *Cognitive Psychology*, Vol. 4, 1973, pp. 55-81.

³ American College of Radiology. Personal communication, 2002.

⁴ A. Lesgold, H. Rubinson, P. Feltovich, R. Glaser, D. Klopfer, and Y. Wang, "Expertise in a Complex Skill: Diagnosing X-Ray Pictures," M. Chi, R. Glaser, and M. Farr, eds., *The Nature of Expertise* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1988).

transfer to other domains.⁵ A master chess player cannot apply chess expertise in a game of poker – although both chess and poker are games, a chess master who has never played poker is a novice poker player. Similarly, a biochemist is not qualified to perform neurosurgery, even though both biochemists and neurosurgeons study human physiology. In other words, the more complex a task is, the more specialized and exclusive is the knowledge required to perform that task.

Experts: Promise



An expert perceives meaningful patterns in her domain better than non-experts. Where a novice perceives random or disconnected data points, an expert connects regular patterns within and between cases. This ability to identify patterns is not an innate perceptual skill; rather it reflects the organization of knowledge after exposure to and experience with thousands of cases.⁶

⁵ M. Minsky and S. Papert, *Artificial Intelligence* (Eugene, OR: Oregon State System of Higher Education, 1974); J. Voss and T. Post, "On the Solving of Ill-Structured Problems," M. Chi, R. Glaser, and M. Farr, eds., *Op. Cit.*

⁶ O. Akin, *Models of Architectural Knowledge* (London: Pion, 1980); D. Egan and B. Schwartz. "Chunking in Recall of Symbolic Drawings," *Memory and Cognition*, Vol. 7, 1979, pp. 149-158; K. McKeithen, J. Reitman, H. Rueter, and S. Hirtle, "Knowledge Organization and Skill Differences in Computer Programmers," *Cognitive Psychology*, Vol. 13, 1981, pp. 307-325.

Experts have a deeper understanding of their domains than novices do, and utilize higher-order principles to solve problems.⁷ A novice, for example, might group objects together by color or size, whereas an expert would group the same objects according to their function or utility. Experts comprehend the meaning of data and weigh variables with different criteria within their domains better than novices. Experts recognize variables that have the largest influence on a particular problem and focus their attention on those variables.

Experts have better domain-specific short-term and long-term memory than novices do.⁸ Moreover, experts perform tasks in their domains faster than novices and commit fewer errors while problem solving.⁹ Interestingly, experts go about solving problems differently than novices. Experts spend more time thinking about a problem to fully understand it at the beginning of a task than do novices, who immediately seek to find a solution.¹⁰ Experts use their knowledge of previous cases as context for creating mental models to solve given problems.¹¹

Better at self-monitoring than novices, experts are more aware of instances where they have committed errors or failed to understand a problem.¹² Experts check their solutions more often than novices and recognize when they are missing information necessary for solving a problem.¹³ Experts are aware of the limits of their domain knowledge and apply their domain's heuristics to solve problems that fall outside of their experience base.

⁷ M. Chi, P. Feltovich, and R. Glaser, "Categorization and Representation of Physics Problems by Experts and Novices," *Cognitive Science*, Vol. 5, 1981, pp. 121-125; M. Weiser and J. Shertz, "Programming Problem Representation in Novice and Expert Programmers," *Instructional Journal of Man-Machine Studies*, Vol. 14, 1983, pp. 391-396.

⁸ W. Chase and K. Ericsson, "Skill and Working Memory," G. Bower, ed., *The Psychology of Learning and Motivation* (New York, NY: Academic Press, 1982).

⁹ W. Chase, "Spatial Representations of Taxi Drivers," D. Rogers and J. Slobada, eds., *Acquisition of Symbolic Skills* (New York, NY: Plenum, 1983).

¹⁰ J. Paige and H. Simon, "Cognition Processes in Solving Algebra Word Problems," B. Kleinmuntz, ed., *Problem Solving* (New York, NY: Wiley, 1966).

¹¹ J. Voss and T. Post, "On the Solving of Ill-Structured Problems," M. Chi, R. Glaser, and M. Farr, eds., *Op. Cit.*

¹² M. Chi, R. Glaser, and E. Rees, "Expertise in Problem Solving," R. Sternberg, ed., *Advances in the Psychology of Human Intelligence* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1982); D. Simon and H. Simon, "Individual Differences in Solving Physics Problems," R. Siegler, ed., *Children's Thinking: What Develops?* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1978).

¹³ J. Larkin, "The Role of Problem Representation in Physics," D. Gentner and A. Stevens, eds., *Mental Models* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1983).

The Paradox of Expertise

The strengths of expertise can also be weaknesses.¹⁴ Although one would expect experts to be good forecasters, they are not particularly good at making predictions about the future. Since the 1930s, researchers have been testing the ability of experts to make forecasts.¹⁵ The performance of experts has been tested against actuarial tables to determine if they are better at making predictions than simple statistical models. Seventy years later, with more than two hundred experiments in different domains, it is clear that the answer is no.¹⁶ If supplied with an equal amount of data about a particular case, an actuarial table is as good, or better, than an expert at making calls about the future. Even if an expert is given more specific case information than is available to the statistical model, the expert does not tend to outperform the actuarial table.¹⁷

There are few exceptions to these research findings, but the exceptions are informative. When experts are given the results of the actuarial predictions, for example, they tend to score as well as the statistical model if they use the statistical information in making their own predictions.¹⁸ In addition, if an expert has

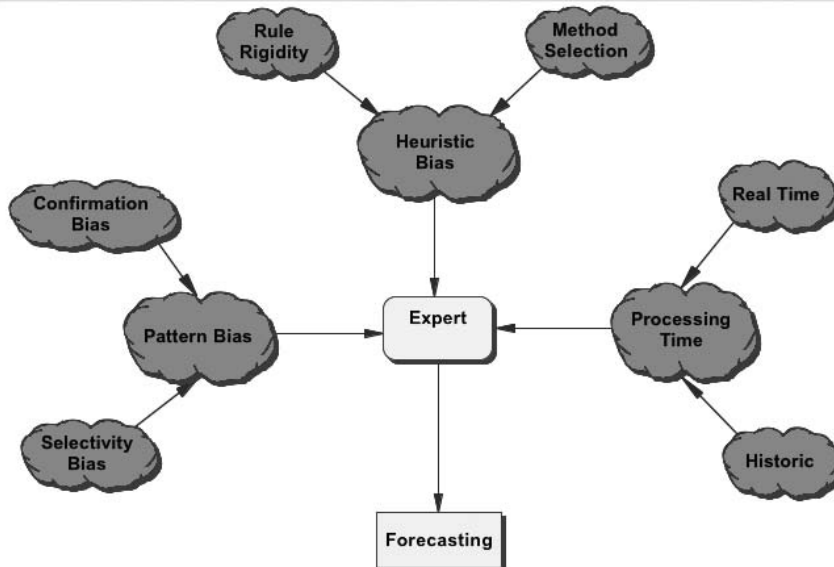
¹⁴ C. Camerer and E. Johnson, "The Process-Performance Paradox in Expert Judgment: How Can Experts Know so Much and Predict so Badly?"; K. Ericsson and J. Smith, eds., *Toward a General Theory of Expertise: Prospects and Limit* (Cambridge, UK: Cambridge University Press, 1991).

¹⁵ H. Reichenbach, *Experience and Prediction* (Chicago, IL: University of Chicago Press, 1938); T. Sarbin, "A Contribution to the Study of Actuarial and Individual Methods of Prediction," *American Journal of Sociology*, Vol. 48, 1943, pp. 593-602.

¹⁶ R. Dawes, D. Faust, and P. Meehl, "Clinical Versus Actuarial Judgment," *Science*, Vol. 243, 1989, pp. 1668-1674; W. Grove and P. Meehl, "Comparative Efficiency of Informal (Subjective, Impressionistic) and Formal (Mechanical, Algorithmic) Prediction Procedures: The Clinical-Statistical Controversy," *Psychology, Public Policy, and Law*, Vol. 2, No. 2, 1996, pp. 293-323.

¹⁷ R. Dawes, "A Case Study of Graduate Admissions: Application of Three Principles of Human Decision Making," *American Psychologist*, Vol. 26, 1971, pp. 180-188; W. Grove and P. Meehl, Op. Cit. (see footnote 16); H. Sacks, "Promises, Performance, and Principles: An empirical study of Parole Decision-making in Connecticut," *Connecticut Law Review*, Vol. 9, 1977, pp. 349-422; T. Sarbin, "A Contribution to the Study of Actuarial and Individual Methods of Prediction," *American Journal of Sociology*, 1943, pp. 48, 593-602; J. Sawyer, "Measurement and Prediction, Clinical and Statistical," *Psychological Bulletin*, Vol. 66, 1966, pp. 178-200; W. Schofield and J. Garrard, "Longitudinal Study of Medical Students Selected for Admission to Medical School by Actuarial and Committee Methods," *British Journal of Medical Education*, Vol. 9, 1975, pp. 86-90.

¹⁸ L. Goldberg, "Simple Models or Simple Processes? Some Research on Clinical Judgments," *American Psychologist*, Vol. 23, 1968, pp. 483-496; L. Goldberg, "Man versus Model of Man: A Rationale, Plus some Evidence, for a Method of Improving on Clinical Inferences," *Psychological Bulletin*, Vol. 73, 1970, pp. 422-432; D. Leli and S. Filskov, "Clinical-Actuarial Detection of and Description of Brain Impairment with the Wechsler-Bellevue Form I," *Journal of Clinical Psychology*, Vol. 37, 1981, pp. 623-629.



privileged information that is not reflected in the statistical table, she will actually perform better than the table. A classic example is the broken leg argument: Judge X has gone to the theater every Friday night for the past ten years. Based on an actuarial table, one would predict, with some certainty, that the judge would go to the theater this Friday night. An expert knows, however, that the judge broke her leg Thursday afternoon and is currently in the hospital until Saturday. Knowing this key variable allows the expert to predict that the judge will not attend the theater this Friday night.

Although this argument makes sense, it is misleading. Forecasting is not simply a linear logical argument but rather a complex, interdisciplinary, dynamic, and multivariate task. Cases are rare where one key variable is known and weighed appropriately to determine an outcome. Generally, no single static variable predicts behavior; rather, many dynamic variables interact, weight and value change, and other variables are introduced or omitted to determine outcome.

Theorists and researchers differ when trying to explain why experts are less accurate forecasters than statistical models. Some have argued that experts, like all humans, are inconsistent when using mental models to make predictions. That is, the model an expert uses for predicting X in one month is different from

the model used for predicting X in a following month, although precisely the same case and same data set are used in both instances.¹⁹

A number of researchers point to human biases to explain unreliable expert predictions. During the last 30 years, researchers have categorized, experimented, and theorized about the cognitive aspects of forecasting.²⁰ Despite such efforts, the literature shows little consensus regarding the causes or manifestations of human bias. Nonetheless, there is general agreement that two types of bias exist:

Pattern bias – looking for evidence that confirms rather than rejects a hypothesis and inadvertently filling in missing data with data from previous experiences.

Heuristic bias – using inappropriate guidelines or rules to make predictions.

The very method by which one becomes an expert explains why experts are much better at describing, explaining, performing tasks, and problem-solving within their domains than are novices, but, with a few exceptions, are worse at forecasting than actuarial tables based on historical, statistical models.

A given domain has specific heuristics for performing tasks and solving problems. These rules are a large part of what makes up expertise. In addition, experts need to acquire and store tens of thousands of cases within their domains in order to recognize patterns, generate and test hypotheses, and contribute to the collective knowledge within their fields. In other words, becoming an expert requires a significant number of years of viewing the world through the lens of one specific domain. It is the specificity that gives the expert the power to recognize patterns, perform tasks, and solve problems.

Paradoxically, it is this same specificity that is restrictive, narrowly focusing the expert's attention on one domain to the exclusion of others. It should come as little surprise, then, that an expert would have difficulty identifying and weighing variables in an interdisciplinary task such as forecasting an adversary's intentions.

¹⁹ J. Fries, *et al.*, "Assessment of Radiologic Progression in Rheumatoid Arthritis: A Randomized, Controlled Trial," *Arthritis Rheum.*, as written by author Vol. 29, No. 1, 1986, pp. 1-9.

²⁰ J. Evans, *Bias in Human Reasoning: Causes and Consequences* (Hove, UK: Lawrence Erlbaum Associates, 1989); R. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999); D. Kahneman, P. Slovic, and A. Tversky, *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge, UK: Cambridge University Press, 1982); A. Tversky and D. Kahneman, "The Belief in the 'Law of Small Numbers,'" *Psychological Bulletin*, Vol 76, 1971, pp. 105-110; A. Tversky and D. Kahneman, "Judgment Under Uncertainty: Heuristics and Biases," *Science*, Vol. 185, 1974, pp. 1124-1131.

The Burden on Intelligence Analysts

Intelligence is an amalgam of a number of highly specialized domains. Within each of these domains, a number of experts are tasked with assembling, analyzing, assigning meaning, and reporting on data, the goals being to describe, solve a problem, or make a forecast.

When an expert encounters a case outside her expertise, her options are to repeat the steps she initially used to become an expert in the field. She can:

- Try to make the new data fit with a pattern that she has previously stored;
- Recognize that the case falls outside her expertise and turn to her domain's heuristics to try to give meaning to the data;
- Acknowledge that the case still does not fit with her expertise and reject the data set as being an anomaly; or
- Consult with other experts.

A datum, in and of itself, is not domain specific. Imagine economic data that reveal that a country is investing in technological infrastructure, chemical supplies, and research and development. An economist might decide that the data fit an existing spending pattern and integrate these facts with prior knowledge about a country's economy. The same economist might decide that this is a new pattern that needs to be remembered (or stored in long-term memory) for some future use. The economist might decide that the data are outliers of no consequence and should be ignored. Or, the economist might decide that the data would be meaningful to a chemist or biologist and therefore seek to collaborate with other specialists who might reach different conclusions regarding the data than would the economist.

In this example, the economist is required to use her economic expertise in all but the final option of consulting with other experts. In the decision to collaborate, the economist is expected to know that what appears to be new economic data may have value to a chemist or biologist, domains with which she may have no experience. In other words, the economist is expected to know that an expert in some other field might find meaning in data that appear to be economic.

Three *confounding variables* affect the economist's decision-making:

Processing time, or context. This does not refer to the amount of time necessary to accomplish a task, but rather the moment in time during which a task occurs – “real time” – and the limitations that come from being close to an event. The economist doesn't have *a priori* knowledge that the new data set is *the* critical data set for some future event. In “real time,” they are simply data to be manipulated. It is only in retrospect, or long-term memory, that the economist can fit the data into a larger pattern, weigh their value, and assign them meaning.

Pattern bias. In this particular example, the data appear to be economic and

the expert is an economist. The data are, after all, investment data. Given the background and training of an economist, it makes perfect sense to try to manipulate the new data within the context of economics, despite the fact that there may be other more important angles.

Heuristic bias. The economist has spent a career becoming familiar with and using the guiding principles of economic analysis and, at best, has only a vague familiarity with other domains and their heuristics. An economist would not necessarily know that a chemist or biologist could identify what substance is being produced based on the types of equipment and supplies that are being purchased.

This example does not describe a complex problem – most people would recognize that the data from this case might be of value to other domains. It is one isolated case, viewed retrospectively, which could potentially affect two other domains. But what if the economist had to deal with one hundred data sets per day? Now, multiply those one hundred data sets by the number of potential domains that would be interested in any given economic data set. Finally, put all of this in the context of “real time.” The economic expert is now expected to maintain expertise in economics, which is a full-time endeavor, while simultaneously acquiring some level of experience in every other domain. Based on these expectations, the knowledge requirements for effective collaboration quickly exceed the capabilities of the individual expert.

The expert is left dealing with the data through the lens of her own expertise. She uses her domain heuristics to incorporate the data into an existing pattern, store the data into long-term memory as a new pattern, or reject the data set as an outlier. In each of these options, the data stop with the economist instead of being shared with an expert in some other domain. The fact that these data are not shared then becomes a critical issue in cases of analytic error.²¹

In hindsight, critics will say that the implications were obvious – that the crisis could have been avoided if the data had been passed to one specific expert or another. In “real time,” however, an expert cannot know which particular data set would have value for an expert in another domain.

The Pros and Cons of Teams

One obvious solution to the paradox of expertise is to assemble an interdisciplinary team. Why not simply make all problem areas or country-specific da-

²¹ L. Kirkpatrick, *Captains Without Eyes: Intelligence Failures in World War II* (London: MacMillan Company, 1969); F. Shiels, *Preventable Disasters: Why Governments Fail* (Savage, MD: Rowman and Littlefield, 1991); J. Wirtz, *The Tet Offensive: Intelligence Failure in War* (Ithaca, NY: Cornell University Press, 1991); R. Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

ta available to a team of experts from a variety of domains? This ought, at least, to reduce the pattern and heuristic biases inherent in relying on only one domain.

Ignoring potential security issues, there are practical problems with this approach. First, each expert would have to sift through large data sets to find data specific to her expertise. This would be inordinately time-consuming.

Second, during the act of scanning large data sets, the expert inevitably would be looking for data that fit within her area of expertise. Imagine a chemist who comes across data that show that a country is investing in technological infrastructure, chemical supplies, and research and development (the same data that the economist analyzed in the previous example). The chemist recognizes that these are the ingredients necessary for a nation to produce a specific chemical agent, which could have a military application or could be benign. The chemist then meshes the data with an existing pattern, stores the data as a new pattern, or ignores the data as an anomaly.

The chemist, however, has no frame of reference regarding spending trends in the country of interest. The chemist does not know if this is an increase, a decrease, or a static spending pattern – answers that the economist could supply immediately. There is no reason for the chemist to know if a country's ability to produce this chemical agent is a new phenomenon. Perhaps the country in question has been producing the chemical agent for years and these data are part of some normal pattern of behavior.

One hope is that neither expert treats the data set as an anomaly, that both report it as significant. Another hope is that each expert's analysis of the data – an increase in spending and the identification of a specific chemical agent – will come together at some point. The problem is at what point? Presumably, someone will get both of these reports somewhere along the intelligence chain. Of course, the individual who gets these reports may not be able to synthesize the information. That person is subject to the same three confounding variables described earlier: processing time, pattern bias, and heuristic bias. Rather than solving the paradox of expertise, the problem has merely been shifted to someone else in the organization.

In order to avoid shifting the problem from one expert to another, an actual collaborative team could be built. Why not explicitly put the economist and the chemist together to work on analyzing data? The utilitarian problems with this strategy are obvious. Not all economic problems are chemical and not all chemical problems are economic. Each expert would waste an inordinate amount of time. Perhaps one case in one hundred would be applicable to both experts; during the rest of the day, the experts would drift back to their individual domains, in part because that is what they are best at and in part just to stay busy.

Closer to the real world, the same example may also have social, political, historical, and cultural aspects. Despite an increase in spending on a specific chemical agent, the country in question may not be politically, culturally, social-

ly, historically, or otherwise inclined to use it in a threatening way. There may be social data – unavailable to the economist or the chemist – indicating that the chemical agent will be used for a benign purpose. In order for collaboration to work, each team would have to have experts from many domains working together on the same data set.

Successful teams have very specific organizational and structural requirements. An effective team requires discrete and clearly stated goals that are shared by each team member.²² Teams require interdependence and accountability – the success of each individual depends on the success of the team as a whole and the individual success of every other team member.²³

Effective teams require cohesion, formal and informal communication, cooperation, and shared mental models, or similar knowledge structures.²⁴ While cohesion, communication, and cooperation might be facilitated by specific work practices, creating shared mental models, or similar knowledge structures, is not

²² D. Cartwright and A. Zander, *Group Dynamics: Research and Theory* (New York, NY: Harper & Row, 1960); P. Fandt, W. Richardson, and H. Conner, "The Impact of Goal Setting on Team Simulation Experience," *Simulation and Gaming*, Vol. 21, No. 4, 1990, pp. 411-422; J. Harvey and C. Boettger, "Improving Communication within a Managerial Workgroup," *Journal of Applied Behavioral Science*, Vol. 7, 1971, pp.164-174.

²³ M. Deutsch, "The Effects of Cooperation and Competition Upon Group Process," D. Cartwright and A. Zander, eds., *Op. Cit.*; D. Johnson and R. Johnson, "The Internal Dynamics of Cooperative Learning Groups," R. Slavin, S. Sharan, S. Kagan, R. Hertz-Lazarowitz, C. Webb, and R. Schmuck, eds., *Learning to Cooperate, Cooperating to Learn* (New York, NY: Plenum, 1985); D. Johnson, G. Maruyama, R. Johnson, D. Nelson, and L. Skon, "Effects of Cooperative, Competitive, and Individualistic Goal Structure on Achievement: A Meta-Analysis," *Psychological Bulletin*, Vol. 89, No. 1, 1981, pp. 47-62; R. Slavin, "Research on Cooperative Learning: Consensus and Controversy," *Educational Leadership*, Vol. 47, No. 4, 1989, pp.52-55; R. Slavin, *Cooperative Learning* (New York, NY: Longman, 1983).

²⁴ J. Cannon-Bowers, E. Salas, S. Converse, "Shared Mental Models in Expert Team Decision Making," N. Castellan, ed., *Current Issues in Individual and Group Decision Making* (Hillsdale, NY: Lawrence Erlbaum Associates, 1983); L. Coch and J. French, "Overcoming Resistance to Change," D. Cartwright and A. Zander, eds., *Op. Cit.*; M. Deutsch, "The Effects of Cooperation and Competition Upon Group Process," D. Cartwright and A. Zander, eds., *Group Dynamics: Research and Theory* (New York, NY: Harper & Row, 1960); L. Festinger, "Informal Social Communication," D. Cartwright and A. Zander, eds., *Op. Cit.*; D. Johnson, R. Johnson, A. Ortiz, and M. Stanne, "The Impact of Positive Goal and Resource Interdependence on Achievement, Interaction, and Attitudes," *Journal of General Psychology*, Vol 118, No. 4, 1996, pp. 341-347; B. Mullen and C. Copper, "The Relation Between Group Cohesiveness and Performance: An Integration," *Psychological Bulletin*, Vol. 115, 1994, pp. 210-227; W. Nijhof and P. Kommers, "An Analysis of Cooperation in Relation to Cognitive Controversy," R. Slavin, S. Sharan, S. Kagan, R. Hertz-Lazarowitz, C. Webb, and R. Schmuck, eds., *Learning to Cooperate, Cooperating to Learn* (New York, NY: Plenum, 1995); J. Orasanu, "Shared Mental Models and Crew Performance," Paper presented at the 34th annual meeting of the Human Factors Society, Orlando, FL, 1990; S. Seashore, *Group Cohesiveness in the Industrial Workgroup* (Ann Arbor, Michigan, MI: University of Michigan Press, 1954).

a trivial task. Creating shared mental models may be possible with an air crew or a tank crew, where an individual's role is clearly identifiable as part of a larger team effort – like landing a plane or acquiring and firing on a target. Creating shared mental models in an intelligence team is less likely, given the vague nature of the goals, the enormity of the task, and the diversity of individual expertise. Moreover, the larger the number of team members, the more difficult it is to generate cohesion, communication, and cooperation. Heterogeneity can also be a challenge: It has a positive effect on generating diverse viewpoints within a team, but requires more organizational structure than does a homogeneous team.²⁵

Without specific processes, organizing principles, and operational structures, interdisciplinary teams will quickly revert to being just a room full of experts who ultimately drift back to their previous work patterns. That is, the experts will not be a team at all; they will be a group of experts individually working in some general problem space.²⁶

Looking to Technology

There are potential technological alternatives to multifaceted teams. An Electronic Performance Support System (EPSS), for example, is a large database, coupled with expert systems, intelligent agents, and decision aids. Applying such a system to intelligence problems might be a useful goal. At this point, however, the notion of an integrated EPSS for large complex data sets is more theory than practice.²⁷ Ignoring questions about the technological feasibility of such a system, fundamental epistemological flaws present imposing hurdles. It is virtually inconceivable that a comprehensive computational system could bypass the three confounding variables of expertise described earlier.

An EPSS, or any other computational solution, is designed, programmed, and implemented by a human expert from one domain: computer science. Historians will not design the “historical decision aid;” economists will not program the

²⁵ T. Mills, “Power Relations in Three-Person Groups,” in D. Cartwright and A. Zander, eds., *Op. Cit.*; L. Molm, “Linking Power Structure and Power Use,” K. Cook, ed., *Social Exchange Theory* (Newbury Park, CA: Sage, 1987); V. Nieva, E. Fleishman, and A. Rieck, *Team Dimensions: Their Identity, Their Measurement, and Their Relationships*, RN 85-12 (Alexandria, VA: US Army Research Institute for the Behavioral and Social Sciences, 1985); G. Simmel, *The Sociology of Georg Simmel*, K. Wolff, trans. (Glencoe, IL: Free Press, 1950).

²⁶ R. Johnston, *Decision Making and Performance Error in Teams: Research Results* (Arlington, VA: Defense Advanced Research Projects Agency, 1997); J. Meister, “Individual Perceptions of Team Learning Experiences Using Video-Based or Virtual Reality Environments,” *Dissertation Abstracts International*, UMI No. 9965200, 2000.

²⁷ R. Johnston, “Electronic Performance Support Systems and Information Navigation,” *Thread*, Vol. 2, No. 2, 1994, pp. 5-7.

“economic intelligent agent;” chemists will not create the “chemical agent expert system.” Software engineers and computer scientists will do all of that.

Computer scientists may consult with various experts during the design phase of such a system, but when it is time to sit down and write code, the programmer will follow the heuristics of computer science. The flexibility, adaptability, complexity, and usability of the computational system will be dictated by the guidelines and rules of computer science.²⁸ In essence, one would be trading the heuristics from dozens of domains for the rules that govern computer science. This would reduce the problem of processing time by simplifying and linking data, and it may potentially reduce pattern bias. But it will not reduce heuristic bias.²⁹ If anything, it may exaggerate it by reducing all data to a binary state.

This is not simply a Luddite reaction to technology. Computational systems have had a remarkable, positive effect on processing time, storage, and retrieval. They have also demonstrated utility in identifying patterns within narrowly defined and highly constrained domains. However, intelligence analysis is neither narrowly defined nor highly constrained. Quite the opposite, it is multivariate and highly complex, which is why it requires the expertise of so many diverse fields of study. Intelligence analysis is not something a computational system handles well. While an EPSS, or some other form of computational system, may be a useful tool for manipulating data, it is not a solution to the paradox of expertise.

Analytic Methodologists

Most domains have specialists who study the scientific process or research methods of their discipline. These people are concerned with the epistemology of their domain, not just philosophically but practically. They want to know how experts in their discipline reach conclusions or make discoveries. Rather than specializing in a specific substantive topic within their domain, these experts specialize in mastering the research and analytic methods of their domain.

In the biological and medical fields, these methodological specialists are epidemiologists. In education and public policy, these specialists are program evaluators. In other fields, they are research methodologists or statisticians. Despite the label, each field recognizes that it requires experts in methodology to main-

²⁸ R. Johnston and J. Fletcher, *A Meta-Analysis of the Effectiveness of Computer-Based Training for Military Instruction* (Alexandria, VA: Institute for Defense Analyses, 1998).

²⁹ J. Fletcher and R. Johnston, “Effectiveness and Cost Benefits of Computer-Based Decision Aids for Equipment Maintenance,” *Computers in Human Behavior*, Vol. 18, 2002, pp. 717-728.

tain and pass on the domain's heuristics for problem solving and making discoveries.

The methodologist's focus is on selecting and employing a process or processes to research and analyze data. Specifically, the methodologist identifies the research design, the methods for choosing samples, and the tools for data analyses. This specialist becomes an in-house consultant for selecting the process by which one derives meaning from the data, recognizes patterns, and solves problems within a domain. Methodologists become organizing agents within their field by focusing on the heuristics of their domain and validating the method of discovery for their discipline.

The methodologist holds a unique position within the discipline. Organizing agents are often called on by substantive experts to advise on a variety of process issues within their field because they have a different perspective than do the experts. On any given day, an epidemiologist, for example, may be asked to consult on studies of the effects of alcoholism on a community or the spread of a virus, or to review a double-blind clinical trial of a new pharmaceutical product. In each case, the epidemiologist is not being asked about the content of the study; rather he is being asked to comment on the research methods and data analysis techniques used.

Well over 200 analytic methods, most from domains outside intelligence, are available to the intelligence analyst; however, few methods specific to the domain of intelligence analysis exist.³⁰ Intelligence analysis lacks specialists whose professional training is in the process of employing and unifying the analytic practices within the field of intelligence. Knowing how to apply methods, select one method over another, weigh disparate variables, and synthesize the results is left to the individual intelligence analysts – the same analysts whose expertise is confined to specific substantive areas and their own domains' heuristics.

Intelligence needs methodologists to help strengthen the domain of analysis. Such methodologists need to specialize in the processes that the intelligence domain holds to be valid. In some fields, like epidemiology and program evaluation, methodologists are expected to be experts in a wide variety of quantitative

³⁰ Exceptions include: S. Feder, "FACTIONS and Policon: New Ways to Analyze Politics," H. Westerfield, ed., *Inside CIA's Private World* (New Haven, CN: Yale University Press, 1995); R. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999); R. Hopkins, *Warnings of Revolution: A Case Study of El Salvador*, TR 80-100012 (Washington, DC: Center for the Study of Intelligence); J. Lockwood and K. Lockwood, "The Lockwood Analytical Method for Prediction (LAMP)," *Defense Intelligence Journal*, Vol. 3, No. 2, 1994, pp. 47-74; J. Pierce, "Some Mathematical Methods for Intelligence Analysis," *Studies in Intelligence*, Summer, Vol. 21, 1977, pp. 1-19 (declassified); E. Sapp, "Decision Trees," *Studies in Intelligence*, Winter, Vol. 18, 1974, pp. 45-57 (declassified); J. Zlotnick, "Bayes' Theorem for Intelligence Analysis," H. Westerfield, ed., *Op. Cit.*

and qualitative methods. In other fields, the methodologists may be narrowly focused – a laboratory-based experimental methodologist, for example, or statistician. In all cases, however, methodologists can only be effective if they are experts at the process of making meaning within their own disciplines.

In order to overcome heuristic biases, intelligence agencies need to focus personnel, resources, and training on developing intelligence methodologists. These methodologists will act as in-house consultants for analytic teams, generate new methods specific to intelligence analysis, modify and improve existing methods of analysis, and increase the professionalization of the discipline of intelligence.

Conclusion

Intelligence analysis uses a wide variety of expertise to address a multivariate and complex world. Each expert uses his or her own heuristics to address a small portion of that world. Intelligence professionals have the perception that somehow all of that disparate analysis will come together at some point, either at the analytic team level, through the reporting hierarchy, or through some computational aggregation.

The intelligence analyst is affected by the same confounding variables that affect every other expert: processing time, pattern bias, and heuristic bias. This is the crux of the paradox of expertise. Domain experts are needed for describing, explaining, and problem solving; yet, they are not especially good at forecasting because the patterns they recognize are limited to their specific fields of study. They inevitably look at the world through the lens of their own domain's heuristics.

What is needed to overcome the paradox of expertise is a combined approach that includes formal thematic teams with structured organizational principles; technological systems designed with significant input from domain experts; and a cadre of analytic methodologists. Intelligence agencies continue to experiment with the right composition, structure, and organization of analytic teams; they budget significant resources for technological solutions; but comparatively little is being done to advance methodological science.

Advances in methodology are primarily left to the individual domains. But relying on the separate domains risks falling into the same paradoxical trap that currently exists. What is needed is an intelligence-centric approach to methodology, an approach that will include the methods and procedures of many domains and the development of heuristics and techniques unique to intelligence. In short, intelligence analysis needs its own analytic heuristics designed, developed, and tested by professional analytic methodologists. This will require using methodologists from a variety of other domains and professional associations at first, but, in time, the discipline of analytic methodology will mature into its own sub-discipline with its own measures of validity and reliability.

Intelligent Learning

*Max Boisot**

Introduction

I will summarise and integrate some of the ideas that have been proposed at this conference. I will do this with the help of a simple conceptual framework for exploring the nature of information flows, the information-space or *I-Space*. Since I am new to this community, I have no idea whose feet I might be treading on as I attempt to interpret what I have experienced.

The Intelligence Challenge: Fast Learning

Intelligence is presented as the gathering, processing, interpretation, and sharing of data under adversarial conditions. Intelligent learning is about doing this ever more efficiently and effectively and in circumstances that are always evolving and changing. In other words, learning, by introducing the time dimension into intelligence processes, adds the challenges of complexity and emergence to the tasks.

Everything that I have heard at this conference has convinced me that intelligence services are involved in a *learning race*. They have to scan fuzzy and ambiguous data for threats and opportunities, plausibly interpret and structure it into something that can be intelligibly communicated, get it shared and then absorbed by the relevant authorities, and all this at a faster pace than that at which the threat or opportunity materializes.

What kind of a challenge does a learning race pose for intelligence services? I will briefly approach the issues from a knowledge management perspective.

* Prof. Max Boisot is professor of strategic management at the Open University of Barcelona.

The Information Space or I-Space

Consider two characters, a Zen Buddhist and a bond trader and how they deal with information.

The Information Environment	
<u>Uncodified</u>	<u>Codified</u>
Slow	Fast
Local	Global
Ambiguous	Clear
Trust	Contract
Face to Face	Impersonal
Focus on Shared Values	Focus on Analysis
<i>The World of Zen Buddhists</i>	<i>The World of Bond Traders</i>

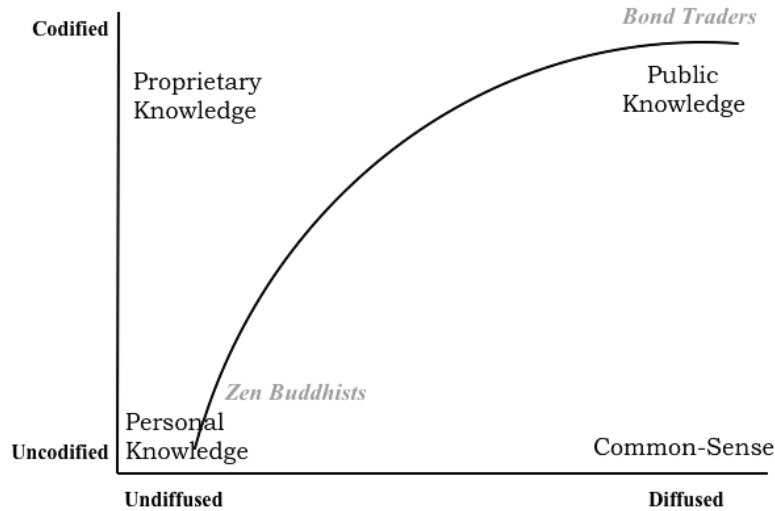
Ref.1.1.1 © Max Boisot 1999

The basic assumption is that the Zen Buddhist is very happy to operate in an information environment that is characterized by ambiguity, complexity, and fuzziness. Communications, therefore, are highly local and face-to-face, and are only effective under conditions of high trust that inevitably limits exchanges to a small number of people.

The Bond trader, by contrast, has a preference for an information environment characterized by clarity and simplicity. He or she wants to be able to communicate impersonally and instantaneously with a large number of unknown people spread around the world.

This difference between the Buddhist and the Bond Trader can be illustrated by means of a simple diagram which is a core of the conceptual framework –the *information space* or *I-Space* – that I will use.

The Information-Space (I - Space)



Ref. 1.1.1

© Max Boisot 1999

On the vertical scale we indicate how far a given phenomenon or experience can be compressed into a compact code – ie, how far it can be *codified*. At the bottom of the vertical scale, phenomena are very intangible and almost impossible to codify – a person’s face, the atmosphere in a room, knowledge of how to ride a bicycle, etc. As one moves up the scale it becomes possible to capture phenomena with progressively compact codes. First one can do it with images, and then further up with words. We reach the limits of codification with abstract algebraic symbols or numbers.

On the horizontal scale in the diagram, we can place a population of intelligent agents (not to be confused with a population of “intelligence” agents!) for whom a message has potential relevance. What the curve in the diagram tells us is that the more you can compress that knowledge into codes – that is to say, the further up the codification scale you can travel, the faster and more extensively you can diffuse it per unit of time. With an uncodified message, for example, only a few agents can be reached within a given time unit. They will be located towards the left on the horizontal scale in the lower regions of the I-Space. With a codified message, by contrast, the whole of the agent population can be reached,

as indicated by the curve reaching out to the right in the upper regions of the I-Space.

In the lower left hand region we are in the world of Zen Buddhist. Their knowledge is tacit and hard to articulate. It does diffuse, but very slowly and only on a face-to-face basis over a long period of time to small groups of people that can be trusted – ie, Zen disciples who are on the same wavelength. Such knowledge is often acquired by *shared socialization*.

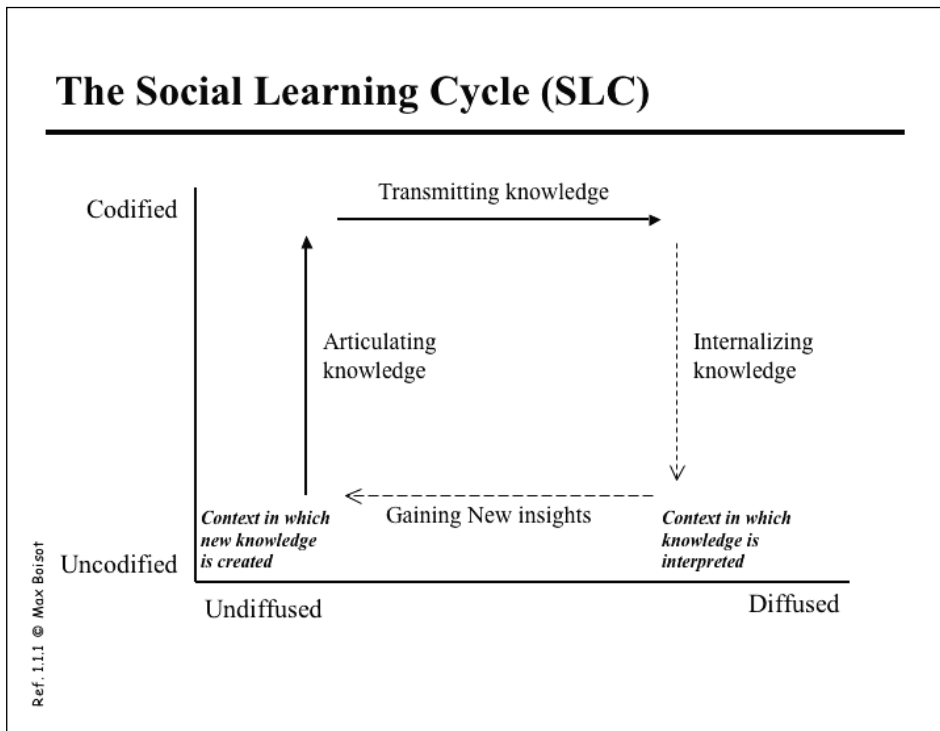
In the top right hand region of the I-Space we are in the world of the Bond Trader, a world in which well-codified information in the form of prices and quantities can diffuse impersonally and instantaneously throughout a given population and the push of a computer key.

In order to achieve speed and communicative efficiency, we try to move our knowledge up the I-space, codifying it in order to facilitate its transmission. But as we do so we lose much of the context that is accessible in the lower part of the I-Space, that is, we sacrifice communicative effectiveness. Context is always less codified than what can be distilled from it and doesn't travel along the diffusion scale in the way that well-codified messages do.

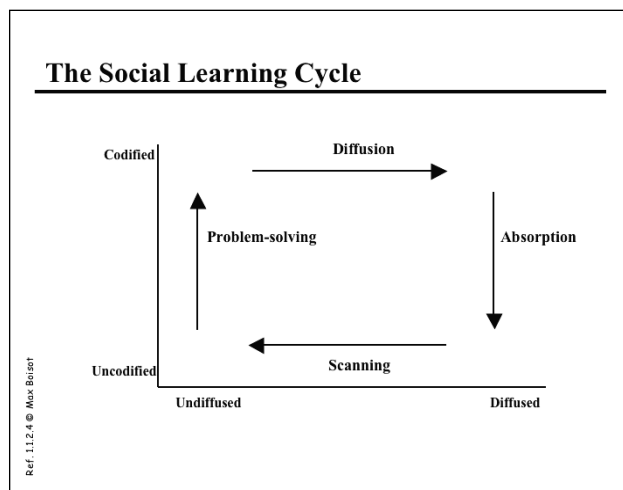
Because knowledge that can be moved up the codification scale is easier to share, then provided that one is in a position to control its diffusion process, it can be traded. It becomes proprietary knowledge. But because much of this knowledge has no context for the recipient, he or she may have difficulty internalising it and integrating it with his or her implicit common-sense models of the world.

The Social Learning Cycle (SLC)

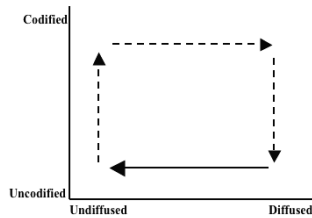
A failure to fully internalise such knowledge, to make sense of it, leads either to frustration or to learning. That is, it either leads to abandoning any attempt to extract information from incoming data or it gives rise to search, in which either further data is sought or new implicit models are sought. In the process, new insights may be developed which in turn have to be codified. *Under adversarial conditions, you want to impose the first reaction on the adversary and to pursue the second strategy yourself.* Understanding the dynamics of the learning process allows you to pursue both options simultaneously.



The process of codifying, sharing, absorption and scanning just described make up the components of a Social Learning Cycle – or *SLC* – that are described in the following figures.



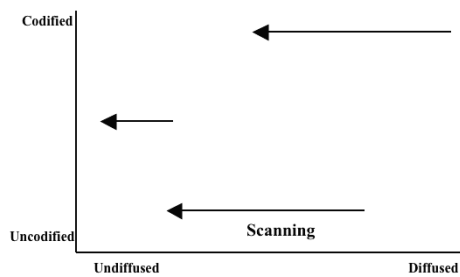
Characteristics of the Social Learning Cycle: Scanning



- Identifies threats and opportunities
- Signals are often fuzzy. detection is slow and uncertain
- Data is often public, interpretations are not- they are often unique
- Group pressure can distort the scanning process

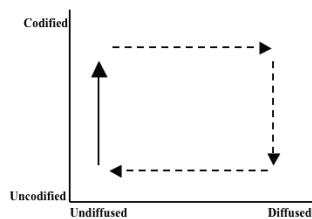
Ref. 11.2 © Max Boisot

How Do You Scan?



Ref. 11.2.4 © Max Boisot

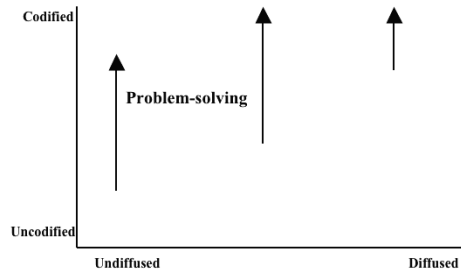
Characteristics of the Social Learning Cycle: Problem Solving



- A response to what is scanned
- Codification gives structure and coherence to the response
- It reduces uncertainty and ambiguity
- It sheds uncodified data along the way
- It generates conflict by forcing selection

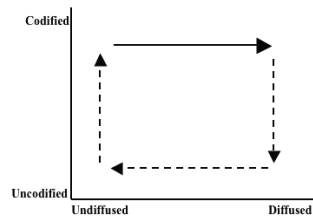
Ref. 11.2 © Max Boisot

How Do You Problem Solve?



Ref. 1.1.2.4 © Max Boisot

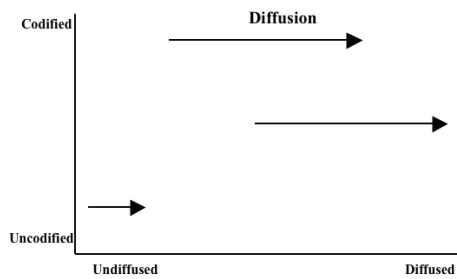
Characteristics of the Social Learning Cycle: Diffusion



- Codified data diffuses rapidly - unless controlled
- It will only register with those who know the codes
- The data is de-contextualised when it is codified
- Diffusing data reduces its scarcity value

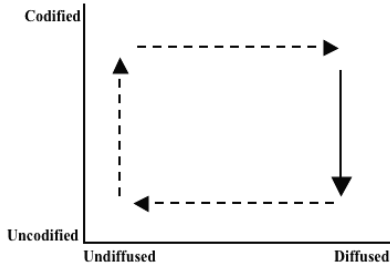
Ref. 1.1.2 © Max Boisot

How Do You Diffuse?



Ref. 1.1.2.4 © Max Boisot

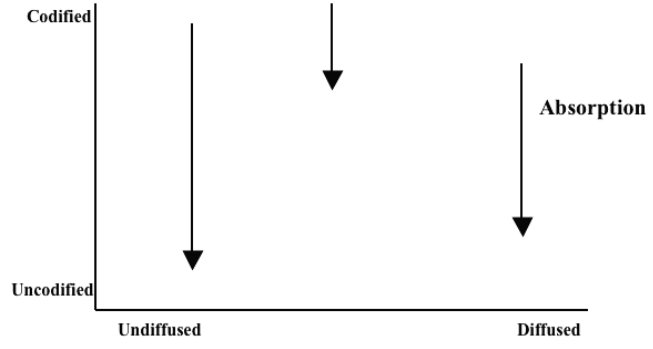
Characteristics of the Social Learning Cycle: Absorption



- Newly diffused data is applied in a learning by doing “fashion”
- An uncodified stock of practical experience builds up around the codified data
- The codified data may or may not match the “common sense” world of the user
- If it does not, a new round of scanning and learning is initiated

Ref. 11.2 © Max Boisot

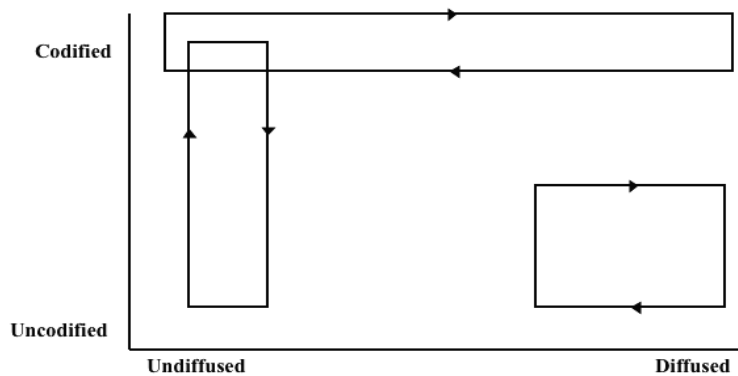
How Do You Absorb?



Ref. 11.2.4 © Max Boisot

As can be seen, the different components of the SLC can start anywhere in the I-Space and end up anywhere. Thus the SLC can adopt any one of a number of shapes that reflect the particular learning strategies or blockages of a group or an organization.

The Many Shapes of the Social Learning Cycle



Ref.1.1.2.1

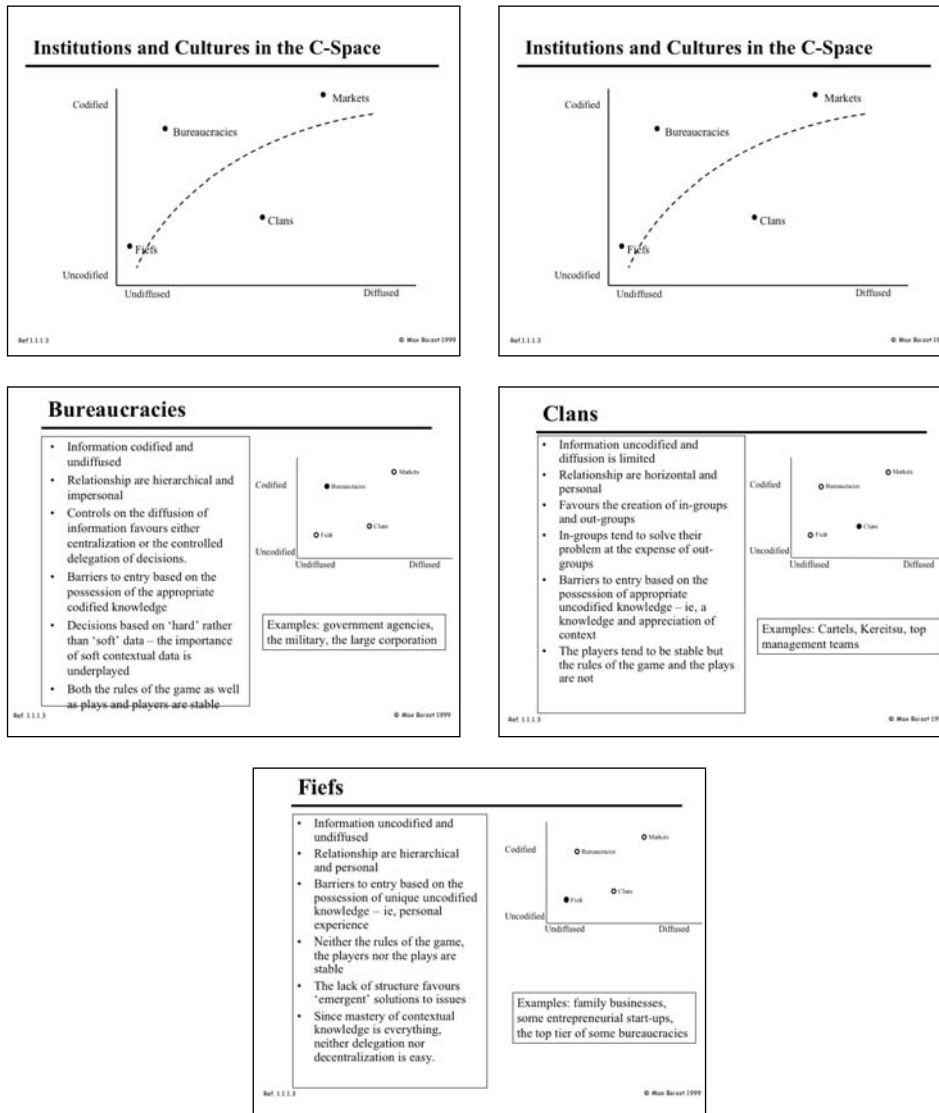
© Max Boisot 1999

The Culture of Learning

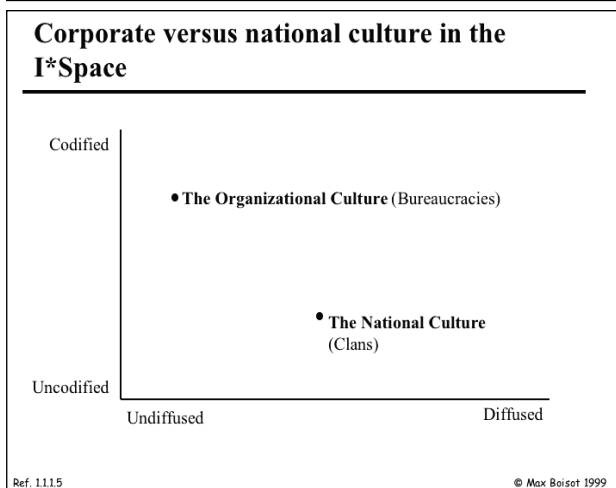
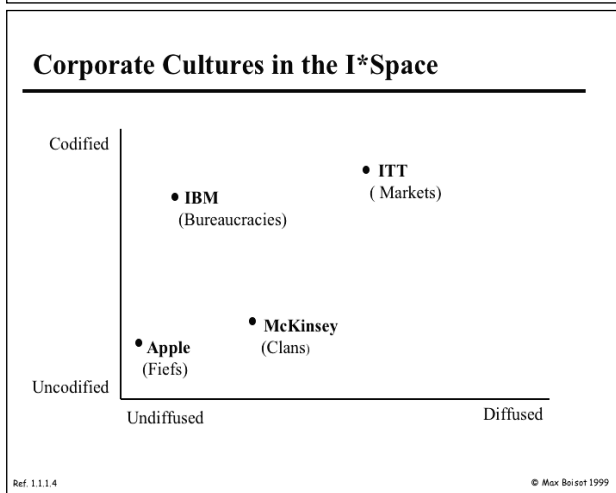
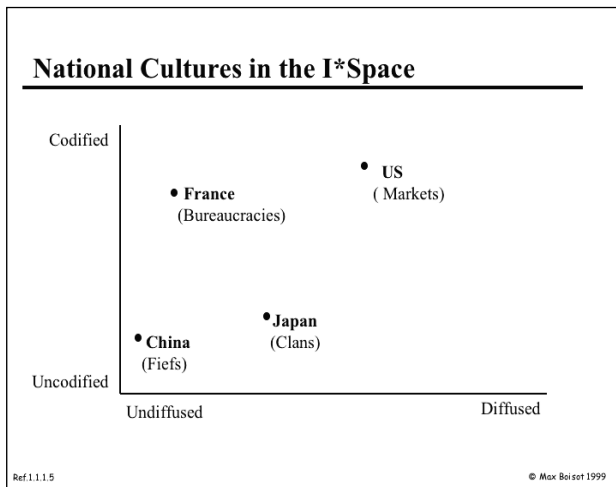
How can one develop a culture of fast learning? Effective learning involves visiting every region of the I-Space. It involves scanning from as broad a population as one can, codifying for maximum compactness, reaching every member of a target audience speedily (one does not want to reach everyone on the diffusion scale with the same message), and making sure that messages are fully internalised and integrated into the implicit models that shape the audience's outlook.

Recurrent information exchanges with agents in different regions of the I-Space, over time, allows institutional structures – markets, bureaucracies, clans, and fiefs – to emerge in these regions that have the effect of facilitating these exchanges. As we have seen with our example of the Bond Trader, *markets* operate in an information environment characterized by the ready availability of well-codified and well diffused information – ie, market prices. The Zen Buddhist, by contrast, operates in an information environment characterized by hard to articulate tacit knowledge that is considered unique and hard to share. Such knowledge is often a source of charismatic personal power for those who possess it which gives rise to *fiefs* – institutions that are based on the exercise of personal power. *Bureaucracies* emerge when the diffusion of well-codified knowledge is brought under some kind of central control, thus giving rise to a hierarchical access to such knowledge. Finally, *clans* are decentralized fiefs in which

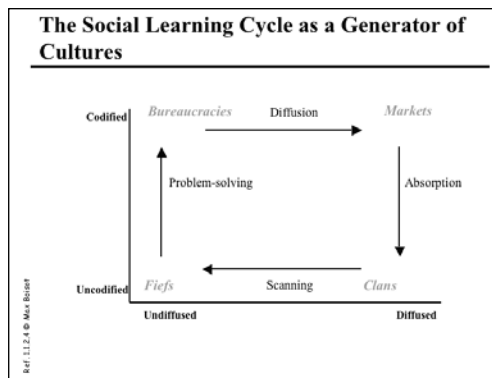
tacit knowledge can only be shared on a face-to-face basis among relatively small groups, Such sharing gives rise to the creation of in-groups – those who have access to such knowledge – and out-groups – those who do not.



Configurations of such institutional structures characterize an organization's or a group's *culture*. Culture is an emergent property of recurrent group communicative processes. It can occur at the level of a street gang, a firm, an industry, a region, or a nation state. Each of these different populations can be located on the diffusion scale of the I-Space and so can give rise to an I-Space analysis at different levels.

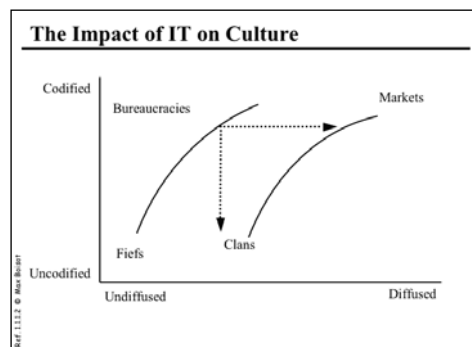


The institutional structures just mentioned can either facilitate the learning process if they speed up the SLC, or they can impede the learning process if they end up monopolizing all information exchanges, thus blocking the growth of alternative institutional structures in other regions of the I-Space.



Information and Communication Technologies (ICTs)

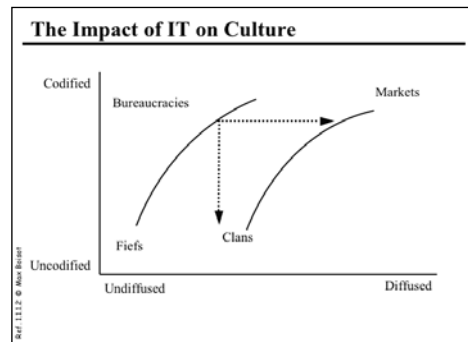
How might the development of ICTs affect the learning and cultural processes that we have just described? One answer is intuitively obvious: at any given level of codification, ICTs have the effect of allowing us to reach more agents with more information per unit of time. This can be thought of as a horizontal shift to the right of the diffusion curve in the I-Space that improves communicative *efficiency*.



But the development of ICTs, by increasing the bandwidth available, also have another effect: for any number of agents that we wish to reach along the diffusion scale, these can now be reached at a lower level of codification than

hitherto. The implications of this second effect are considerable, since what it implies is that one need no longer sacrifice context to the need for speedy and efficient communication. Thus the new ICTs will also improve communicative *effectiveness*.

Note, however, that the new ICTs, by shifting the diffusion curve to the right, will lower the costs of operating in markets and clans, but increase the costs of operating in bureaucracies and fiefs. This poses a challenge of cultural adaptation and change for those cultures that are heavily invested in bureaucracies and fiefs. Bureaucracies and fiefs will not disappear – fast learning requires an institutional capacity in *all* regions of the I-Space – but they will need to diversify and accommodate values and belief systems that arise in information environments quite different from those that they are accustomed to.



Conclusion

Framing this problem of cultural adaptation as a learning race between intelligence services and their adversaries brings out the fact that these adversaries may well have developed this cultural capacity – mutating, for example from highly local fiefs to decentralized clans – and may thus be in a better position to take advantage of existing ICTs than intelligence services who continue to view them as technological fixes – ie, as *alternatives* to the need for cultural and institutional change rather than as *drivers* for them.

APPENDIX

Appendix A

NEW FRONTIERS OF INTELLIGENCE ANALYSIS Shared Threats, Diverse Perspectives, New Communities

Istituto Superiore di Polizia, Rome (Italy), 31 March-2 April 2004

CONFERENCE PROGRAM

Concept:

This is an international, “by invitation only,” unclassified conference. It is organized by the Global Futures Partnership of the Sherman Kent School for Intelligence Analysis in Washington D.C., the Link Campus University of Malta in Rome, and the Gino Germani Center for Comparative Studies of Modernization and Development, with the support of Italy’s Presidency of the Council of Ministers.

It has invited broad participation from national government ministries, intelligence and security services, law-enforcement agencies, and selected participation by academic, private sector, and non-government counterparts. Participants have come from all regions of the world, but principally from Europe and the United States.

Objectives:

1. To continue the transnational dialogue, initiated at the International Conference in Priverno, Italy in February 2001, on the nature and role of intelligence analysis in 21st century democratic societies.

2. To discuss whether and how intelligence analysis should adapt to deal more effectively and creatively with the new global threat environment and other emerging challenges.

3. To explore avenues for better transnational and transsectoral cooperation in the intelligence analysis of global threats by:

- sharing concepts and best practices to increase common understanding of advanced analytical practices;*
- developing a common lexicon for intelligence analysis;*

- *exchanging national perspectives on common analytical challenges, particularly concerning transnational threats;*
- *building relationships and networks across national borders, between intelligence, security, and law-enforcement communities, and between government, NGO and business communities;*
- *identifying opportunities and innovative possibilities for better transnational cooperation.*

WEDNESDAY 31 MARCH

Conference Opening Ceremony

Moderator: Ms. Carol Dumaine

Chief, Global Futures Partnership, Sherman Kent School for Intelligence Analysis, Washington D.C.

Pref. Dott. Carlo De Stefano

Director of the Italian Preventive Police

Prof. Vincenzo Scotti

President of Link Campus University of Malta, Rome

Ms. Jami Miscik

Deputy Director for Intelligence, Directorate of Intelligence, Washington D.C.

Heads, Italian Intelligence Services

On. Dott. Gianfranco Fini

Deputy Prime Minister of Italy

Conference Introduction

Prof. Luigi Sergio Germani

Director of the Gino Germani Center, Rome, and Academic Director, Master of Arts in Intelligence and Security Studies, at Link Campus University, Rome.

Ms. Carol Dumaine

Chief, Global Futures Partnership of the Sherman Kent School for Intelligence Analysis, Washington D.C.

PANEL ONE

Thinking About a Changing Threat Environment: Emerging Global Trends, New Paradigms, and Implications for Intelligence Analysis

Moderator: Dr. Bowman Miller

Director for Analysis of Europe, U.S. Department of State, Bureau of Intelligence and Research, Washington, D.C.

Three distinguished speakers from Europe, the USA, and Asia will offer contrasting views on emerging global trends and changes in the threat environment. The focus of the panel will be transnational forces and their implications for the practice of intelligence analysis.

Ambassador Robert Hutchings

Chairman, National Intelligence Council, Washington, D.C.

Looking Over the Horizon: Strategic Choices, Intelligence Challenges

Mr. Bruno Joubert

Assistant Secretary for Africa, French Foreign Ministry

Are the Deeper Factors of Analysis Useful?

Mr. Peter Ho

Permanent Secretary of Defense for Singapore

Emerging Trends in the Threat Environment: An Asian Perspective

Special Presentation

Prof. Christopher Andrew

Professor of Modern and Contemporary History and Chair of the Faculty of History, Cambridge University, UK

Historical Attention Span Deficit Disorder:

Why Intelligence Needs to Look Back Before Looking Forward

Introduced by: Mr. Roy Wiese

Director of the Kent Center, Sherman Kent School for Intelligence Analysis, Washington, D.C.

PANEL TWO

New and Emerging Challenges for Intelligence Analysis

Moderator: Mr. Anthony Campbell

President, Canadian Association of Security and Intelligence Studies (CASIS)

Speakers will offer contrasting presentations on how the organization and practice of intelligence analysis must change in light of new and evolving trends and challenges. The discussion will center on the impact transnational and asymmetric threats and information overload, as well as challenges to the resourcing, staffing, tradecraft, and professional cultures of analytic organizations.

Mr. Greg Fyffe

Executive Director, Intelligence Assessment Secretariat, Privy Council Office

A Canadian Perspective

Hr. Dr. Markus Ederer

Deputy Director of Analysis, Bundesnachrichtendienst (BND), Germany

A German Perspective

Dr. David Chuter

Senior Research Associate, Centre for Defence Studies, London

A British Perspective

Mr. Federico de Torres Muro

Director of Intelligence, Center for National Intelligence, Spain

A Spanish Perspective

Closing remarks

Dinner Speech

Welcome Remarks by co-hosts:

Gen. C.A. Dott. Nicolò Pollari

Director of SISMI, Italy

Ms. Jami Miscik

Deputy Director for Intelligence, Directorate of Intelligence

Featured Speaker: Mr. Peter Schwartz
Co-founder, Chairman, Global Business Network, Emeryville, California
Inevitable Surprises

Introduced by Dr. Warren Fishbein
Principal, Global Futures Partnership

THURSDAY 1 APRIL

Breakout Groups

Participants will be organized into groups of approximately 15. Each group will have a facilitator and rapporteur. Participants will discuss their conclusions from the first two panel sessions and dinner speaker, comment on key challenges facing intelligence from their national or organizational perspective, and identify three top priorities for change.

PANEL THREE

Responding to New Analytical Challenges: Analysis of Transnational Threats by Inter-Governmental and Non-Governmental Organizations

Moderator: Prof. Gianni Ricci
Link Campus University of Malta, Rome

Four speakers will address analysis of transnational threats from perspectives outside traditional government intelligence systems. Speakers will illustrate “lessons learned” that may be applicable to government intelligence organizations and identify opportunities for cooperation between government and non-government analysts.

Prof. Phil Williams
Professor of International Security at the Graduate School of Public and International Affairs, University of Pittsburgh

Terrorists, Tipping Points and Typhoid Mary: Networks and Transnational Threats

Prof. Amy Sands
Dean, Graduate School of International Policy Studies, Monterey Institute of International Studies, Monterey, California

Implications of Transnational Actors for WMD Terrorism and Proliferation Analysis

Mr. Jan Garton
Assistant Director, Criminal Analysis Sub-Directorate, INTERPOL, Lyon, France

Criminal Intelligence Analysis in International Law Enforcement

Prof. Georg Frerks
Professor of Conflict Studies, Utrecht University; Head Conflict Research Unit, Netherlands Institute of International Relations “Clingendael”; and Trustee of the Forum on Early Warning and Early Response, London

Early Warning and Response in Transnational Conflict: Best Practices and “Lessons Learned”

Feedback from Breakout Group Discussions (Rapporteurs report to the plenary)

PANEL FOUR

Responding to New Analytical Challenges: Analysis of Transnational Threats by Government Intelligence Organizations

Moderator: Ms. Sylvia Beatriz Cucovaz
General Director of Strategic Planning, Presidency of Argentina

Three speakers from government intelligence organizations from around the world will discuss their experiences and their organizations’ “best practices” in the analysis of transnational threats.

Dr. David Gordon
Director, Office of Transnational Issues, Directorate of Intelligence, Washington, D.C.

Evolving Approaches to Analyzing Transnational Threats: Key Challenges and Potential Partnerships

Dr. Michael Wesley
Assistant Director-General, Transnational Issues, Office of National Assessments, Australia

Analyzing Transnational Intelligence

Mr. Christian Jenny
Head of the Proliferation/Terrorism Analysis Branch, Swiss Strategic Intelligence Service (SIS)

Adapting to the Analysis of Transnational Threats: Challenges for a Small Intelligence Service

Special Presentation

Dott. Franco Ionta

Magistrate, Italy

Analysis of the International Terrorist Threat in Italy

FRIDAY 2 APRIL

PANEL FIVE

Tools, Techniques, and Teams for Analysis and Warning

Moderator: Dr. Mary O. McCarthy

Visiting Fellow, Center for Strategic and International Studies and former US National Intelligence Officer for Warning

Mr. Gilman Louie

CEO of In-Q-Tel, Washington, D.C.

In-Q-Tel's Vision of Advanced Analytic Tools

Dr. Rob Johnston

Institute for Defense Analysis, Alexandria, Virginia

Analytic Expertise: Promise and Paradox

Mr. Max Boisot

Professor of Strategic Management at the Open University of Barcelona

Intelligent Learning

Breakout Groups

Towards Better Ways of Doing Analysis and Enhancing Warning

This breakout group session will take the top challenges for intelligence analysis identified by breakout groups the day before and discuss possible responses to these challenges. Facilitators will guide breakout members to look at both responses to the challenges of content as well as responses to the challenges of cooperation. At the same time, facilitators will be noting any "lessons learned" discovered by their groups.

Plenary – Reports from Breakout Groups

Special Presentation

Dott. Piero Saviotti

Magistrate, Italy

Protecting Privacy and Conducting Intelligence Analysis

Roundtable with Senior Officials: Reflections

Moderator: John McShane

Dean, Sherman Kent School for Intelligence Analysis, Washington, D.C.

Ms. Jami Miscik

Deputy Director for Intelligence, Directorate of Intelligence, Washington, D.C.

Gen. C.A. Dott. Nicolò Pollari

Director of SISMI, Italy

Looking Ahead

Conference co-directors Ms. Carol Dumaine and Prof. L. Sergio Germani summarize and synthesize the key ideas and conclusions of the conference based upon panel and break out group discussions and will address next steps.

CLOSING REMARKS

Lead Facilitator:

Mr. Alain Wouters

Facilitators, by Breakout Group:

1. Tim Bolderson-United Kingdom
2. Robert Bood-Netherlands
3. Jaap Leemhuis-Netherlands
4. Aarne Nurmio-Finland
5. Raimondo Boggia-Italy
6. Luca Gatti-Italy
7. Philippe Vandebroek-Belgium
8. Alain Wouters-Belgium
9. Beverly Neale Rush-United States, Anthony Campbell-Canada
10. Roger George-United States, Warren Fishbein-United States

Rapporteurs, by Breakout Group:

1. Michael Herman-United Kingdom
2. Margaret Purdy-Canada
3. Steve Artner-United States
4. Jean-Louis Tiernan-Canada
5. David Robson-United Kingdom
6. L. A. Williams-Trinidad and Tobago
7. Tim Buch-United States
8. Martin Munkelt-Sweden
9. Alessandro Politi-Italy
10. T. Raja Kumar-Singapore

Acknowledgements

The New Frontiers conference organizers extend their appreciation and thanks to the leadership and administration of the Istituto Superiore di Polizia in Rome for their generous support for this program.

In particular, we wish to thank:

Pref. Dott. Mario Esposito, *Director*
Dott. Gerardo Cautilli, *Deputy Director*
Dott. Artenio Libriani
Dott.ssa Luciana Franchini
Dott. Italo De Astis
Dott. Paolo Zirilli
Isp. Alessandro Mallozzi

We also wish to express our gratitude to Mrs. Jenny Clarke for her excellent contribution to the organizational effort and to the preparation of this book.

We are also grateful to Link Campus University of Malta graduate students in Intelligence and Security Studies Stefano Izzi, Diego Cazzin, Gianluigi Davì and Diego Abbo, as well as to Paola Oliviero of the Link Campus University of Malta Office of Graduate Programs.

Printed in Italy by C.G.E. srl - Rome (Italy)
May 2005