International Journal of Intelligence and CounterIntelligence

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ujic20

The Revolution in Intelligence Affairs: 1989-2003
Eric Denécé
Published online: 20 Nov 2013.

To cite this article: Eric Denécé (2014) The Revolution in Intelligence Affairs: 1989-2003, International Journal of Intelligence and CounterIntelligence, 27:1, 27-41, DOI:
10.1080/08850607.2014.842796
To link to this article: http://dx.doi.org/10.1080/08850607.2014.842796
That a “Revolution in Military Affairs” (RMA) took place in the early 1990s is widely known. The concept was born of technological, political, social, and economic changes that were to fundamentally alter the future of warfare, introducing a completely new type of military and organizational structure for the effective projection of force.

Though most experts accepted the reality of a fundamental transformation in the practice of warfare, few saw that a parallel revolution was occurring in the intelligence world, even though this specific field of national security was undergoing similar challenges and change.

That a “Revolution in Intelligence Affairs” in the 1990s and early 2000s actually occurred and its effects has become increasingly evident. This
“intelligence revolution” resulted from a combination of changes in international politics, information technologies, and socio-political context.

**Geopolitical Upheaval**

In the early 1990s, the intelligence community was hit hard by geopolitical upheaval and the collapse of the former international paradigm. The Cold War, a conflict involving covert operations, lasted nearly a half-century. Over that period an East–West rivalry drove the activities of intelligence agencies in both the North Atlantic Treaty Organization (NATO) and Warsaw Pact countries. The sudden loss of an opponent, which had up until then justified their very existence, first disoriented the agencies, and then made them question their future.

**Information Technologies (IT) Revolution**

Since the late 1980s, the world has undergone a far-reaching technological revolution with innovations in data communications, electronics, and telecommunications. The combined effect of these innovations has radically altered today’s world. Digital technologies led to a convergence of sound, image, and data, allowing instant transmission, automatic processing, and increased computing capacity and storage. This technological revolution has had a major impact on intelligence practice.

**New Socio-Political Context**

The rise of new democratic demands and political requirements (better governance, ethics, pressure groups, etc.) has also impacted the intelligence agencies.

These three factors combined to transform the context in which agencies operate, their areas of focus, and their tradecraft. They have led to major changes in the rules governing intelligence activities.

**CONSEQUENCES OF GEOPOLITICAL UPHEAVAL**

**New Threats and New Enemies**

From one major threat emanating from a single opponent (the former Soviet Union/USSR), Western intelligence agencies now face and must track six dangerous phenomena involving new players with highly unpredictable patterns of behavior.

*Radical Islamic Terrorism.* Since 11 September 2001 (9/11), Islamic jihad has been the main threat to international security. Al-Qaeda is a new kind of terrorist organization in that it does not depend on any one nation state
and no one has direct control over it. No other terrorist group enjoys such a
degree of independence. Jihadist networks operate in more than 60 countries,
but without a hierarchical structure.¹

The late Osama bin Laden did not himself exert direct control over any
terrorist groups. The organization he founded operates more like a
“holding company,” defining strategy and targets, and offering volunteers
money, training, or logistical support. Al Qaeda is—and was—primarily a
technical assistance center for Islamic terrorists. It taught other radical
groups how to use the Internet to communicate and disseminate
bomb-making techniques, and provided them with skills to increase their
operational capabilities.

Transnational Criminal Organizations. Criminal cabals constitute the major
threat of the twenty-first century. These organizations have turned the IT
revolution and economic globalization to their advantage to develop the
illegal economy.² They are continually expanding and diversifying their
activities: drugs, weapons, human trafficking, smuggling, and counterfeiting.

Specialists report that criminal money represents more than 7 percent
of today’s global economy. At the beginning of the 1990s, criminal activity
represented 2 percent of global gross domestic product (or gross world
product). The illegal economy thus grew threefold in two decades.

The financial power wielded by criminal organizations is awesome. Whole
regions of Latin America, Africa, and the Caucasus are now in the hands of
criminal organizations. Their development is a serious threat to the national
security of some states. They do not seek to control territory, rather they wish
to control institutions and commercial companies and banks that allow them
to launder money.

Proliferation of Weapons of Mass Destruction. Most of the former USSR’s
nuclear weapons have remained under the control of Russia. But some
Soviet nuclear scientists provided expertise to spread nuclear technology
and materials to ideologically radical states, such as Iran,³ Pakistan, and
North Korea. The unpredictable behavior of these states and their
relations with terrorist groups are a major cause for concern.

Increased Economic Competition Between Developed Countries. The main
consequence of the end of East–West rivalry has been increased
competition among developed nations. States and companies are engaged
across all sectors in a veritable war for access to markets or global natural
resources. The fierce competition has led to some analysts talking of a new
economic war, and saying that the rules of this new “game” are far from
fair.⁴
Some countries—for instance the United States—have redirected part of the activities of their intelligence services to support exports and to destabilize foreign competitors. More and more people with backgrounds of working in state intelligence agencies are now employed in the private sector.

Rise of New Violent Activists. The victory of the liberal model over Communist totalitarianism has paradoxically led to a proliferation of anti-capitalist groups, seeking to challenge or fight the evolution of modern societies for a range of reasons, ranging from Communist nostalgia to anarchy, and far-Right and far-Left ideologies.

Post-industrial societies have also given rise to a myriad protest groups on almost every issue: anti-globalization, opposition to vivisection, environmental protection, anti-consumerism, anti-advertising.

Most of these movements are willing to take violent action or even carry out terrorist attacks to promote their ideas. Such groups (eco-terrorists, animal rights groups) specialize in sabotage, kidnapping, and bomb attacks. They see themselves at war and adopt a covert organizational approach like that used by terrorist groups.

For example, in the United Kingdom, the Animal Liberation Front (ALF) has destroyed medical laboratories and sent letter bombs to scientists working in the pharmaceutical industry. In the United States, the Earth Liberation Front (ELF) has been even more violent in the name of protecting the Earth. As a result, these movements have been blacklisted, as have terrorist groups like al-Qaeda.

New Unpredictable Events or “Disrupters.” The fragmentation of the New World Order, as evidenced in the Balkans and Central Asia among others, means that crises are likely to break out in even more regions. Some states will try to take advantage of the new world situation—for instance, Iraq in 1991. Other new phenomena, notably the Arab Spring, erupt without warning. A myriad threats, a diversification of crises, and growing unpredictability are the hallmarks of this new situation.

Most new threats stem from the development of non-state actors. Today, many organizations have taken full advantage of new technologies, world decompartmentalization, and globalization. Non-governmental organizations (NGOs) as well as transnational terrorists, international criminal organizations, cyber hacktivists, and protest groups are increasingly Internet-savvy and globally operational. They have developed strategies beyond the control and scope of nation states through new kinds of organizations: networks, Starfish system, etc.

Though new actors are now taking part in “The Great Game,” previous threats such as secessionism, political violence and extremism, civil war, and the threat of military action remain.
Traditional intelligence methods no longer worked against al-Qaeda, criminal organizations, and newly emerged activists. Indeed, nothing is more difficult than fighting a virtual organization that has no land or physical headquarters to protect and operates without a central command. Intelligence agencies have had to change their operational practices, largely inherited from the Cold War. Accordingly, intelligence practice has gone through five major transformations.

1) From Macrointelligence to Microintelligence. During the Cold War, intelligence agencies were looking to acquire knowledge on large targets: garrisons holding several thousand men, air or naval bases, missile sites, and weapons production plants. The information being sought was necessarily housed in several different places, due to the high number of staff or forces involved, the importance of telecommunications, and the large number of subcontractors. Those resources offered many targets for the recruitment of agents and intercepts. Moreover, the security services were working tirelessly to better understand the capabilities of an enemy whose intentions were well-known. After 1991, the situation changed dramatically.

Al-Qaeda does not have a centralized command. This absence makes the identification of decision centers more complicated and increases the number of potential targets. Gathering data that will prevent a terrorist act is extremely difficult. Security agencies are looking for information of a microscopic nature, specifically protected within “closed societies.” The critical data is often housed only in the brain of the terrorist, in an off-line, off-grid computer, in a message lost among the plethora of phone calls made each day, in a suitcase, or in a hotel room where three or more Salafi terrorists might meet. Secrets are shared among a small number of people, who live in a state of constant paranoia, and who implement stringent security measures.

Such target data, called microscopic intelligence, differs greatly from the intelligence acquisition of the Cold War era, where the objective was to acquire information on macroscopic targets.

2) New Challenges for HUMINT and the Running of Agents. The gathering of information through illegal means remains an essential part of intelligence work but is difficult because of the nature of the objectives.

The penetration of a terrorist network or criminal organization is an extremely difficult operation. Jihadist groups are “closed societies.” In each cell, men often come from the same village, have usually known each other for a long time, and may speak a dialect unknown to Westerners. For them to immediately detect and eliminate an intruder is easy.
Recruiting within terrorist movements is almost impossible. Their very strongly-held, radical Islamic beliefs make them resistant to conventional methods of recruitment as double agents. Western agencies have to recruit men from outside the movement in order to infiltrate them. But that process often involves working with individuals whose loyalty remains fragile.\(^{11}\)

Moreover, when Western intelligence succeeds in infiltrating an agent into a jihadist group, ensuring secure and constant communication with the agent becomes a huge challenge because terrorist cells apply drastic security measures. The group’s members live closely together, monitor each individual member, and prohibit any contact with the outside world. And, obviously, information about a future attack has no value if it comes too late.

Finally, infiltrating a terrorist organization poses a moral problem: The agent usually has a very short lifespan—often only a few weeks to a few months—since the objective of the Jihadist cell is to carry out a suicide bomb attack. Few men and services agree to risk such an outcome in the service of an intelligence or police organization.

Consequently, gathering secret intelligence via human assets (HUMINT) has become increasingly difficult and dangerous: recruitment and penetration are still possible, but increasingly complex.

(3) Limits of Technical Intelligence. Because penetrating such groups is very difficult agencies must seek out information on the periphery, in areas where technology is key. Although, during the Cold War, understanding the Soviet mindset from the outside was possible, countering terrorist strategy without penetrating their organizations is impossible.

(4) Growing Interdependence Among Agencies. An increasing segment of today’s intelligence work is done in conjunction with international cooperation programs. To investigate and monitor a jihadist group or criminal organization, an overview of its global activities is necessary. No country can do it alone.

Yet, some cooperation is sensitive and may generate problems for democratic countries. Cooperation with Middle East intelligence agencies, in particular, is difficult due to the widespread use of torture in most of those countries. Western public opinion has become more vocal in its criticism of such partnerships, even when in the interests of their own security.

(5) New Economic Rivalries and Coopetition. Though intelligence agencies around the world are increasingly working together a rivalry among them still exists, mostly for political or economic reasons, resulting in what may be termed “coopetition.”

A good example is the French/United States relationship of 2003. At the time, the two countries were strong adversaries on the Iraqi invasion issue, but very close allies in the fight against al-Qaeda.\(^{12}\)
CONSEQUENCES OF THE INFORMATION TECHNOLOGIES REVOLUTION

Limits of Signals Intelligence

One of the biggest paradoxes of modern intelligence is signals intelligence (SIGINT). In Western countries, intelligence by technical means grew substantially during the Cold War, mostly because human research provided only limited results against the Communist security system. Eighty percent of the information collected on the Soviet Union was of a technical origin.¹³

These tools are now clearly limited.¹⁴ Technical intelligence, also comprising imagery intelligence (IMINT), and the other “INTs,” is increasingly effective, but cannot provide all the answers, for several reasons:

(A) Exponential Growth of World Telecommunications. The incredible growth of modern communications—telephone, GSM, Internet—is a major challenge for SIGINT agencies. A short forty years ago only 5,000 computers were in use worldwide. These computers were neither linked to each other nor connected to a fax machine or phone.

Today, some 400 million computers are in use worldwide, all interconnected, as well as nearly 20 million fax machines, and hundreds of millions of mobile phones. In 2000, the U.S. provider America Online (AOL) transmitted 225 million e-mails per day. Today, traffic on the electronic networks is more than twelve times greater.

Of course, the development of SIGINT satellites, combined with the rise of new supercomputer capacity, has made significant progress, and data storage is also improving rapidly. Yet, the reality is that security agency technological capacity has failed to match the growth of telecommunications. Even the U.S. cannot effectively monitor the hundreds of millions of e-mails, phone calls, and electronic money transfers made every day worldwide, though it attempts to do so. And, among the huge number of communications surveiled every day by the U.S., only about 10 percent is seriously processed and analyzed on time.

(B) Development of Private Cryptology. A rapid development in cryptography has taken place. Encryption by companies and private individuals is growing everyday, posing a major challenge to the SIGINT agencies. The fight between the cryptologists and those seeking secure communications has slowly turned to the advantage of the latter. Of course, breaking a code with adequate computing capability will always be technically possible. But such a process can take weeks, and most terrorist or criminal organizations need to protect their secret talks for just a few days, mainly as they plan their operation.
Above all, many means of communications are now available that allow an individual, terrorist, or criminal to bypass the issue of encryption altogether, meaning that most of them can send high-value messages by simply using non-monitored devices and means.

For example, al-Qaeda uses both modern means of communication (Internet, encrypted cell and satellite phones, and radio) and human operatives who carry messages. By using several mobile phones instead of only one, a jihadist can thwart wiretaps set by intelligence agencies. Wiretaps are occasionally of no use at all because terrorists often communicate among themselves using direct human contact.

(C) Translation Problems. Another challenge for SIGINT is translation. The National Security Agency (NSA) reports that some 6,500 languages are spoken around the world. For intelligence agencies to find enough translators in the rare languages used by mafia or terrorist organizations is extremely difficult.

In 2000, the Federal Bureau of Investigation’s (FBI) linguistic department had 900 translators and a budget of 21 million dollars. By 2004, the figures had climbed to 1,200 translators with a 70 million dollar budget. However, that same year, 30 percent of intercepted communications were stored without being translated. After a three-year period, due to data storage problems, a large percentage of the intercepts had been deleted without being processed.

New Challenges of Data Processing

Today, more information is available to the public than ever before. A major challenge facing modern intelligence is not information gathering, but data processing. Three areas where this is particularly important are:

Open Source and Social Media. The IT Revolution has generated an explosion in information resources. Information is found everywhere and in all forms, among them books, journals, videos, CD-ROMs, Internet, and social media. The volume of online resources is growing incredibly fast. About 10 million Web pages are created every day, and the total volume doubles every four years. Specialized commercial databases are created and updated every day, creating more new sources of information. Commercial imagery, a new resource available to anyone, has put an end to the monopoly of State intelligence from space. More recently, the growth of social media—Twitter, Facebook, and similar sites—has provided another channel of access to individuals and their private life.

Opportunities to acquire knowledge on any subject have changed. Considering the huge amount of data collected every day, the great
challenge facing modern intelligence is to separate “the wheat from the chaff” and “to connect the dots.”

**PROPINT and Personal Data Protection.** Proprietary Intelligence (PROPINT) is the term applied to data-protected personal information found in digital databases that are in either public or private sector hands. It concerns personal communications, movements, air travel, financial transactions, immigration status, and national insurance records. People leave tracks behind them as they go about their lives in a high-tech society.

PROPINT is very useful for counterterrorism or counterintelligence, and much more so than OSINT (open source intelligence). These databases are—or not, as the case may be—legally accessible to intelligence and security agencies, depending on applicable personal data protection legislation. Every country has a different approach to, and legislation on, data protection, but most often the price to pay is the end of peoples’ privacy.

For twenty years, the amount of data and product to process has grown at a rapid pace. The work of intelligence agencies has changed as they expand their spheres of activity. They have had to develop new skills in such new directions as technology, finance, economics, market research, technology, climate change, and international crime.

Consequently, the issue involves the benefits and risks of information technologies.

The information revolution has provided many new tools: data mining and automated analysis software, and increased computer and data storage capacity. But enemies or disrupters are also using these tools to criminal ends. This gives them unmatched power for covert activities; even small organizations can take advantage of low-cost technologies to develop highly effective intelligence systems.

**Privatization and Diversification of Intelligence Operators and Suppliers**

The information revolution has also led to the development of private intelligence companies, creating new partners as well as new competitors for state agencies.

**New Partners...** Companies are new customers of Intelligence. Over the last decade, economic competition has become much more intense. This has led many companies to develop their own business intelligence capabilities to meet their information needs and to protect themselves from acts of destabilization.

Consultants are new providers of intelligence. Many consultants—mainly former members of state security agencies—have taken advantage of this
new market to develop their business. They are given missions that were previously part of the tasks of state agencies. Some of them also perform intelligence, training, or security missions on behalf of governmental agencies.

In 2010, the newly appointed U.S. Director of National Intelligence (DNI) found that 70 percent of the intelligence budget was allocated to private contractors and 50 percent of employees working for the Defense Intelligence Agency were private contractors.

The industrial sector also offers a wide range of intelligence products, from databases to software.

...And New Competitors. The privatization of intelligence challenges the traditional position of state agencies, which have long been the only sources for policymakers. For the first time in their history, they are in competition with new elements from the private sector, who are often able to provide high-quality intelligence, and sometimes more quickly and accurately than the agencies themselves. As a result, national intelligence agencies must accept some form of comparison with private players.

CONSEQUENCES OF THE NEW SOCIO-POLITICAL CONTEXT

The third major evolution for security agencies comes from the new demands made by modern democratic societies involving ethics, governance, and transparency, and new requests from politicians who must face and meet the threat of terrorist attack.

New Demands of Democratic Societies

Ethics: The Rejection of Torture and Demands for Protection of Personal Data.

Law enforcement, security, and intelligence agencies should accept the reality that ethics do matter to democratic public opinion: certain “red lines” must not be crossed.

Indeed, the non-respect of international law and the development of coercive methods, as seen at Guantanamo and Abu Ghraib—and which are considered counterproductive by specialists—deeply shocked democratic societies and was a source of embarrassment to the U.S. authorities.15

Ethical principles should also be applied to govern the use of PROPINT and intrusive investigative methods.

Governance: Generalization of Parliamentary Oversight and Performance Auditing Leading to the Proper Use of Intelligence and Security Agencies.

Historically, security agencies have long enjoyed a freedom of action justified by “la Raison d’État.” However, democratic societies no longer consider acceptable that organizations working in the shadows are unaccountable for their actions.16
Moreover, citizens and their elected representatives need to be sure that executive branch authorities are using intelligence agencies properly and that they are delivering “the best result for the money spent.”

**Transparency: Publicized Intelligence—Communication vs. Secrecy.**

To the modern citizen, transparency is ineffective without proper communications. Intelligence agencies must develop or improve their public relations abilities because, since 9/11, they have been under the spotlight. As never before, they are a subject of public interest and debate.

Security agencies should explain their job, mobilize public opinion, and attract the best people in the country. Communicating to the public is also useful to explain how taxpayer money is being used and how the effectiveness of the intelligence agencies can actually be determined. Yet, the public and media must in turn accept the secrecy involved in intelligence work, as it is a key component for the success of intelligence operations and consequently for the security of the general public.17

**New Behavior of Policy Makers**

**New Political Pressure.** A terrorist attack always has a profound effect on public opinion. When such an event happens, government and security services are often considered to have failed. So policymakers are aware that such attacks must not occur on their own soil, both to protect the nation’s citizens, and also to ensure their own reelection. Therefore, political pressure on agencies is increasing. Political leaders are demanding more and more of the intelligence and securities agencies, applying pressure on them to avoid any surprises that could destabilize their government.

**Manipulated Intelligence.** Unfortunately, democratic governments most often refuse to bear their responsibilities and tend to blame the security agencies for their own mistakes when attacks occur. Doing so is easy for them, as an intelligence agency is unlikely to protest. An example of this approach occurred on 9/11 in the United States.

Moreover, some government behavior—for example the U.S. and the United Kingdom in 2003—has led to a politicization of intelligence. Some political leaders, like President George W. Bush and British Prime Minister Tony Blair, seemingly manipulated intelligence to promote their own agenda and interests. The White House requested intelligence, not to have a clear assessment of the situation in Iraq, but rather to find information that would support its decision to invade that country. This led to such disinformation as the alleged and spurious links between Iraqi dictator Saddam Hussein and al-Qaeda, as well as the questionable existence of Iraqi weapons of mass destruction (WMD). The ultimate result of the internal conflict was that some agencies have lost their independence.
Terrorism: A Narrow Focus for Intelligence and Security Agencies. Focusing solely on terrorism and hostages, to the detriment of everything else, is dangerous. These are not the only threats agencies have to deal with. For example, in February 2013, a secret report highlighted certain intelligence blind spots because the U.S. Intelligence Community was still so focused on al-Qaeda. A panel of White House advisers warned President Barack Obama that U.S. spy agencies were paying inadequate attention to China, the Middle East, and other national security flash points because they had become too focused on Islamic terrorism.

Persistent Misunderstandings with Policymakers. Intelligence is not a magic tool, able to do everything, at all times. Intelligence works under only specific conditions. But in most countries policymakers ignore the real role of intelligence agencies and what can be asked of them.

EVOLUTIONARY STAGES OF INTELLIGENCE

In looking back at the history of modern intelligence, three different stages emerge—three major “evolutions”:

World War I. The early years of the twentieth century featured the birth of modern telecommunications (telegraphy), and with it the development of cryptology and intercepts, which grew significantly during the war. Here, the main driving force was technology, seconded by global geopolitical conflict.

World War II. In the early 1940s, intelligence agencies operated on an unprecedented scale all over the world, with a major evolution in the use of HUMINT, Counterintelligence, SIGINT, and Special Operations. The main reason was geopolitics, seconded by a series of technological/military innovations introduced during the war. At the end of the war intelligence and security agencies became permanent bodies of national state administrations. The Cold War brought nothing really new, just a global spread of the innovations that had emerged during World War II.

1989–2003: “The Third Wave.” This “revolution” took place over a fourteen-year period, from the fall of the Berlin Wall to the U.S.–U.K. invasion of Iraq. It resulted both from geopolitical and technological upheavals, but also from socio-political changes.

The developments constituted a real revolution: context, matters of interest, opponents, methods, technologies, and time of response have all changed, and the new situation has little in common with the intelligence landscape of the Cold War. Something huge has happened to transform “The Great Game.” It could be called a “Copernican Revolution.”

Today, intelligence and security agencies furnish a smaller part of policymakers’ information needs. Though the modern services are
increasingly effective, they paradoxically cover a smaller proportion of the information needs of decisionmakers on world issues and challenges. This is a normal evolution. Open source intelligence has reduced the focus of intelligence agencies down to their core business: gathering the secrets of others. But, despite some efforts to make it so, studying climate-change is not part of the intelligence agency remit.

Intelligence and security agencies are not forecast institutes or prospective bodies. Forecasting is another profession entirely. This is not the direction for the agencies to take. Prospective reports do not constitute intelligence. They should not try to, and are not able to, predict the future.

These agencies should do what others do not. They are government “secrets finding and problem solving” organizations. They are not “global intelligence” agencies. Intelligence agencies are not the ones who provide a total picture, but rather deliver the missing parts of the puzzle.21

WHAT NEXT? LOOKING FORWARD

Because of the urgency of, and narrow focus on, Islamic terrorism question marks exist as to whether the next intelligence threats have actually been scoped out. Unfortunately, in most countries, the answer is a negative.

Intelligence agencies should develop prospective analysis for their own purposes:

- Threat dynamics and evolution;
- Threat convergence (terrorism + crime, islamism + far-left extremism22);
- Identification of new threats.

Though intelligence work cannot be reduced to mere foresight, the security services should try to detect the rise of future opponents. They should track particular states or organizations that, given their financial or technological clout, could become the disruptive actors of tomorrow.

But if intelligence and security agencies try to predict the future in all directions, on every subject, they will surely commit more mistakes in the future than they did in the past.

Intelligence is an art. Not a science.

REFERENCES


19 Ibid.

